Land Power Revue der Schweizer Armee, Nr. 3, Dezember 2005

Nr. 3, Dezember 2005

LAND POWER REVUE

DER SCHWEIZER ARMEE
DE L'ARMEE SUISSE

Politik und Gesellschaft

Bedrohung und Schutz der Informationsgesellschaft
Stephan Loretan, Martin Dietrich

Network Enabled Operations – vernetzte Operationsführung; nicht nur eine technologische Herausforderung Andreas Moschin

INFORMATION IMPERIALISM
Wissen ist Macht – Wie steht es mit dem Schutz unseres Wissens? Jörg A. Bischof

Network Enabled Operations (NEO): L'approche suisse de la transformation
Christian Bühlmann

Teilstreitkraft Heer

Das operativ/taktische ISTAR-System der Schweizer Armee zur Erstellung der erkannten Bodenlage
André Kotoun

Geschichte

Operation «MERKUR»: Die deutsche Luftlandung auf Kreta als Prüfstein des neuseeländischen Gefechtsnachrichtendienstes
Hans Rudolf Fuhrer, Adrian Baschung

Beilage zur ASMZ 12/2005

Herausgeber:	KKdt Luc Fellay, Kdt Heer	
Chefredaktor:	Oberst i Gst Michael A.J. Baumann	Chef Heeresdoktrin
Joint-Redaktions-kommission:	Br a D Rudolf Läubli	Vorsitz, Redaktor ASMZ
	Oberst i Gst Michael A.J. Baumann	Chef Heeresdoktrin
	Dr. Michael Grünenfelder	Chef Luftwaffendoktrin
	Oberst Hans Dickenmann	G 5/USC Planung TSK Heer
	Oberst i Gst Peter Suter	Chef Planung – Projekte – Versuche Luftwaffe
	Oberst i Gst Alain Vuitel	Chef Militärdoktrin der Armee

Verlag und Druck: Huber & Co. AG, Grafische Unternehmung und Verlag, 8501 Frauenfeld

Beilage zur «Allgemeinen Schweizerischen Militärzeitschrift» ASMZ, Nr. 12, Dezember 2005

Die ***Land Power Revue*** ist ein offenes Forum, das Studium, Gedanken und Diskussion zur Landstreitmacht im weitesten Sinne und zu ihrer Anwendung für die Schweizer Sicherheitspolitik und Armee im Besonderen fördert.

Sie unterstützt das Heer in der

- Entwicklung von Doktrin und Konzepten
- Beitragsleistung zur sicherheitspolitischen Debatte
- Ausbildung der Kader der Armee
- Führung des internationalen Dialogs

Vorwort des Kdt Heer

Technologische Entwicklungen haben in der Vergangenheit immer wieder tief greifende Veränderungen in der Gesellschaft und damit auch in Streitkräften ausgelöst. Jene Armeen, denen es nicht gelang, zweckmässige Antworten auf diesen Wandel zu finden, waren im Einsatzfall benachteiligt. Sie konnten ihrer Aufgabe als Machtmittel des Staates nicht – oder im Bedarfsfall teilweise nur mit schrecklichen Folgen – nachkommen.

Wir nehmen heute in verschiedenen militärischen Bereichen technologisch bedingte Veränderungen wahr. Im Waffenwirkungsbereich sind zum Beispiel die Erhöhung der Reichweite, die prägnante Steigerung der Treffgenauigkeit und die Verwendung von unterschiedlichsten, optimal dem Zweck entsprechenden, Wirkmitteln augenscheinlich. Ebenso, wenn auch nicht ganz so klar, lassen sich im Schutzbereich (zum Beispiel durch die Anwendung von Stealth-Eigenschaften) Veränderungen erkennen. Im Führungsbereich sind es die eklatant gesteigerten Fähigkeiten zur Feststellung der aktuellen Lage und die Möglichkeiten zur markanten zeitlichen Verkürzung der Entscheidungsprozesse durch die Verwendung immer leistungsfähigerer Informatiksysteme.

Die Schweizer Armee trägt diesen Veränderungen Rechnung. Im Führungsbereich kommt das im Aufbau des künftigen Führungs- und Wirkungsverbundes der Armee zum Tragen, welches es ihr ermöglichen soll, die Aufträge noch effizienter zu erfüllen.

Integrale Bestandteile dieses Verbundes bilden die Systeme C4I (Command, Control, Communication, Computers, Information) und ISTAR (Intelligence, Surveillance, Target Acquisition, Reconnaissance).

Beide Systeme der Schweizer Armee sollen dazu beitragen, den Entscheidträgern aller Stufen rechtzeitig, umfassend und bedarfsgerecht erforderliches Wissen als Grundlage für die im Führungsprozess zu treffenden Entscheidungen zur Verfügung zu stellen. Das Wissen über die eigenen und die nachbarlichen Kräfte wird durch das Führungssystem C4I generiert. Das ISTAR-System soll das Wissen um die Widersacher – symmetrischer, asymmetrischer oder dissymmetrischer Art – beitragen und zudem sicherstellen, dass erkannte Schlüsselziele durch mit dem System vernetzte Effektoren nach kürzester Zeit (teil-) automatisiert bekämpft werden können.

Mit der vorgesehenen, mittelfristig abgeschlossenen Implementierung des künftigen Führungs- und Wirkungsverbundes wird die Schweizer Armee im Führungsbereich technologisch zweck- und zeitgemässe Voraussetzungen haben, um ihre Aufträge effizient erfüllen zu können.

Die vorliegende Ausgabe der Land Power Revue ist diesem künftigen Führungs- und Wirkungsverbund, schwergewichtig dem Thema ISTAR, gewidmet.

Ich hoffe, die Beiträge dieses Heftes vermitteln Ihnen ebenso Informationen und Erkenntnisgewinn wie neue Denkanstösse. In diesem Sinne wünsche ich Ihnen eine anregende Lektüre.

Kommandant Heer
Korpskommandant Luc Fellay

Editorial des Redaktors

Sun Tzu um 500 v. Chr.: «Deswegen sage ich:
– Kenne deinen Feind und kenne dich selbst, und in 100 Schlachten wirst du nie in Gefahr geraten;
– Kennst du den Feind nicht, aber dich dafür umso besser, sind die Aussichten auf Sieg oder Niederlage etwa gleich;
– Bist du über deinen Feind und über dich selbst im Unklaren, wirst du sicher in jeder Schlacht in Gefahr sein.»

Er sagt auch:
– «Der Grund, warum kluge Herrscher und gute Heerführer den Feind schlagen, (...), ist das Vorauswissen.
– Was man als Vorauswissen bezeichnet, kann man weder von Geistern noch von Göttern erfahren, weder mit Vergleichen mit vergangenen Begebenheiten noch durch Berechnungen. Man muss es von den Leuten erfahren, die die Feindlage gut kennen.»

Der Drang, die Informationsüberlegenheit über einen Widersacher zu erlangen, ist ein Merkmal verantwortlicher Führung geblieben. Sun Tzu hat als Mittel und Methoden den Einsatz von Spionen, Agenten und Aufklärern zur Subversion und zur Aufklärung des Feindes sowie die Anwendung von Täuschung und List gekannt. Die technologische Entwicklung eröffnet uns heute zusätzliche Möglichkeiten. Wer im Zeitalter der Informationsgesellschaft nicht im Stande ist, solche zu nutzen und die unfreundliche Anwendung neuer Mittel und Methoden gegen sich zu verhindern, ist in einer Auseinandersetzung im Nachteil.

Auch die Schweizer Armee hat die Veränderungen erkannt und als Antwort darauf ein Schwergewicht auf die Entwicklung eines neuen Führungs- und Wirkungsverbundes gelegt.

Diesen Themenkreis hat die vorliegende Ausgabe der Land Power Revue zum Inhalt. Mein Dank für tatkräftige und umfassende redaktionelle Unterstützung geht an Oberst Stefan Räber, lic. phil. I, Politischer Berater, sowie Major Ariel Sergio Goekmen, Direktor der Credit Suisse. Beide Milizoffiziere des Heeresstabes haben mir die zeit- und sachgerechte Herausgabe ermöglicht.

Unter der Rubrik **Politik und Gesellschaft** *befassen sich Stephan Loretan und Martin Dietrich mit der Bedrohung und dem Schutz der Informationsgesellschaft. Andreas Moschin stellt die Grundsätze der vernetzten, militärischen Operationsführung dar. Er zeigt dabei auch internationale Trends auf und illustriert diese an Hand von Beispielen ausländischer Streitkräfte. Jörg A. Bischof gibt uns unter anderem Informationen über ein heute aktives, globales, elektronisches Aufklärungssystem, welches den gesamten E-Mail-, Telefon-, Fax- und Telexverkehr überwacht und auswertet. Christian Bühlmann schliesslich erläutert Ihnen kurz den schweizerischen Ansatz zur Nutzung der technologischen Entwicklung in der militärischen Operationsführung.*

Aus der **Teilstreitkraft Heer** *gibt uns André Kotoun einen tiefen Einblick in das sich noch in der Planungsphase befindliche, operativ/taktische ISTAR-System-Projekt der Schweizer Armee zur Erfassung, Bearbeitung und Nutzung der erkannten Bodenlage.*

Fast schon traditionellerweise liefert uns Hans Rudolf Fuhrer, diesmal zusammen mit Adrian Baschung, den Beitrag zur **Geschichte.** *An Hand der 1941 durchgeführten deutschen Luftlandung auf Kreta zeigen sie auf, dass die Militärgeschichte neben der Untersuchung dokumentierter historischer Ereignisse in der Wehr- und Kriegsgeschichte – besonders wenn die Vorkommnisse gut dokumentiert sind – durchaus als Analyseinstrument für aktuelle Fragen verwendet werden kann. Stehen sie damit im Widerspruch mit den Aussagen von Sun Tzu, der doch behauptet hat, dass Vorauswissen nicht durch das Vergleichen mit vergangenen Begebenheiten erarbeitet werden kann? Beurteilen Sie selbst.*

Michael A. J. Baumann

Bedrohung und Schutz der Informationsgesellschaft

Die beiden Autoren stellen im folgenden Artikel die Information als volks- und betriebswirtschaftliche Grösse in den Mittelpunkt. Nach einer abgrenzenden Definition erläutern die Autoren, welche Bedrohungsformen existieren und skizzieren, wie sich Unternehmen mittels einer adäquaten Sicherheitsarchitektur dagegen schützen können.

Stephan Loretan, Martin Dietrich *

Die Volkswirtschaften der Industrieländer haben sich in der Vergangenheit stark verändert. Die Liberalisierung der Telekommunikationsmärkte, das rasante Wachstum des Internets und die zunehmende Vernetzung von Wirtschaft und Gesellschaft führten allesamt zur Entstehung der Informationsgesellschaft. Unsere Gesellschaft und unser (all-) tägliches Leben stützen sich in vielfältigster Art und Weise auf Informationen. Diese sind sowohl in geschriebener, gesprochener, aber immer mehr und aktueller auch in digitaler Form unterschiedlichster Ausprägung vorhanden. Im Verlaufe der letzten Jahre wurden Informationen und deren Inhalte zu einer nicht mehr wegzudenkenden Ressource des wirtschaftlichen, sozialen und privaten Geschehens. Sowohl aus betriebs- wie auch aus volkswirtschaftlicher Sicht ist die Ressource Information längst ein Gut wie die klassischen (althergebrachten) Faktoren Arbeit, Kapital und Boden.

Information als Ressource

Für viele Gesellschaftsbereiche hat sich die Ressource «Information» mittlerweile zur strategisch wichtigsten Komponente entwickelt. Die Schweiz ist bei der Entwicklung zu einer Informationsgesellschaft weit fortgeschritten.

Gemäss dem Informatikstrategieorgan Bund (ISB) gibt sie am meisten Geld pro Kopf und Jahr für Informations- und Kommunikationstechnologien (IKT) aus. Dies zeigt sich deutlich, indem ein wesentlicher Teil des Lebens und Arbeitens darin besteht, Informationen und Wissen zu gewinnen, zu speichern, zu verarbeiten, zu vermitteln und zu nutzen. Grundlage all dieser Aktivitäten ist und bleibt der Einsatz von IKT. Exemplarisch für diese Entwicklung können die folgenden Beispiele aufgeführt werden:

- Innerhalb der IKT ist das Internet aufgrund seiner Verbreitung wohl am bedeutendsten. Sowohl im privaten als auch im unternehmerischen Bereich hat seine Nutzung stark zugenommen. Es wird über Informationsbeschaffung und Werbepräsenz hinaus zunehmend für Kommunikation und Transaktionen genutzt. Viele der neuen Internetdienste durchleben gerade die Umwandlung vom «Gratis»-Medium zum Wirtschaftsgut. Auf längere Sicht gesehen ist die weitere Ökonomisierung des Internets und die Transformation zu einer weit gehend digitalisierten Dienstleistungsgesellschaft eine zentrale Herausforderung der Zukunft.
- Die Entwicklung der Informations- und Kommunikationstechnik war Antrieb für wesentliche Neuerungen in Produktion und Dienstleistung der letzten Jahre. Die Weiterentwicklung der Technologie ist entscheidend, um auch in Zukunft international konkurrenzfähige Produkte und Dienstleistungen anbieten zu können. Mehr als die Hälfte der Industrieproduktion und ein Grossteil der Exporte hängen heute vom Einsatz moderner IKT und elektronischer Systeme ab. Sie bilden die Grundlagen der wirtschaftlichen Leistungsfähigkeit jeder Industrienation. Sie wirken zusammen mit der Produktionstechnologie, Material- und Werkstofftechnologie, den optischen Technologien und der Mikrosystemtechnik. Für den Maschinen- und Anlagenbau liefern IKT Steuerungen, Test- und Prüfeinrichtungen, in der Chemischen Industrie regeln sie Verfahrensabläufe.
- IKT sind oft und meist ausschliesslich die Schlüsseltechnologien für Innovationen. Die dabei getätigten Investitionen tragen wesentlich zum Wirtschaftswachstum bei. Die gesamtwirtschaftliche Bedeutung der IKT geht aber weit über die der IKT-Branche hinaus. Durch die Generierung von Innovationen erzeugen IKT Wachstum und schaffen zukunftssichere neue Arbeitsplätze.

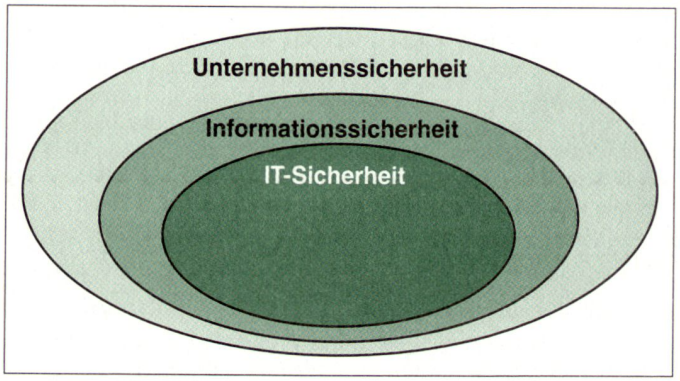
Informations- und Kommunikationstechnologien als Mittler

All diese Beispiele zeigen, dass die Nutzung und Verbreitung modernster IKT in der Informationsgesellschaft eine hohe wirtschaftliche und auch soziale Priorität haben. Im selben Umfang wie deren Bedeutung zunahm, steigerte sich jedoch auch die Abhängigkeit unserer Gesellschaft vom Vorhandensein und dem Informationsgehalt der IKT in den nachfolgend aufgeführten so genannten kritischen Infrastrukturen eines Landes:

- Energieerzeugung und -verteilung (Elektrizität, Öl, Gas)
- Transport von Gütern und Personen
- Telekommunikation
- Medien
- Finanzindustrie (Banken, Versicherungen)
- Notfall- und Rettungsdienste
- Versorgung (Gesundheitswesen, Lebensmittel, Wasser)
- Regierungsfunktionen von Bund, Kantonen und Gemeinden einschliesslich Polizei, Zoll und Armee.

In der Vergangenheit konnte man diese Schlüsselinfrastrukturen relativ gut schützen. Mit der zunehmenden Bedeutung der Ressource Information hat sich dies drastisch geändert.

Ein umfassender Schutz durch die Sicherheitsapparate eines einzelnen Staates (oder einer zuständigen Organisation) gestaltet sich aufgrund der umfassenden Vernetzung aller Bereiche, der teilweisen Privatisierung und der Globalisierung vieler Funktionen sehr schwierig. Eine Partnerschaft zwischen staatlichen Organen und der Privatwirtschaft ist ein absolutes Muss, um die Sicherheit der Infrastrukturen als nationale Aufgabe zu gewährleisten.



Sicherheitsebenen.

* Stephan Loretan, lic. oec. HSG, Berater für Projektmanagement und Organisation bei der BSG Unternehmensberatung. Ehemalige militärische Funktion: Hptm der Art in der Funktion als Nof, heute Stabschef ziviler Gemeindeführungsstab

Martin Dietrich, lic. oec. HSG, CISA, studierte Informationsmanagement. Er leitet die Entwicklung der BSG ITSEC ToolBox der BSG Unternehmensberatung, ist Sicherheitsexperte und führt Sicherheitsaudits durch.

Die Sicherheitsebenen

Mit dem Entstehen der Informationsgesellschaft muss zusätzlich zur physischen Sicherheit auch die Sicherheit der Ressource Information mitberücksichtigt werden. Diese integrale Sicht der Sicherheit beinhaltet so auch die Informationssicherheit. Sie grenzt sich von der Informatiksicherheit (IT-Sicherheit) ab, indem sich Letztere ausschliesslich mit elektronisch gespeicherten Informationen befasst, Erstere sich dagegen für den Schutz sämtlicher Informationen ungeachtet ihrer Darstellung und Speicherung verantwortlich zeichnet.

Wie durch das ISB richtig festgestellt wird, ist die Informationssicherung trotz ihrer hohen Affinität zu den IKT keine rein technische Aufgabe. Ein wirksames Informations-Sicherheits-Management-System (ISMS) hat auch die Bereiche Organisation und Prozesse, Politik und Gesetze und Ressourcen (Bsp. Personalausbildung) zu berücksichtigen.

Erforderliche IT-Sicherheit

Im Zentrum der folgenden Überlegung steht nun die IT-Sicherheit. Hierzu kann festgestellt werden, dass ohne sie kein (oder nur ein geringes) Vertrauen in die Informationssysteme vorhanden ist. Dies umso mehr, als dass der beständig zunehmende Einsatz von Informationstechniken in Produktion und Dienstleistungsgewerbe, in sozialen und öffentlichen Einrichtungen zu einer wachsenden Abhängigkeit aller Anwendungsbereiche von Informationstechnik führt. Wirtschaftliche Gründe und ein optimaler Wertschöpfungsprozess erfordern einen zuverlässigen IT-Betrieb, der ohne frühzeitige Planung, geeignete Sicherheitsmassnahmen und deren regelmässige Überprüfung nicht gewährleistet werden kann. Im Zentrum stehen dabei die verschiedenen Dimensionen der IT-Sicherheit:

- Die *Verfügbarkeit* bezieht sich auf die Funktionsfähigkeit, den eigentlichen lauffähigen Betrieb der eingesetzten Lösung und ist zukunftsorientiert; die IT soll so betrieben werden, dass die Systeme ab dem aktuellen Zeitpunkt in die Zukunft hinein verfügbar sind, und sie soll den Ausfall der Informationsverarbeitung und die Sabotage von Verarbeitungsprozessen verhindern.
- *Datenexistenz:* Die Dimension Datenexistenz ist bewusst von der Verfügbarkeit der Systeme getrennt. Grund dazu ist, dass die Ursachen und die Folgen von nicht verfügbaren Systemen oder nicht vorhandenen Daten unterschiedlich sein können. Zudem ist sie vergangenheitsorientiert, indem die IT so betrieben werden soll, dass keine Daten von heute, gestern und früher verloren gehen dürfen. Sie verhindert das bösartige Zerstören und unbeabsichtigte Löschen von Daten durch Personen und/oder Maschinen.
- *Integrität:* Die Integrität der Daten bezieht sich auf die inhaltliche Richtigkeit der Informationen. Sie stellt die Genauigkeit und Vollständigkeit der Informationen und ihrer Verarbeitungsmethoden sicher. Fehler in den Daten haben in der Regel direkte Auswirkungen auf das Vertrauen in die Informationen.
- Die Dimension *Vertraulichkeit* der Daten besteht in der Forderung, Informationen nur den berechtigten Personen zugänglich zu machen.

Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in der Folge von IT-Risiken erhöhen den Handlungsdruck, durch ein aktives IT-Sicherheitsmanagement die vier Dimensionen bestmöglich zu gewährleisten und so Schäden zu verhindern und das verbleibende Restrisiko zu minimieren.

Akute Bedrohungsformen

Dieses Restrisiko geht in einem grossen Teil von der Verwundbarkeit der Informationsnetze aus. Was zu Beginn mit dem Phänomen der «Hacker» eher belustigend zur Kenntnis genommen wurde und unter sportlichen Gesichtspunkten beargwöhnt wurde, ist mittlerweile zur ernsthaften Bedrohung geworden. Inzwischen eröffnet sich ein grosses Spektrum illegaler Datenzugriffe, das von Software- oder Datenmanipulation über Betrug, Datendiebstahl und Desinformation bis hin zu organisierter Kriminalität wie Wirtschaftsspionage und Terrorismus reicht. Im Visier der Angriffe stehen dabei ohne Unterschied die Computernetze von Staat, Wirtschaft und Wissenschaft. Nach einer Untersuchung von Price Waterhouse Coopers wurden 42 Prozent der grösseren Unternehmen der Europäischen Union (EU) Opfer der so genannten Cyberkriminalität. Die Dunkelziffer der nicht erkannten oder nicht gemeldeten Angriffe dürfte noch weit höher liegen. Dabei kamen die Angreifer keineswegs immer von aussen, sondern waren zu 60 Prozent so genannte Innentäter, also Personal der eigenen Unternehmung. Neben dem Täterkreis der Innentäter wird der freie und sichere Umgang mit Daten und Informationen noch von weiteren Seiten bedroht. Das ISB geht dabei von folgenden Kreisen aus:

- Einzeltäter, wie gelangweilte oft jugendliche Script-Kiddies, Cracker oder Hacker
- Gruppierungen, die aus politischen Motiven handeln
- Unternehmen, die aus wirtschaftlichen Motiven handeln
- Nationalstaaten mit kriegerischen Absichten

Nebst all diesen als illegal einzustufenden Handlungen und Betrachtungen darf nicht vergessen werden, dass die Sicherheit zusätzlich durch unbeabsichtigtes menschliches Fehlverhalten, technisches Versagen und Naturereignisse gefährdet sein kann.

Notwendige Schutzbedarfsdiskussion

Die Dimensionen der IT-Sicherheit und die aktuellen Bedrohungsformen verlangen die Etablierung und Durchführung eines Risikodialogs. Im Zentrum steht dabei die Ermittlung des Schutzbedarfs aufgrund der prozess- bzw. anwendungsspezifischen Anforderungen in den IT-Sicherheits-Dimensionen Verfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit.

Ermittelt wird der Schutzbedarf durch Beurteilung der wichtigsten Schadenszenarien und ihrer Ausprägungen, entsprechende Formeln ermöglichen ein nachvollziehbares Umrechnen (i. S. Quantifizieren?) der Szenarien in Schutzbedarfswerte. Folgende relevante Schadensaspekte werden berücksichtigt:

- Beeinträchtigung der Betriebsabläufe
- Personenschäden an Leib und Leben
- Rechtliche Folgen, Schadenersatzklagen
- Anzahl Mitarbeiter, die nicht arbeiten können
- Imageverlust
- Materieller Schaden
- Vorteil für die Konkurrenz
- Volkswirtschaftlicher Schaden

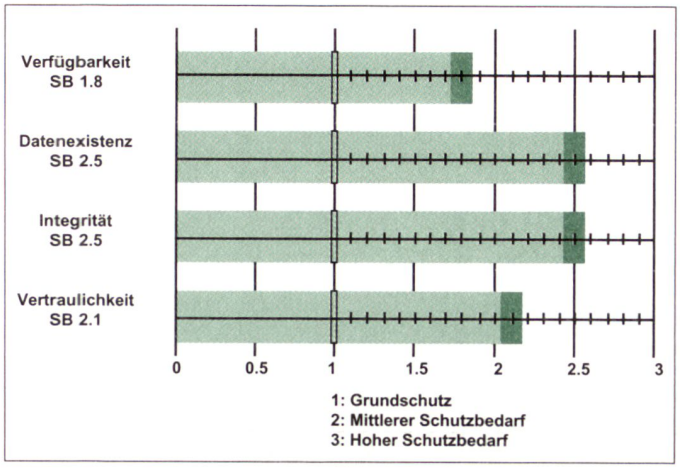
Die Ergebnisse lassen sich im Schutzbedarfsdiagramm darstellen und bilden die Anforderungen an die an der Leistungserbringung beteiligten Informatikkomponenten:

Messbarer Sicherheitszustand

Die in der Schutzbedarfsdiskussion bestimmten Sicherheitsanforderungen erlauben den Vergleich mit dem tatsächlichen Sicherheitszustand. Dazu empfiehlt sich die Gliederung in Prüfobjekte, an denen die einzelnen Prüfthemen gemessen werden:

- Rechenzentrum und seine Infrastruktur
- Server
- Operator
- Kommunikation
- Benutzer

Bewährt hat sich in diesem Vorgehen der Einsatz standardisierter Prüflisten respektive Fragestellungen, die auf internationalen Standards (Bsp. ISO), ergänzt mit praktischen Erfahrungen, beruhen und bereits mit möglichen bewerteten Antworten versehen sind. Für die Feststellung des Sicher-



Schutzbedarfsdiagramm.

heitszustandes dienen die im Voraus festgelegten Antwortmöglichkeiten. Sie enthalten die Anforderungen an einen hohen, genügenden und ungenügenden Schutz. Der mit den Prüflisten durchgeführte Soll-/Ist-Vergleich führt zu Massnahmen- und Pendenzenlisten zur Behebung der festgestellten Sicherheitslücken.

Angemessene Sicherheitsarchitektur

Sicherheitslücken lassen sich in der Regel nicht unmittelbar beseitigen. Die Etablierung einer adäquaten Sicherheitsarchitektur bedingt daher ein durchdachtes Setzen von Prioritäten unter Einbezug der Ergebnisse aus der Schutzbedarfsanalyse zur Verhinderung existenzgefährdender Schäden. Die Überlegungen umfassen Aussagen für Server, Kommunikationsinfrastrukturen und Benutzerarbeitsplätze und stellen die angestrebte Sicherheitsarchitektur und allfällige Variante mit ihren Auswirkungen auf

- minimale Ausfallzeit (Best Effort)
- maximale Ausfallzeit (garantiert)
- minimaler Datenverlust (Best Effort)
- maximaler Datenverlust (garantiert)

dar. Sie beinhalten zusätzlich Empfehlungen für grundlegende Entscheidungen, sowohl auf Seite der Informatik als auch auf Benutzerseite, z. B.

- Pikett-, Alarm- und Notfallorganisation
- Verschlüsselung von Informationen
- Ausweichlösungen
- geforderte Infrastruktur- und Hardware-Redundanzen

Bewältigte Ausnahmesituationen

Ausnahmesituationen treten meist ohne Vorwarnung und ohne Berücksichtigung einer angenommenen Wahrscheinlichkeit ein. Bei ihrer Bewältigung spielen die Umsetzung der oben dargestellten Massnahmen und Entscheidungen eine wichtige Rolle.

Je umfassender die Schutzbedarfsdiskussion geführt, je genauer der Sicherheitszustand analysiert und je adäquater die Sicherheitsarchitektur realisiert wurden, umso rascher und besser kann die Ausnahmesituation bewältigt werden, sodass der Normalzustand der Informationsgesellschaft wieder erreicht ist. ●

Network Enabled Operations – vernetzte Operationsführung; nicht nur eine technologische Herausforderung

Der Autor befasst sich im nachfolgenden Artikel mit den Grundsätzen der vernetzten Operationsführung und den der Konzeption zu Grunde liegenden technologischen, strukturellen und am Rande auch gesellschaftlichen Rahmenaspekten. Er zeigt dabei internationale Trends auf und illustriert diese an Hand konkreter Beispiele ausländischer Streitkräfte.

Andreas Moschin *

Beginn einer neuen Ära

Das neue Millennium bedeutet auch für moderne Streitkräfte eine neue Ära. Diese Ära ist geprägt durch ein sich veränderndes strategisches Umfeld und eine rasante technologische Entwicklung. Die fortschreitende Globalisierung, die Vernetzung der Gesellschaften, das Aufbrechen traditioneller Strukturen sowie die verstärkte Bedeutung der Information als Wettbewerbsvorteil. Zusammen mit dem enormen Bevölkerungswachstum und den sozialen und wirtschaftlichen Folgen sind strategische Entwicklungen, denen sich auch die Schweiz nicht verschliessen kann. Nach der vergangenen Epoche der Bipolarität bleibt die Welt zwar nach wie vor geteilt, die Grenzen bewegen sich aber ständig. Somit verändern sich auch die Konflikte. Waren früher politische Ideologien die Ursache von Konflikten, so ist im neuen Jahrtausend eine Tendenz hin zum religions- oder kulturbasierten Konflikt erkennbar. Diese Art von Auseinandersetzung zeichnet sich neben anderen Merkmalen durch eine zeitliche Synchronisation des Konfliktes und der gewaltsamen Umsetzung (Terror) aus. Diese Konfliktformen führen zu neuen und grenzüberschreitenden Risiken, Bedrohungen und Gefahren. Die neue Multipolarität ist einhergehend mit einem Verlust an Souveränität einzelner Staaten, und es besteht in verschiedenen Regionen der Welt eine Tendenz zum Zerfall der staatlichen Ordnung. Die sicherheitspolitische Antwort auf diese Herausforderungen des Informationszeitalters liegt im Erkennen der gegenseitigen Abhängigkeiten der Gesellschaften und der globalen Wirtschaft und der Notwendigkeit der gemeinsamen Vernetzung.

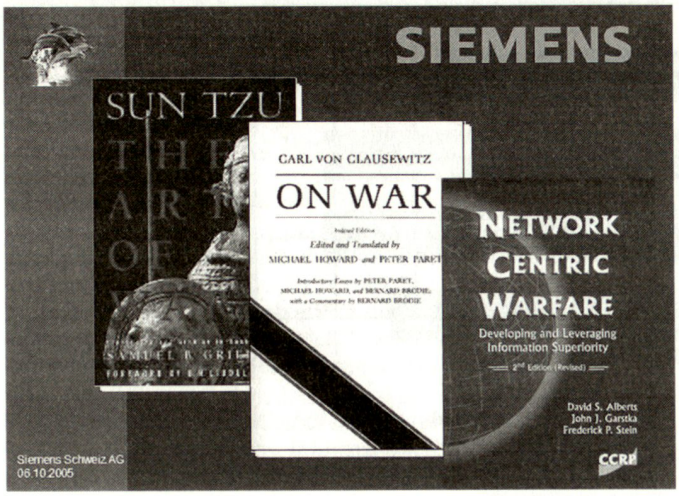
Die Wirtschaft hat den Nutzen der globalen Vernetzung längst erkannt. Sie setzt diese Erkenntnis auch um. Informationsmanagementsysteme ermöglichen die globale Verbreitung und Nutzung von Informationen. In multinationalen Unternehmen ist das «state of the art». In technologischer Hinsicht bringt der Übergang vom Industriezeitalter ins Informationszeitalter eine exponentielle Steigerung der Leistungsfähigkeit mit sich. Die zunehmende Verfügbarkeit und breite Anwendbarkeit der Informationstechnologie eröffnet bisher unbekannte Möglichkeiten zur Ausübung von gesellschaftlicher, industrieller, wirtschaftlicher, aber auch militärischer Macht. Im Gegensatz zu vergangenen Jahrzehnten ist heute jedoch nicht mehr der militär-industrielle Komplex die treibende Kraft bei der Entwicklung neuer Technologien, sondern die Industrie im zivilen Markt.

*Andreas Moschin, Oberstlt i Gst, Head of Sales Defense bei Siemens Schweiz AG, Civil and National Security.

Die veränderte Rolle der Streitkräfte

Als bewaffnete Instrumente der nationalen Sicherheitspolitik sind auch Streitkräfte dem Wandel im Sinne einer «Revolution of Military Affairs» unterzogen. Diese ist charakterisiert durch den raschen technologischen Fortschritt. In der Schweiz wie auch im Ausland findet zurzeit eine Transformation der Streitkräfte statt. Sie führt zu grundlegenden strukturellen und doktrinalen Anpassungen. Vor allem Streitkräfte der «grossen» Nationen übernehmen neue Rollen:Verstärkt werden Truppen als Mittel zur politischen Konfliktbeeinflussung benutzt, was auch eine glaubwürdige Projektion der militärischen Macht über weite Distanzen bedingt. Die Zunahme der friedensfördernden Einsätze, die hohe Bedeutung des Schutzes der eigenen Truppen, die Vermeidung von Kollateralschäden und die gestiegene Bedeutung der Medien sind klare Rahmenbedingungen für die Transformation der Streitkräfte. Da die meisten Einsätze in Zukunft im Rahmen von Koalitionen durchgeführt werden, ist dem Aspekt der Interoperabilität grosses Gewicht beizumessen. Sie beschränkt sich allerdings nicht nur auf die Aspekte teilstreitkraftübergreifend *(joint)* und multinational *(combined)*, sondern muss in gleichem Masse zur organisationsübergreifenden Zusammenarbeit ziviler und militärischer Organisationen *(interagency)* werden. Neben der Dateninteroperabilität sind auch die Faktoren syntaktische-, semantische und pragmatische Interoperabilität zu berücksichtigen. Nur mit dieser Berücksichtigung kann der ganze «Workflow» von der Erfassung über die Darstellung des streitkäftegemeinsamen Lagebildes bis hin zum Endbenutzer umgesetzt werden.

Damit den genannten Herausforderungen wirksam begegnet werden kann, müssen neue Konzepte wie zum Beispiel dasjenige der *Network Enabled Capabilities (vernetzte Operationsführung)* umgesetzt werden. Streitkräfte müssen die Fähigkeit erhalten, «Intelligence» zu akquirieren und die Informationen der Aufklärung, Erkundung und Zielakquirierung an alle Nutzer über sämtliche Kommandostufen hinweg zugriffsfähig zu machen. Zu diesem Zweck muss die Netzwerkfähigkeit bei allen Truppen und Systemen vorhanden sein. Eine der grössten Herausforderungen dabei wird die Integration der bestehenden Teilsysteme in ein Gesamtsystem sein. Diese Integration sollte bereits getätigte Investitionen berücksichtigen. Erfolgreich eingeführte Systeme, wie zum Beispiel das Führungsinformationssystem der Schweizer Luftwaffe, können als Beispiel dienen. Die grösste Herausforderung bietet aber die Ausrichtung der Köpfe auf die neue Konzeption. Oberst i G Tjarck Rössler vom Zentrum für Transformation der Bundeswehr meinte dazu treffend: *«Der längste und schwierigste Weg zur Umsetzung von vernetzter Operationsführung ist der zwischen den beiden Ohren!»*[1]



Die drei wichtigsten Grundlagenwerke der Operationsführung. Grafik Oberst i G Rössler, Anlass am 22. Juni 2005 «Vernetzte Sicherheit und Netcentric Operations» in Bern

Die Grundlagen von Netcentric Operations

Konzeption

Wegweisend bezüglich der Konzeption ist die US-Publikation «Network Centric Warfare» aus dem Jahr 1999.[2] Sie kann neben «The Art Of War»[3] von Sun Tzu und dem Werk «Vom Kriege» des grossen Clausewitz[4] als drittes Standardwerk der Strategieentwicklung im militärischen Umfeld gewertet werden. Network-Centric Warfare (NCW) ist eine Theorie der Kriegführung im Informationszeitalter. Diese Theorie ist die militärstrategische Antwort auf die Herausforderungen des Informationszeitalters. NCW ist die Kombination von Strategie, Taktik, Technik, Prozessen mit dem Ziel, einer Streitkraft einen entscheidenden Vorsprung zu ermöglichen.

Durch umfassende Vernetzung von Aufklärung, Führung und Waffenwirkung wird ein gemeinsames Lagebild geschaffen.

Durch umfassende Vernetzung von Aufklärung, Führung und Waffenwirkung wird ein gemeinsames Lagebild geschaffen. Es ermöglicht ein gemeinsames Lageverständnis. Ziel ist die Informationsüberlegenheit im Sinne der Fähigkeit, vor dem Gegner zu erkennen, zu entscheiden und zu handeln. Dies ermöglicht den Kommandanten eine effizientere Umsetzung ihrer Entschlüsse. Gleichzeitig bietet NCW einen kontinuierlichen, qualitativ hochwertigen Informationsfluss. Er ermöglicht Einsatzkräften, sich jederzeit wieder auf das definierte Operationsziel auszurichten (Selbstsynchronisation). Die wesentlichen Elemente des Verbundes bilden Sensoren, Entscheidungsträger (Führung) und Effektoren. Die umfassende Vernetzung dieser Elemente führt zur netzwerkzentrierten Führungsfähigkeit.

Ein zentrales Element der NCW ist die Abkehr von der «plattformzentrierten» Kriegführung. Früher agierten auf dem Gefechtsfeld luft-, boden- und seegestützte Streitkräfte und ihre Waffenplattformen (shooters) unabhängig, ja teilweise sogar in Konkurrenz zueinander. Auf einer Plattform wurden alle notwendigen Sensoren, Entscheidungsträger und Effektoren vereint. Die Plattformen waren in sich zwar optimiert, konnten jedoch kaum Information austauschen oder gar zusammenarbeiten. In den letzten Jahren wurden zunehmend integrierte Systeme entwickelt. Einzelsysteme wurden so konzipiert, dass sie im Verbund (Stichwort: Kampf der verbundenen Waffen) ihre spezifische Aufgabe erfüllen können. Die Trennung in der plattformzentrierten Kriegführung wird mit NCW überwunden. Die netzwerkzentrierte Führung treibt die Integration aller Systeme einen entscheidenden Schritt weiter. Die grundsätzliche Idee ist es, dass alle Einzelsysteme über ein gemeinsames Netz Informationen austauschen können. Allen Akteuren (Sensoren, Führung, Entscheidungsträger) wird ermöglicht, die Fähigkeiten der anderen je nach Bedarf und Berechtigung einzusetzen. Dieser Ansatz fördert Synergien und erhöht die Flexibilität. Der kooperative Einsatz von Sensor- und Kampfeinheiten wird als so genannte *Cooperativ Engagement Capability* (CEC) bezeichnet.

[1] Anlässlich seiner Rede am Anlass «Vernetzte Sicherheit und Netcentric Operations» der Siemens Schweiz AG vom 22. Juni 2005 in der Kaserne Bern, nachfolgend: Anlass Netcentric Operations.

[2] Alberts, David S., Garstka, John J. Stein, Frederick P.: Network Centric Warfare, Washington DC, 2000.

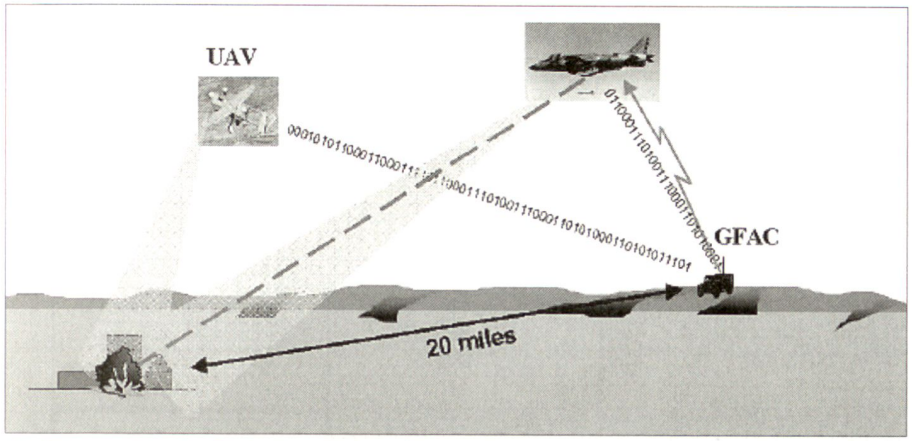
[3] Lionel Giles, «Sun Tzu die Kunst des Krieges.» Droemersche Verlagsanstalt, 1988.

[4] Clausewitz Carl. «Vom Kriege.» Reinbek bei Hamburg, 1963.

[5] Close Air Support ist die Luftnahunterstützung der Luftwaffe zu Gunsten der Erdkampfformationen.

[6] Quelle: Schäfer, Operationsführung.

[7] US DoD, Office of Force Transformation. «The Implementation of Network-Centric Warfare.» 2005, Washington DC.



Einführung NetOpFü, Luftwaffenamt D.

Beispiel: Ein unbemanntes Aufklärungsflugzeug (UAV) übermittelt aktuelle Bilder des Operationsgebietes an einen Ground Forward Air Controller (GFAC). Er identifiziert als potenzielles Ziel ein bestimmtes Haus in einer Stadt. Die Bekämpfung soll von einem bereits in der Luft befindlichen Kampfflugzeug übernommen werden. Ein erster Versuch scheitert, weil das Kampfflugzeug nur per Sprache mit dem GFAC kommunizieren konnte und so nicht in der Lage war, das Ziel positiv zu identifizieren. Erst mit einem anderen Kampfflugzeug, das über die technische Fähigkeit verfügt, sein Bild zeitgleich dem GFAC zu übermitteln, gelingt eine genaue Zielzuweisung. So kann sichergestellt werden, dass alle Beteiligten von demselben Ziel sprechen. Im zweiten Fall vergingen von der Auffassung bis zur Bekämpfung nicht einmal neun Minuten.[6]

Das Herz des NCW besteht in der Möglichkeit, auf dem Gefechtsfeld allen Kämpfern oder Einsatzkräften die benötigten Informationen zum erforderlichen Zeitpunkt bereitzustellen. Anstelle der Informationen durch C2-Stäbe *(Nachrichtenstäbe)* gefüttert zu bekommen, müssen diese allerdings durch die Einsatzkräfte selber für ihre Zwecke massgeschneidert aufbereitet werden können.

Ein weiterer Begriff ist *«Smart Push»*. Smart Push ist zum Beispiel die Möglichkeit, dass auf dem *Kriegsschauplatz* irgendein Kämpfer, ohne die Operationsführung oder Frequenz der Luftwaffe zu kennen, zeitgerechten und zielgenauen *«Close Air Support»*[5] anfordern kann.

Lehren und Prinzipien von Network-Centric Warfare (Tenets and Principles)[7]

Das Office of Force Transformation des US-Verteidigungsdepartementes beschreibt vier Lehren und neun Prinzipien, die als Grundlage für die NCW gelten. Gemeinsam ergeben diese Lehren und Prinzipien den Kern von NCW als bahnbrechende Theorie für die Krieg- (Operations-) führung im Informationszeitalter.

Governing Principles of a Network-Centric Force

- Fight first for information superiority
- Access to information: shared awareness
- Speed of command and decision making
- Self-synchronization
- Dispersed forces
- Demassification
- Deep sensor roach
- Alter initial conditions at higher rates of change
- Compressed operations and levels of war

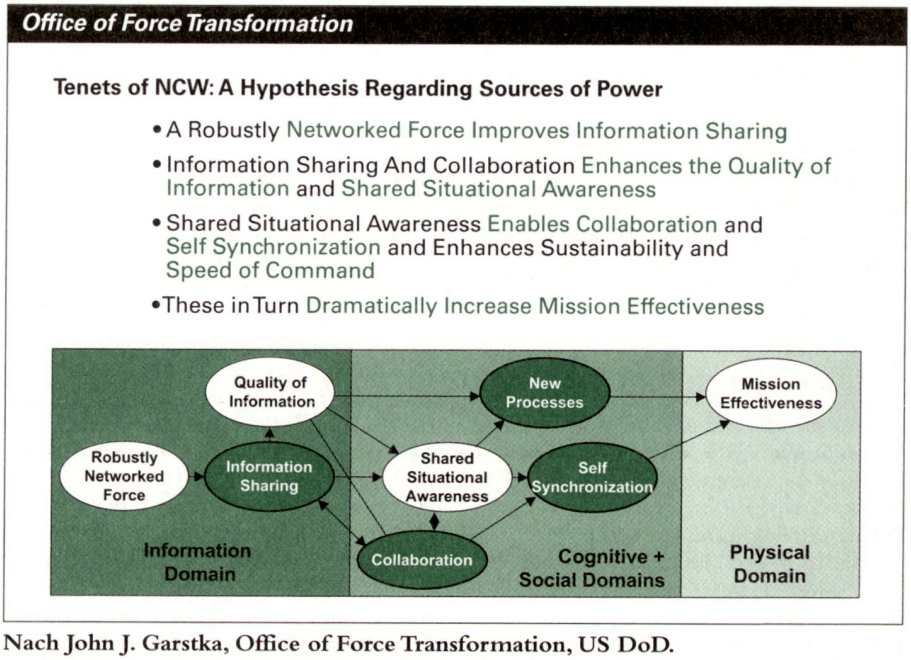
Office of Force Transformation, US DoD

US Joint Chiefs of Staff, Joint Vision 2020

In den US-Streitkräften findet zurzeit die Umsetzung der Joint Vision 2020 statt. Diese Vision ist auf die Bildung der Joint Force 2020 fokussiert. Das Ziel der Joint Vision 2020 ist, eine Streitkraft zu bilden, die im gesamten Spektrum der militärischen Operation dominieren kann. Primär in den Bereichen Schnelligkeit, Letalität und Präzision sollen neue Massstäbe geschaffen werden. Die Hauptaspekte der zur Umsetzung der Joint Vision 2020 notwendigen Force Transformation betreffen schwergewichtig die Landstreitkräfte (Army). Im Dokument Joint Vision 2020 werden vier operative Grundsätze angeführt, die basierend auf der Informationsüberlegenheit den Weg zur so genannten «Full Spectrum Dominance» ebnen sollen. Diese vier Grundsätze sollen in der Folge kurz definiert werden:

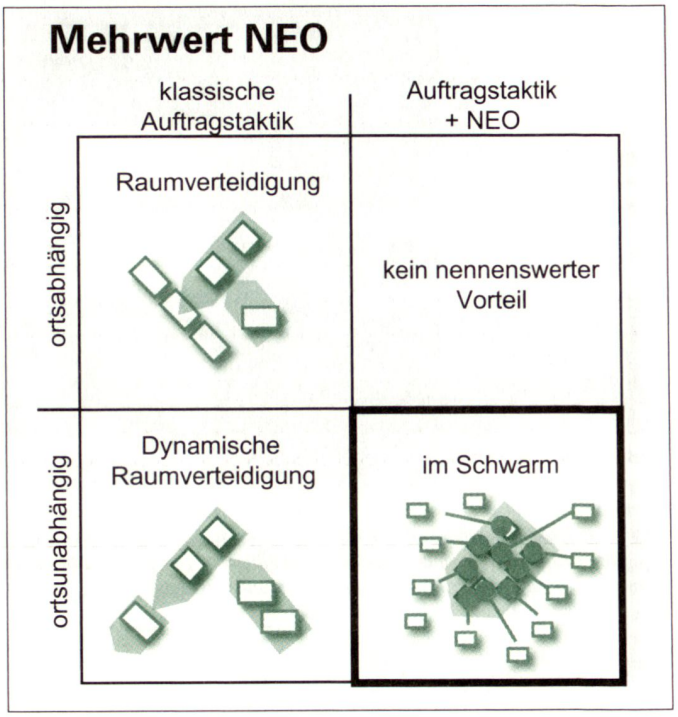
- **«Dominant Manouver»** (überlegene Bewegung): durch überlegene Geschwindigkeit und Beweglichkeit sowie der Fähigkeit, das Feuer von weit dezentralisierten Effektoren (land-, luft-, seegestützt, auch special operations forces) zu konzentrieren bzw. zu skalieren, wird Überlegenheit im Manöver erreicht.
- **«Precision Engagement»** (gezielter Kräfteeinsatz): die Fähigkeit von Joint Forces, Ziele und Objekte zu lokalisieren, zu erkennen, auszuwählen und das richtige System zum Einsatz zu bringen. Erkannte Ziele werden mittels kooperativem Einsatz der Streitkräfte präzise bekämpft.
- **«Focused Logistics»** (einsatzgesteuerte Logistik): durch die Vernetzung aller Truppenteile können die zur Verfügung stehenden bzw. benötigten Ressourcen und Dienstleistungen effizient und rechtzeitig dem richtigen Nutzer zugeführt werden.
- **«Full Dimensional Protection»** (umfassender Schutz): mittels Informationsüberlegenheit können die gegnerischen Aktivitäten frühzeitig erkannt und unterbunden werden. Weiter werden alle Massnahmen getroffen, um geplante Operationen im Rahmen einer vertretbaren Gefährdung *(eines kalkulierten Risikos?)* durchführen zu können.

Die US-Landstreitkräfte der Zukunft sollen durch den Einsatz der Network-Centric Capabilities befähigt werden, folgendes Prinzip anzuwenden: «See first, Understand first, Act first, Finish decisively». Weiter sollen ihnen durch die zeitverzugslose Vernetzung drei fundamentale Fähigkeiten eröffnet werden:



Nach John J. Garstka, Office of Force Transformation, US DoD.

Die US-Landstreitkräfte der Zukunft sollen durch den Einsatz der Network-Centric Capabilities befähigt werden, folgendes Prinzip anzuwenden: «See first, Understand first, Act first, Finish decisively».



Grafik nach Divisionär Jakob Baumann, Chef Planungsstab der Armee, anlässlich seines Referates im Rahmen der Tagung «Vernetzte Sicherheit und Netcentric Operations» vom 22. Juni 2005.

- Zugang aller Mitglieder (auch Einzelplattformen) des Netzwerks zu allen vernetzten Ressourcen über etablierte Sicherheitsprotokolle. Diese Ressourcen beinhalten das Teilen der Lagebilder, sodass jeder sofort den Überblick über das gesamte «Battle Theater» gewinnen kann.
- Vernetzte Kommandanten können ihre Entscheidungen auf besseren Grundlagen treffen; durch das Teilen der Information sind die Kommandanten aller Stufen in der Lage, die Gesamtzusammenhänge viel besser und schneller zu verstehen und somit gesamtheitlicher zu denken.
- Eine NCW-Streitkraft kann ihre Mittel effektiver und effizienter synchronisieren. Das macht die Operation in den Bereichen Geschwindigkeit, Reaktionsfähigkeit und Flexibilität wesentlich effizienter.[8]

Informationsüberlegenheit

Jeder militärische Führer definiert die Informationsüberlegenheit als Schlüsselelement auf dem Weg zum Erfolg. Die laufende «Revolution in Military Affairs» bringt nicht nur einen quantitativen, sondern auch einen qualitativen Wechsel im Bereich der Information. Er wird in Zukunft Auswirkungen auf die Operationsführung haben. Joint Vision 2020 definiert Information wie folgt: *«– the capability to collect, process, and disseminate an uninterrupted flow of informations while exploiting or denying an adversary's ability to do the same. Information superiority is achieved in a noncombat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives».*[9]

Die Informationsüberlegenheit dient allerdings nicht dem Selbstzweck. Sie kann einer Joint Task Force den entscheidenden Vorteil verschaffen. Das gelingt aber nur, wenn Informationen in Wissens- und Entscheidungskompetenz überführt werden.

Wechsel von Push- zu Post & Pull-Informationsmanagement

Die Idee der vernetzten Operationsführung ist es nicht, dass grundsätzlich jeder mit jedem ständig Daten austauscht. Ziel ist es vielmehr, dass jeder prinzipiell mit jedem vernetzt ist und somit eine sich dynamisch im Laufe der Operation entwickelnde Kommunikation erreicht wird. Dabei geht es darum, die Informationen in der richtigen Qualität zur richtigen Zeit am richtigen Ort verfügbar zu haben. Hier drängt sich ein Paradigmenwechsel in der in Streitkräften üblichen Informationskultur auf. Die Zeiten, in denen unterstellte Kommandanten ungeduldig auf Informationen, Befehle oder Nachrichtenbulletins warten, werden vorbei sein. Die Verantwortung wird umgekehrt. Künftig wird nicht mehr der Besitzer der Informationen zuständig sein, dass die Informationen den richtigen Empfänger erreichen. Es wird vielmehr am Empfänger sein, zweckdienliche Informationen proaktiv abzurufen. Jeder weiss selbst am besten, was er wissen muss. Die Aufgabe der operativen Führung wird es sein, die Informationen ohne gezielten Empfänger zur Verfügung zu stellen (post), sodass jeder das abrufen kann, was er benötigt (pull).[10]

Künftig wird nicht mehr der Besitzer der Informationen zuständig sein, dass die Informationen den richtigen Empfänger erreichen. Es wird vielmehr am Empfänger sein, zweckdienliche Informationen proaktiv abzurufen.

Auftragstaktik und vernetzte Operationsführung

In der Führungs- und Stabsorganisation der Schweizer Armee wird die Auftragstaktik wie folgt definiert: *«Die Auftragstaktik ist ein Führungsverfahren, bei dem der Unterstellte ein Maximum an Handlungsfreiheit im Rahmen der Absicht des vorgesetzten Kommandanten erhält, um einen Auftrag zu erfüllen».*[11] Die Tatsache, dass die Grundlagen der vernetzten Operationsführung in den USA entwickelt wurden, lässt den Schluss zu, dass die Konzeption der vernetzten Operationsführung eher der in den dortigen Streitkräften üblichen Befehlstaktik nahe kommt. Bei genauem Hinsehen erkennt man, dass die vernetzte Operationsführung nur unter Anwendung der Auftragstaktik ihre volle Wirkung entfalten kann. In Streitkräften, die dieses Führungskonzept anwenden, ist das Verantwortungsbewusstsein bis in viel tiefere Ebenen des Systems verwurzelt. Im Idealfall sollte diese Grundfähigkeit in Kombination mit vernetzter Operationsführung zum folgenden Ablauf führen: Der Kommandant der operativen Stufe formuliert seine Absicht mit Schwergewichten und Zielen. Diese wird durch die nachfolgenden Ebenen in Eigenverantwortung, basierend auf dem ständig verfügbaren gemeinsamen Lagebild, umgesetzt. Die höhere Führungsebene beschränkt sich auf das Controlling und greift nur noch korrigierend ein, beispielsweise im Falle eklatanter Zielabweichungen.

Dieses Führungsprinzip ist in der Wirtschaft unter dem Begriff «Management by Exception» (MbE) schon länger verbreitet.

[8] Army Science and Technology for Homeland Security Report 2 C4ISR, National Academy of Sciences, Washington DC, 2004.

[9] Joint Vision 2020, US Joint Chiefs of Staff, Washington DC, 2004.

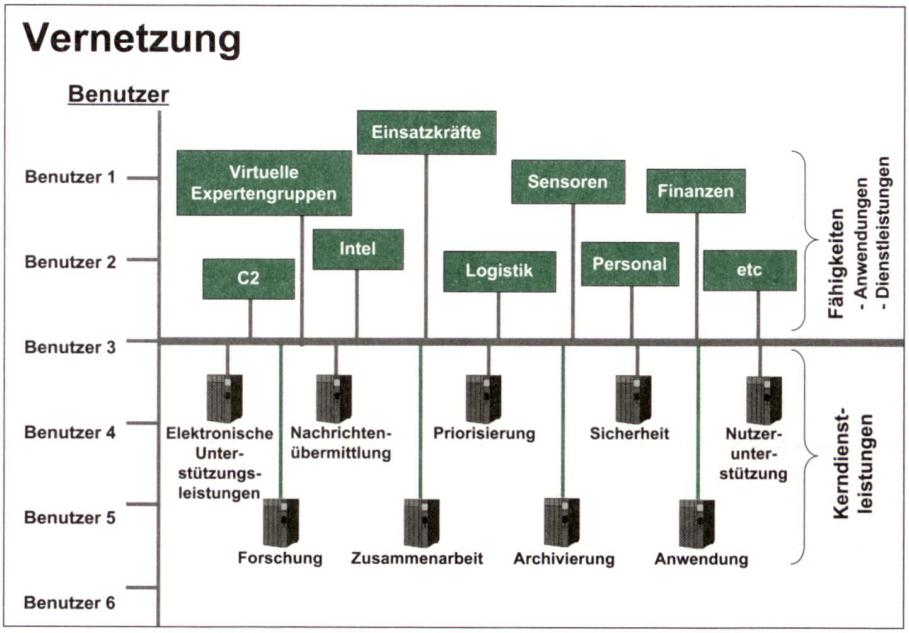
[10] Sebastian Schäfer. «Vernetzte Operationsführung».

[11] Führungs- und Stabsorganisation, Regl. Chef der Armee, gültig ab 01.01.04, Seite 5.

[12] Div Jakob Baumann, Chef Planungsstab der Armee, am Anlass Netcentric Operations.

[13] http://www.dhs.gov/dhspublic/

MbE ist eine Verschärfung des Management by Delegation. Im Sinne des MbE findet Führung nur auf Anforderung der unteren Ebene bei Situationen statt, die eine Eskalation auf die nächste Führungsebene erfordern. Häufig wird das System durch Führung mittels Zielvereinbarung ergänzt. Voraussetzung dafür ist die Delegation der erforderlichen Kompetenzen an jede Organisationseinheit und an jeden Mitarbeiter. Sie ermöglicht, Aufgaben ohne Eingreifen der nächsten Führungsebene zu lösen. Anschaulich dargestellt wird der Mehrwert der Kombination Auftragstaktik – Network Enabled Informations in der nachstehenden Grafik von Divisionär Jakob Baumann.[12]



Grafik nach Oberst i G Rössler.

Informations Technology (IT)

Informations Technology ist die technologische Grundlage der Netzwerkzentrierten Führung. Das Netz ist die physikalische Grundvoraussetzung für jede Network enabled Operation. Es ist von vitalem Interesse, den möglichst zeitverzugslosen Austausch der erforderlichen Informationen sicherzustellen. Nur so kann die Basis für ein gemeinsames umfassendes Lagebild, common relevant operational picture (CROP), generiert werden. Der Weg zu diesem CROP muss schrittweise angegangen werden. Es gilt zuerst, die Lagebilder der taktischen und der höheren taktischen Ebenen zu etablieren und rollenspezifisch zu verdichten bzw. zu justieren. Im nächsten Schritt müssen auch die Informationen der Logistik bzw. des Führungsgrundgebietes 2 und weiterer Gebiete in der entsprechenden Verdichtung integriert werden.

Netcentric Operations und Homeland Security

Im Zusammenhang mit den eingangs veränderten sicherheitspolitischen Rahmenbedingungen wird das enge Zusammenspiel aller für die Sicherheit zuständigen Organisationen unumgänglich. Unter dem Zeichen der Anschläge des 11. September 2001 wurde zu Beginn des Jahres 2002 in den USA der so genannte Homeland Security Act verabschiedet. Darauf basierend wurde das Departement of Homeland Security gebildet,[13] welches in seiner Strategie das folgende Ziel ausweist: *Ensure national and international policy, law enforcement and other actions to prepare for and prevent terrorism are coordinated. Increasing and coordinating information sharing between law enforcement, intelligence and military organizations will improve our ability to counterterrorists everywhere.* Dem Teilen der Information zwischen den verschiedenen Sicherheitsorganisationen wird somit ein grosses Gewicht beigemessen.

Jede Organisation, die im Bereich der nationalen oder inneren Sicherheit tätig ist, sieht sich heute vor immer komplexere Aufgaben gestellt. Das Spektrum der Bedrohungen erweitert sich nicht nur und ist komplex geworden, sondern ändert sich auch ständig. Einer der Schlüssel für eine sichere Zukunft liegt im erfolgreichen Zusammenwirken der verschiedenen existierenden Sicherheitsorganisationen. Durch eine konsequente Berücksichtigung der Interessen und Anliegen der zivilen Partner im Sicherheitsverbund wird die Grundlage geschaffen, dass durch das Teilen von Informationen neue Wertschöpfungsquellen erschlossen werden können. Eine Wertschöpfung, die sich konkret messen lässt anhand von Faktoren wie Kosten, Funktionalität und Transparenz. Bei Militär und Blaulichtorganisationen kommen darüber hinaus die Faktoren Überlebensfähigkeit, Geschwindigkeit, Effizienz, zeitliche Synchronisation und Reaktionsfähigkeit hinzu.

> Das Spektrum der Bedrohungen erweitert sich nicht nur und ist komplex geworden, sondern ändert sich auch ständig.

In diesem Zusammenhang wird auch der Begriff der effektbasierenden Operationen häufig verwendet. Insbesondere bei Aktionen im eigenen Land ist das Ziel, eine raschmöglichste Stabilisierung der Lage zu erreichen. Die Vernichtung des Gegners steht auch in Konfliktszenarien nicht im Zentrum. Es geht vielmehr darum, den Fokus auf den gewünschten Effekt zu richten, der bestmöglich zur nachhaltigen Zielerreichung beiträgt. Danach richtet sich die Wahl der Mittel. Eine Rahmenbedingung ist dabei die möglichst gesamtheitliche Betrachtung, in der mögliche Auswirkungen auf allen relevanten Ebenen berücksichtigt werden (Politik, Militär, Wirtschaft, Industrie, Infrastruktur usw.).

So wie Netcentric Operations auf dem Gefechtsfeld die Wirkung als «force multiplier» entfaltet, kann das Konzept auch einen Mehrwert im Bereich der Homeland Security generieren. Es ist absehbar, dass einige der in Zukunft unter der Idee von Netcentric Operations entwickelten Fähigkeiten und Anwendungen zu teuer oder komplex sein werden, um bei zivilen Sicherheitsorganisationen eingesetzt zu werden. Mit Bestimmtheit wird es aber auch einige Technologieanwendungen geben die, im Sinne eines Sicherheitsnetzwerkes, auch für die Blaulichtorganisationen sehr nützlich sein können. Als Beispiel kann die Zugriffsmöglichkeit auf das erwähnte Common relevant operational picture (CROP) sein.

Die Netzwerkzentrierte Operationsführung ist auf eine optimale Führung des Aktionsplanungs- und Aktionsführungsprozesses durch die Stäbe angewiesen. Neben organisatorischen, strukturellen und doktrinalen Voraussetzungen und des «command and control»-Mechanismus bleibt das Training der Stabsoffiziere, wie es die Schweizer Armee heute im Technisch Taktischen Trainingszentrum der Generalstabsschulen (TTZ mit Fhr Sim 95) in Kriens durchführt, ein zentraler Aspekt. Eine notwendige Ausrichtung auf die Zukunft ist allerdings die Planung und Umsetzung der nötigen Erweiterungen im Rahmen der Vernetzung der Simulatorenlandschaft zu einem «Joint Simulationssystem», unter Einbindung der Führungsinformationssysteme. ●

INFORMATION IMPERIALISM

Wissen ist Macht[1] – Wie steht es um den Schutz unseres Wissens?

Im vorliegenden Artikel befasst sich der Autor mit der Frage, wie offen unsere Daten in jeglicher Telekommunikation übermittelt werden, und stellt anschaulich dar, welche Systeme verdeckt und weltweit daran arbeiten, Zugang zu diesen Daten zu erhalten, um ihren Betreibern einen Informationsvorsprung zu verschaffen. Wissen ist Macht – Macht ist aber auch Geld wert. Es geht also nicht nur um militärische Macht, sondern auch um wirtschaftliche. Im Schlussteil zeigt der Autor mögliche Schutzmassnahmen auf.

Jörg A. Bischof *

Ausgangslage

Bis in die 80er- und 90er-Jahre des letzten Jahrhunderts lag der Wert eines Unternehmens hauptsächlich im Forschungs-, Entwicklungs-, Produktionswissen, im Potenzial der Infrastruktur und in den verfügbaren Kapazitäten begründet. Informationen wurden vor allem lokal benötigt, gelagert und ausgetauscht. Wenig bis nichts wurde elektronisch übermittelt. Der Austausch von Informationen erfolgte in der Regel per Briefverkehr, später auf postversandten elektronischen Datenträgern allenfalls manuell oder per Analog-Fax oder Telex. Das Telefon wurde nur zur Sprachübertragung eingesetzt und – bedingt durch die hohen Kosten – um das operative Geschäft zu steuern, aber praktisch nie, um Schlüsselwissen zu übermitteln. Telefon- und Videokonferenzen waren seltene Ausnahmen und wurden hauptsächlich zur Steuerung operativer Aufgaben eingesetzt.

Seit der Digitalisierung der Sprache fällt die Unterscheidung in Sprache und Daten weg.[2] Die Informatiklösungen von Unternehmen und Organisationen sind von Beginn weg uneinheitlich gewachsen. Selbst innerhalb von Organisationen sind Verfahrenslandschaften verschieden, das heisst

> Seit der Digitalisierung der Sprache fällt die Unterscheidung in Sprache und Daten weg.

meist unter Anwendung verschiedener Softwaresprachen und Protokollen, insgesamt ohne ein Gesamtkonzept. So verfügten beispielsweise Entwicklungs-, Finanz-, Verkaufsabteilungen derselben Organisation über unkompatible Softwareapplikationen. Komplexe Schnittstellen wurden jedoch rasch notwendig, um bereichsübergreifend arbeiten zu können. Das führte zu Sicherheitslücken, die allmählich erkannt und so gut wie möglich behoben wurden.

Die Entwicklung der letzten zehn Jahre hat dazu geführt, dass der Wert einer Organisation sich heute viel mehr über das elektronisch gespeicherte und schnell verfügbare Wissen definiert. Die meisten Organisationen haben sich aus einem abgeschotteten Inseldasein mit tiefer Wertschöpfungskette in vernetzte Firmengruppen gewandelt, die exorbitante Mengen an Daten national, kontinental und interkontinental austauschen.

Betrachtet man den Informationsfaktor, so ist erkennbar, dass Inhalte und Daten den Grossteil der schützenswerten Information ausmachen *(Abbildung 1)*. Diese Inhalte und Daten werden heute über bestehende Netzwerke ausgetauscht. Aber nur ein kleiner Teil dieser Daten ist zum Beispiel mittels Chiffrierung genügend vor fremdem Zugriff gesichert. Der Absender von Daten weiss nur in den wenigsten Fällen, über welche Übertragungsmedien die Datenübertragung erfolgt. Breitbandige Punkt-Punkt-Leitungen sind zwar verfügbar, aber sehr teuer. Dazu kommt, dass in den wenigsten Fällen die gesamte Leitungslänge überwacht werden kann.

> Inhalte und Daten werden heute über bestehende Netzwerke ausgetauscht. Aber nur ein kleiner Teil dieser Daten ist zum Beispiel mittels Chiffrierung genügend vor fremdem Zugriff gesichert.

Die Entwicklung hin zur Mobilität hat in den letzten Jahren in ungeahnte Dimensionen geführt. Hauptsächlich hat der Mobilfunk für die Sprache im Sinne digitaler Daten eklatant zugenommen und verdrängt je länger je mehr den Festnetzverkehr. Dies ist hinsichtlich der Datensicherheit relevant, weil der Mobilfunk den Übermittlungsinhalt über zwei verschiedene Medien transportiert: zunächst wie ein Funkgerät bis zum nächsten Sende-, Empfangsmasten durch die Luft; vom Masten an werden die Daten per Draht, Glasfaser oder Richtstrahl weiterübermittelt. Mit höheren Bandbreiten, neuen Standards und Technologien wie UMTS und WLAN haben sich die frei abgestrahlten Datenmengen drastisch vervielfacht. Schützenswerte Daten werden nun ausserhalb drahtgebundener Netze durch die Luft zu Basisstationen übertragen, entweder in geschützten oder in ungeschützten Netzwerken.

Die wachsende Anzahl an entscheidrelevanten Informations- und Datenmengen sind für die Empfänger nur noch gezielt und zeitgerecht verfüg- und brauchbar, wenn Führungssysteme verwendet werden. In zivilen Anwendungen werden Führungssysteme mit Hilfe von Softwarelösungen verwendet. Diese Software ist aber im Vergleich zu militärischen Führungssystemen wenig komplex. Sie generieren und integrieren zwar viele Informationen, kennen aber weder komplexe Interpretationshilfen wie Lagebeurteilung und Entscheidungsvorschläge noch verfügen sie zur Führung von Operationen über eine *real-time-world*. Im zivilen Umfeld kommen solche Führungssysteme nur in internen und drahtgebundenen Netzwer-

[1] Sir Francis Bacon (1561–1626), aus: Novum Organum, 1620.

[2] Nachfolgend wird nicht zwischen Daten und Sprache unterschieden.

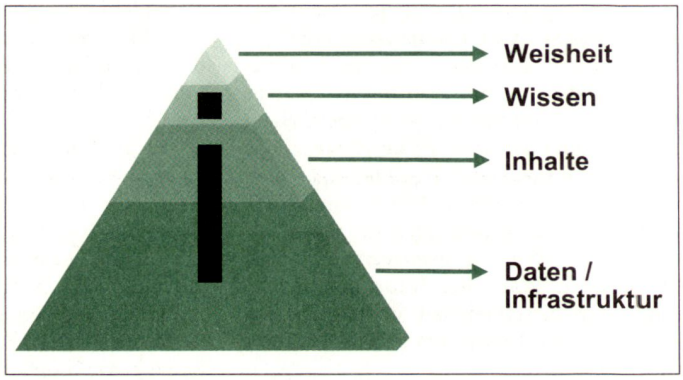


Abbildung 1: Information und ihre Faktoren.

*Jörg A. Bischof, CEO der GOFORIT Management Services, 6300 Zug.

ken zum Einsatz und kennen keine mobilen Elemente. Militärische Führungssysteme, vor allem in multinationalen und/oder interkontinentalen Operationen, verfügen über mobile Elemente und Übertragungsstrecken der verschiedensten Art.

Nebst militärischen Anwendern verfügen vor allem Finanzdienstleister über die nötige Sensibilität und notabene auch über die nötigen Budgets, um ihre Systeme und Netzwerke so wirkungsvoll wie möglich zu schützen.

Nebst militärischen Anwendern verfügen vor allem Finanzdienstleister über die nötige Sensibilität und notabene auch über die nötigen Budgets, um ihre Systeme und Netzwerke so wirkungsvoll wie möglich zu schützen.

Gefährdet sind konkurrierende Industrieunternehmen mit hohem informationsbasiertem *Know-how,* aber geringen Mitteln oder Sensibilität, was die Datensicherheit anbelangt. Dazu kommt, dass sie aus Kostengründen oft Leistungen, die für ihr Kerngeschäft von essenzieller Bedeutung sind, durch organisationsfremde Anbieter erledigen lassen *(outsourcing).* Dabei werden weder die Sicherheit der Übertragungswege noch die Sicherheit des Anbieters entsprechend beachtet. Ausgesprochen gefährdet sind Universitäten und Forschungsinstitute. Sie stehen naturgemäss bezüglich ihrer Forschungsresultate, ihres Wissens, ihrer Kapazitäten oder ihres *Know-how* vor dem Dilemma «Geheimhaltung versus Öffentlichkeit». Zudem haben sie Schwierigkeiten, wenn es um die wirkungsvolle Durchsetzung ihrer Sicherheitsvorschriften geht: Die am Institut Tätigen sind grösstenteils nicht per Arbeitsverträge gebunden, wie in anderen Organisationen, sondern temporär immatrikulierte Studenten oder Angestellte.

Information wird immer mehr auch zur zeitlich beschränkt gültigen und schützenswerten Momentinformation. Es gilt, sie nicht nur umfangmässig zu handhaben, sondern auch bezüglich ihres Wertes zum Schutze zu klassifizieren. Und weil Information zur Momentinformation geworden ist, muss sie häufig lediglich für einen bestimmten Zeitraum klassifiziert werden, das heisst, der Inhalt ist nach kurzer Zeit nicht mehr schützenswert. Aus diesem Grund müssen Aufwand und Ertrag bezüglich eines möglichen Schadens in angemessenem Verhältnis stehen. Der Begriff *end of security* (EoS) definiert den Zeitpunkt, nach dem der Schutzaufwand gemessen am Informationswert unverhältnismässig wird.

Bekannte Bedrohungsformen

Unternehmen und Organisationen sind mittlerweile zumeist gegen das unstrukturierte Vorgehen von so genannten Hackern und Cyberhooligans mehr oder weniger gewappnet. Demgegenüber gehen Cyberterroristen oder staatliche Akteure weit strukturierter vor. Eine ernst zu nehmende Bedrohung (und wenig ernst genommene) stellen so genannte Insider dar. Das können frustrierte und demotivierte Mitarbeiter sein oder solche, die sich in den Sold anderer stellen (Konkurrenz, Spionage). Untersuchungen belegen, dass der Schaden durch Insider wesentlich höher ist als derjenige durch externe Akteure. Die gleichen Untersuchungen zeigen auch, dass in mehr als einem Drittel der Fälle die Verursacher nie ermittelt werden konnten.

Eine ernst zu nehmende Bedrohung (und wenig ernst genommene) stellen so genannte Insider dar. Das können frustrierte und demotivierte Mitarbeiter sein oder solche, die sich in den Sold anderer stellen.

Die andere Bedrohung

Der ehemalige amerikanische Präsident Bill Clinton hat als Erster wiederholt den Begriff *INFORMATION IMPERIALISM* verwendet. Er bezeichnete damit den fehlenden Informationsfluss zwischen den westlichen und den afrikanischen Staaten. Das sei, so Clinton, entscheidender Vorteil der *more developed countries* gegenüber den *lesser developed*. Clinton spielte mit dem Begriff allerdings auch auf die diesbezügliche Überlegenheit der USA an. Wie meinte er das? – Die USA sind der übrigen Welt[3] in vielen Sachen immer einen Schritt voraus. Seit dem Zweiten Weltkrieg sind Innovationen in Forschung und Technik mehrheitlich von den USA ausgegangen. Zu diesen Bereichen gehört auch der Vorsprung in der Informationstechnologie. Der damit implizierte Informationsvorsprung wird beispielsweise dazu genutzt, im Ringen um Grossaufträge, sei es bei der Beschaffung von Rüstungs- oder zivilen Gütern, die Nase vorn zu haben.

Den meisten Ländern der Europäischen Union (EU) und insbesondere deren Zentrale in Brüssel war bis zum Ende der 90er-Jahre des vorigen Jahrzehntes nicht bewusst, um was es ging. Dies obwohl zehn Jahre zuvor, im August 1988, der englische Journalist Duncan Campbell in der Zeitschrift *New Statesman* den Artikel *Somebody's listening*[4] veröffentlichte, der zumindest einige Fragen hätte aufwerfen müssen. Duncan beschrieb in seinem Artikel das Projekt P415: Ein globales elektronisches Überwachungssystem, im Investitionswert von Milliarden von US-Dollar. Weitere Artikel zum Thema folgten zwischen 1988 und 1998. Darin taucht auch erstmals der Begriff ECHELON auf. Die Fragen waren gestellt – wenige Reaktionen folgten.

Duncan beschrieb in seinem Artikel das Projekt P415: Ein globales elektronisches Überwachungssystem, im Investitionswert von Milliarden von US-Dollars. Weitere Artikel zum Thema folgten zwischen 1988 und 1998. Darin taucht auch erstmals der Begriff ECHELON auf.

Anfang 1998 veröffentlichte das Europäische Parlament ein Arbeitspapier des Autors Steve Wright zuhanden des Ausschusses *Scientific Technology Options Assessment* (STOA) unter dem Titel *An Appraisal Of Technologies of Political Control.*[5] Der Autor behauptete darin, dass alle E-Mails, Telefongespräche und Faxübermittlungen in Europa durch den amerikanischen Nachrichtendienst *National Security Agency* (NSA) routinemässig aufgezeichnet würden.[6] Das Arbeitspapier machte in Europa die bisher bloss vermutete Existenz eines umfassenden globalen Abhörsystems, genannt ECHELON, zum breiten Thema.

1998 liess sich der damalige EU-Kommissar Martin Bangemann zu Fragen bezüglich ECHELON verlauten, dass die EU nichts darüber wisse und auch nicht ausreichend Beweise für dessen Existenz vor-

[3] *rest of the world;* ein in den USA geprägter Begriff, der alle Länder ausserhalb der Vereinigten Staaten von Amerika bezeichnet.

[4] http://duncan.gn.apc.org/echelon-de.htm *«They've got it taped»* und http://duncan.gn.apc.org/stoa.htm

[5] http://www.europarl.eu.int/stoa/default_en.htm, http://www.europarl.eu.int/dg4/stoa/en/publi/publi.htm siehe auch: http://www.heise.de/tp/r4/artikel/6/6280/1.html#s1

[6] Kapitel 4.4, *National & International Communications Interceptions Networks*

lägen.[7] 1999 hat dann ausgerechnet ein Amerikaner, der republikanische Kongressabgeordnete Bob Barr, die Sache ins Rollen gebracht und vom Direktor der *Central Intelligence Agency* (CIA), Direktor der NSA und dem Generalstaatsanwalt innerhalb 60 Tagen einen Bericht verlangt. Darin sollte die Frage beantwortet werden, wie die Privatsphäre der amerikanischen Bürger gegenüber dem Projekt ECHELON geschützt werde.

1999 erschien ein zweiter STOA-Bericht: *(...) in order to find out more about this subject, STOA commissioned a five-part study of the 'development of surveillance technology and risk of abuse of economic information'. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particulary the mode of operation ECHELON (...)*

Dieser Bericht hat im Wesentlichen zur Erkenntnis geführt, dass das ursprünglich zur Überwachung der Aktivitäten der ehemaligen Ostblockstaaten konzipierte System ECHELON nun schwergewichtig zur Wirtschaftsspionage diene. Als Beweis wurden einige Grossaufträge angeführt, die Firmen wie Airbus und Thomsen CSF wegen ECHELON an amerikanische Konkurrenzfirmen verloren hätten. Als Resultat des zweiten STOA-Berichtes wurde über ECHELON im Europäischen Parlament debattiert. Frankreich und Belgien verfassten in der Folge eigene Berichte. Im Juli 2000 beschloss das Europäische Parlament, eine temporäre Arbeitsgruppe zum Thema *ECHELON Interception System* zu bilden.

Der Bericht kam zum Schluss *(...) that a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA agreement, is no longer in doubt.*

Anfang Juli 2001 verabschiedete die Arbeitsgruppe den Entwurf zu ihrem knapp 140 Seiten umfassenden ECHELON-Bericht. Der Bericht kam zum Schluss (...) *that a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA agreement, is no longer in doubt.* Das Europäische Parlament behandelte den Bericht Mitte Juli 2001.[8]

[7] http://cryptome.org/echelon-fi.htm#leprevost
[8] http://cryptome.org/echelon-ep-fin.htm

Was ist ECHELON?

Heute gilt als gesichert, dass im Jahre 1948, kurz nach Ende des Zweiten Weltkrieges, die Länder USA, Kanada, Grossbritannien, Australien und Neuseeland einen geheimen Vertrag abgeschlossen haben, der der Grundstein für das Projekt ECHELON war. Zweck des Vertrages war es, ein weltumspannendes System von Horchposten aufzubauen, um den gesamten internationalen elektronischen Verkehr und den grössten Teil des lokalen elektronischen Verkehrs in allen Ländern der Welt auszuhorchen. Die wichtigsten heutigen Standorte des Systems sind in Grossbritannien *(Morwenstow/Cornwall, Menwith Hill/Yorkshire)*, in der Bundesrepublik Deutschland *(Bad Aibling)*, in Australien *(Shoal Bay, Geraldton)* und Neuseeland *(Waihopai)*, in Kanada *(Leitrim)*, sowie in den USA *(Yakima Firing Centre/Washington State, Sugar Grove/West Virginia)*.

Zweck des Vertrages war es, ein weltumspannendes System von Horchposten aufzubauen, um den gesamten internationalen elektronischen Verkehr und den grössten Teil des lokalen elektronischen Verkehrs in allen Ländern der Welt auszuhorchen.

Alle diese Basen haben Rechner, die in der Lage sind, Telefongespräche (Mobil und Festnetz), E-Mails und Fax nach Suchbegriffen zu filtern. Die entscheidende Priorisierung der Suchbegriffe erfolgt auf nationaler Ebene. Alle fünf ECHELON-Mitglieder verfügen über eigene Suchwörterbücher. Werden Suchbegriffe durch ECHELON aufgefangen, wird zuerst eine Grobanalyse mit Hilfe einer Software durchgeführt, die Feinfilterung erfolgt danach durch Mitarbeiter. Um länderspezifische gesetzliche Grundlagen zu umgehen, ist es üblich, die Partnerorganisationen anzufragen, die Überwachungen selber durchzuführen. Der EU-Bericht listet Beispiele auf, wie die britische Regierung unter Margaret Thatcher ihr unbequeme englische Politiker durch die NSA und der amerikanische Präsident Ronald Reagan seinerseits unangenehme amerikanische Politiker durch das britische *Government Communication Headquarters* (GCHQ) abhorchen liessen. ECHELON beschäftigte zu dieser Zeit rund 15000 Mitarbeiter mit einem jährlichen Budget von rund 500 Millionen US-Dollar.

Neben den vielen Horchposten in den Äther, die sich in Form riesiger Antennenanlagen rund um den Globus erstrecken,

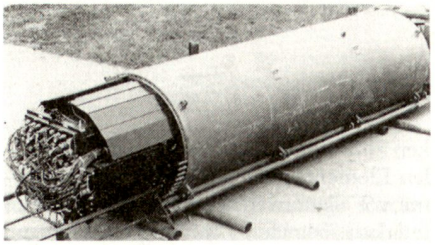


Abb. 2: Unterwasser-Abhorchkanister.

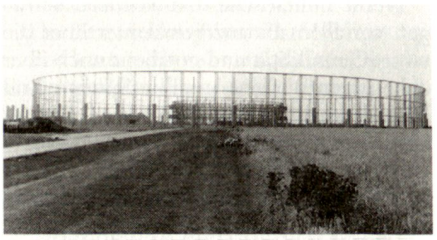


Abbildung 3: Horchposten in den Äther.

hat ECHELON ab 1950 systematisch auch sämtliche Unterwasser-Kommunikationskabel angezapft. Diese geheime Aktivität wurde erst publik, als die Russen in der Barentssee in den 80er- und 90er-Jahren einen Abhorchkanister bargen, der neben einem, unter Wasser verlegten, Telekommunikationskabel auf russischem Hoheitsgebiet lag. Sie stellten das *corpus delicti* kurzerhand in einem Moskauer Museum aus *(Abbildung 2,3)*. Bedingt durch die Länge der unterwasserverlegten Kupferkabel mussten Zwischenverstärker geschaltet werden. In der Umgebung dieser Zwischenverstärker waren die Signale am stärksten und somit der ideale Ort, um die auf induktiver Basis arbeitenden Abhorchkanister zu positionieren. Dies war allerdings nur dann nötig, wenn die Kopfstationen der Unterwasserverbindungen auf beiden Seiten der Ufer nicht direkt angezapft und somit ins ECHELON-System eingebunden werden konnten. Zufällig enden die meisten transatlantisch verlegten Kabel auch heute noch in *Cornwall*/Grossbritannien. Zufällig ist auf der Klippe bei *Sharpnose Point* die Anfang der Siebzigerjahre

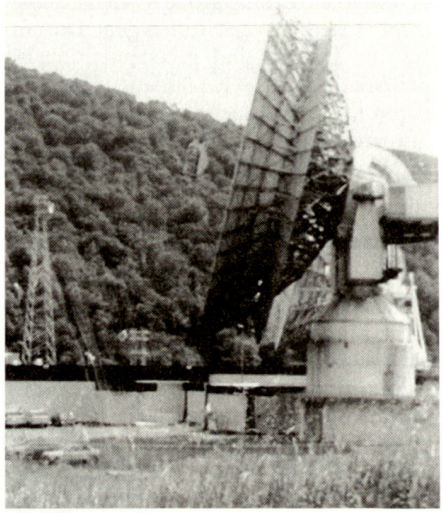


Abbildung 4a: Sharpnose Point, Morwenstow.

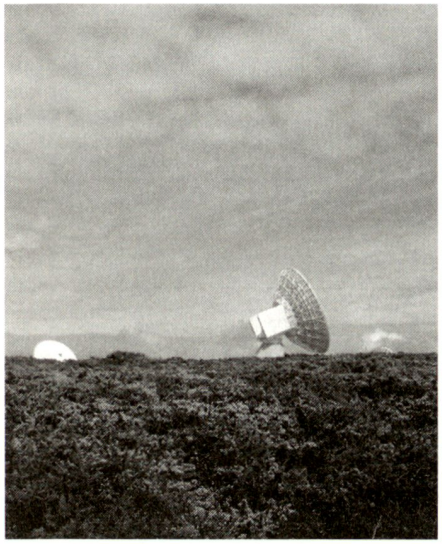


Abbildung 4b: Teilsystem zu ECHELON.

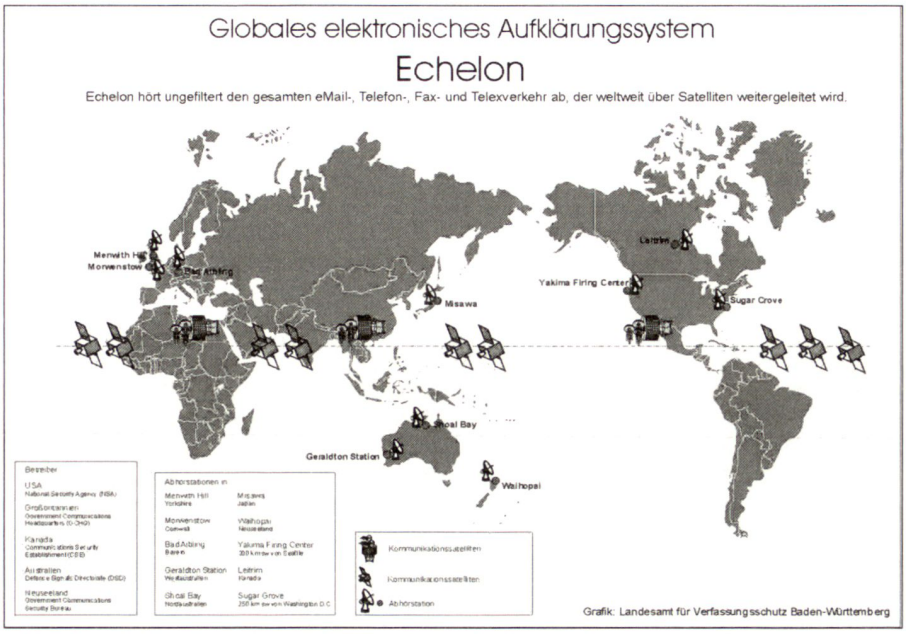


Abbildung 5: Das bekannte ECHELON-Stationierungskonzept.

gebaute und ins ECHELON-System eingebundene Station von *Morwenstow* gelegen *(Abbildung 4)*. Zufällig liegt diese nur 110 km nördlich der *satellite up and down link station* der *British Telecom* in *Goonhilly,* die wiederum für die Satelliten über dem Atlantischen und Indischen Ozean gebaut wurde. Zusätzlich zu *Morwenstow* ist eine zweite Station für die Satelliten über dem Pazifischen Ozean notwendig. Sie befindet sich auf einem Tafelberg in *Yakima Firing Centre,* Bundesstaat Washington, 200 km südlich von *Seattle.*

In den 70er- und 80er-Jahren wurde ein grosser Teil des Fernmeldeverkehrs nicht mehr über die langsamen Unterwasser-Kupferkabel, sondern neu über Satellitenverbindungen geführt. Diese über dem Äquator geostationär positionierten Satelliten der ersten Generation (sog. Intelsat) hatten zwar nur wenige tausend Kanäle, aber lediglich drei Satelliten mit breiter Abstrahlcharakteristik waren notwendig, um die Welt zu umspannen. Anfänglich genügten die zwei Stationen in *Morwenstow* und *Yakima* zur Überwachung des gesamten Intelsat-Verkehrs. ECHELON wurde indes Schritt für Schritt erweitert.[9] Der Ausbau des Intelsat-Netzes von wenigen Satelliten der ersten bis dritten Generation bis zu 20 Satelliten der siebten Generation bis Mitte der Neunzigerjahre führte zum Bau neuer Stationen, die ins ECHELON-Netz eingebunden werden konnten *(Abbildung 6)*. Heute sind 200 Länder über das Intelsat-Satellitennetz erschlossen *(Abbildung 5)*. Intelsat-Satelliten sind aber nur einige von vielen interessanten Zielobjekten. Aufgrund der immer dichteren Erschliessung mit Fernmeldeanschlüssen und der immer grösser werdenden Datenmenge wurden zusätzliche Satelliten für regionale oder landesspezifische Bedürfnisse in Betrieb genommen.[10] Neben den mindestens sechs Stationen, mit denen Intelsat abgehorcht wird, wurden in der Folge mindestens fünf weitere Stationen gebaut, um den regionalen Satellitenverkehr überwachen zu können.

Von der Schweiz aus gesehen ist die nächstgelegene Station des ECHELON-Systems die Feldstation F-81 in Mietraching bei Bad Aibling, zwischen München und Salzburg gelegen.[11] Bad Aibling kam mehrmals in die Schlagzeilen der deutschen Presse. Mehr als 1000 amerikanische Staatsangehörige arbeiten dort, ohne dass die Bundesrepublik selber Zutritt zu den Anlagen hätte. Letztes Jahr hätte diese Station für den ECHELON-Betrieb geschlossen und nach Griesheim bei Darmstadt verlegt werden sollen. Auf dem ehemaligen August-Euler-Flughafen stehen seit 2004 mindestens fünf neue so genannte Radarkuppeln (sog. Radome) mit Antennen. Ob die Verlegung wirklich vollzogen worden ist, weiss man allerdings nicht.

Das wirtschaftliche Gipfeltreffen des *World Economic Forum* (WEF) hat nach einer kurzzeitigen Verlegung nach New York im Jahre 2002 umgehend wieder im Talkessel von Davos in den Bündner Bergen stattgefunden. Obwohl nahe bei Bad Aibling gelegen, bedingt es technisch einen wesentlich höheren Aufwand, die lokal geführten Gespräche abhorchen zu können, als in New York.

In einsehbaren Geländen werden Radome nicht nur zum Schutz der Antennen vor Umwelteinflüssen eingesetzt, sondern hauptsächlich, um Bauart und Ausrichtung der Antenne verdeckt halten zu können. Seit im Internet Satellitenaufnahmen auch von ECHELON-Abhorchstationen einsehbar sind, hat die Verwendung von Radomen stark zugenommen.

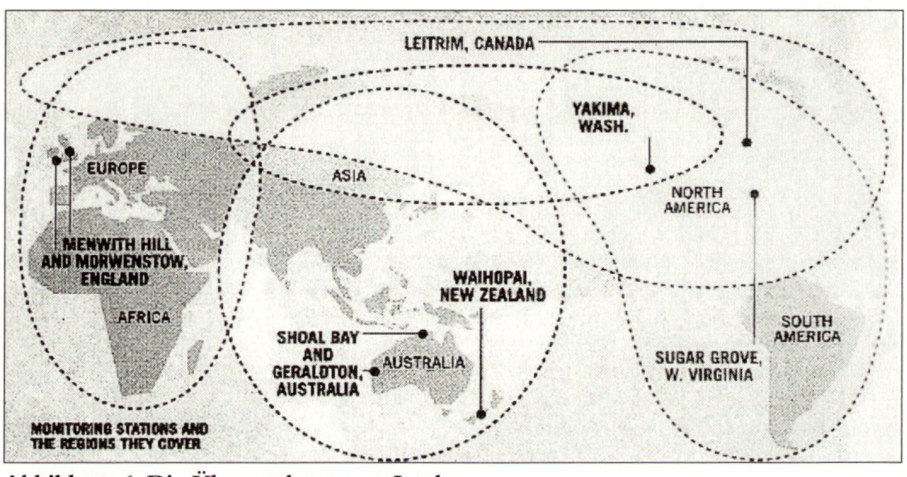


Abbildung 6: Die Überwachung von Intelsat.

[9] http://www.fas.org/irp/eprint/sp/sp_c2.htm

[10] http://de.wikipedia.org/wiki/Echelon. In Europa zum Beispiel Eutelsat oder für Italien Italsat.

[11] http://kai.iks-jena.de/miniwahr/badaibling.html

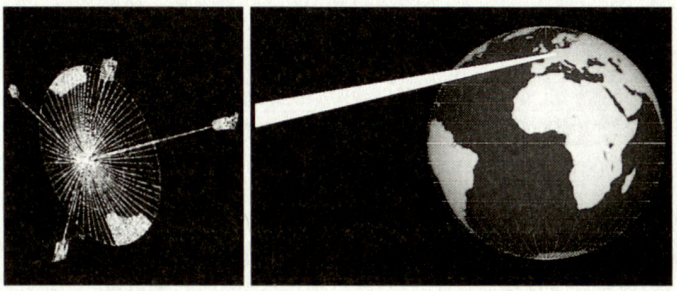


Abbildung 7: Vortex-Satellit.

Eine weitere Ebene im ECHELON-System sind Spionagesatelliten. Da inzwischen weltweit mehr als 1000 für Kommunikationssatelliten um die Erde kreisen, musste ECHELON nebst terrestrischen Abhörstationen auch Satelliten einsetzen. Diese horchen sowohl die Kommunikation per Satellit direkt im Weltall ab als auch diejenige auf der Erde aus dem Weltall.

Die mit dem Codenamen versehenen Orion- und Vortex-Satelliten werden von der amerikanischen Firma TRW konstruiert. Sie dienen der *telecom surveillance* und sind auf einer mittleren Höhe von 35700 Kilometer über der Erde positioniert *(Abbildung 7)*. Mit der sich ausbreitenden Verwendung des Mobilfunks wurden Satelliten mit dem Codenamen *Trumpet* der Herstellerfirma Boeing im Weltraum stationiert. Diese Satelliten haben eine Einsatzhöhe von 320 bis 35700 Kilometer.

Das Internet bedingte eine weitere ECHELON-Ebene. Die meisten Internetknoten stehen vor allem in den USA auf dem Gelände der Armee und können somit einfach «angezapft» und direkt dem ECHOLON-System zugeführt werden. Experten gingen vor dem 11. September 2001 davon aus, dass über 90% des gesamten Internetverkehrs durch ECHELON überwacht wird. Nach der Terrorattacke sind es nahezu 100%. Dabei hat diese Überwachung auch seine nützlichen Seiten, wie beispielsweise erfolgreiche internationale Operationen gegen die Kinderpornografie zeigen. Sie stützten sich auf US-Daten ab. Oder: Dass zur Ausführung der Terrorattacke in New York für Mobiltelefone Schweizer Prepaid-Karten verwendet wurden und Al-Kaida-Anführer Khalid Sheikh Mohammed deswegen verhaftet wurde, ist bekannt.[12] Weniger bekannt ist, dass die nachträgliche Eingabe der entsprechenden Suchbegriffe ins ECHELON-System diesen Fahndungserfolg ermöglicht hat.

Experten gingen vor dem 11. September 2001 davon aus, dass über 90 % des gesamten Internetverkehrs durch ECHELON überwacht wird. Nach der Terrorattacke sind es nahezu 100 %.

Das zunehmende Bedürfnis an grösserer Bandbreite führte dazu, dass neben Satelliten auch neue Übertragungsmedien gefunden werden mussten. Die Glasfasertechnologie setzte sich durch. Diese Technologie hat eine hohe Abhörsicherheit, da die Leitungen nicht abstrahlen und nicht einfach «angezapft» werden können. Die Kabel verfügen über optische Verstärker. Das heisst, leistungsfähigere Unterwasserkabel kommen wieder zum Zuge. In den letzten 20 Jahren wurden zahlreiche Glasfaserkabel unter Wasser verlegt oder sind noch im Bau.[13] Schon 1998 erreichte man damit eine transatlantische Datenrate von 26 Gbit pro Sekunde; heute ist es bereits ein Vielfaches. Alle diese Kabel enden an Kopfstationen in den USA, wo der Verkehr durch ECHELON überwacht werden kann. Es ist daher von strategischem Interesse der ECHELON-Partner, Kopfstationen kontrollieren zu können, um mit verhältnismässig geringem Aufwand an Daten zu gelangen, die ins ECHELON-System eingespiesen werden können.

Die Betreiber von ECHELON

Der wichtigste und grösste Betreiber des ECHELON-Systems ist die amerikanische *National Security Agency* (NSA). 1999 beschäftigte sie mehr als 40000 Mitarbeiter. Man vermutet, dass mit den zusätzlichen Aufgaben nach dem 11. September 2001 noch wesentlich mehr Mitarbeiter dazugekommen sind. Über 35000 Personen arbeiten am Hauptsitz in *Fort Meade/ Maryland,* 16 km nördlich von *Washington (Abbildung 8)*. Auf dem Gelände gibt es 1670 Gebäude und 150 km Strassen. Die Gebäude sind aufwändig abgeschirmt, um elektromagnetische Abstrahlung zu vermeiden. 30000 Tonnen an geheimen Akten wurden jährlich von NSA-Kurieren zwischen *Fort Meade* und *Washington* hin und her transportiert. Heute scheint ein stark abgeschirmtes Intranet benützt zu werden, das von 35 Geheimdiensten mit Information versorgt wird und 3000 Nutzer umfassen soll. Es gibt für die Angestellten eine eigene Autobahnausfahrt, und Fotos zeigen rund 18000 Parkplätze. Damit ist die NSA die weltweit grösste nachrichtendienstliche Organisation. Gemäss der NSA-Webseite beläuft sich das Budget für die Elektrizität am Hauptsitz auf 21 Millionen US-$ pro Jahr. Alle übrigen Verbraucher eingerechnet und vorsichtig geschätzt, ergibt das eine Rechenleistung der dort eingesetzten Computer von rund 160000 GFLOPS[14], also 16x10 hoch 13 Operationen pro Sekunde. Die NSA ist der weltweit grösste Arbeitgeber für Mathematiker (rund 16000) und der grösste Abnehmer für Hochleistungsrechner. Man darf annehmen, dass die NSA bezüglich Verschlüsselung allen übrigen auf der Welt um Jahre voraus ist. Gemäss der *Free Congress Research & Education Foundation* in Washington kann die NSA Verschlüsselungen bis zur Menge von gegen 1000 Bit entschlüsseln.

[12] www.guardian.co.uk *«How mobile phones and an 18£ bribe trapped 9/11 mastermind»*

[13] http://www.ita.hsr.ch/vorlesungen/computernetze/Transatlantiklink.pdf

[14] http://de.wikipedia.org/wiki/NSA

Abbildung 8: Das National Security Agency (NSA)-Hauptquartier Fort Meade, Maryland, USA.

Es ist auch kein Geheimnis, dass Nachrichtendienste bevorzugt Mieter in gleichen Gebäuden wie Telecom-Gesellschaften sind. Die NSA hatte jahrelang über der deutschen Hauptpost in Frankfurt residiert. Nach einigem Verwirrspiel gab sich der Bundesnachrichtendienst (BND) als offizieller Mieter der Räume zu erkennen, die Besucher waren jedoch mehrheitlich Amerikaner.[15]

Es ist auch kein Geheimnis, dass Nachrichtendienste bevorzugt Mieter in gleichen Gebäuden wie Telecom-Gesellschaften sind.

Das letzte veröffentlichte Budget für die US-Geheimdienstaktivitäten im Jahre 1998 wies 26,7 Milliarden US-Dollar aus. Ein Gerichtsbeschluss ordnete 1999 an, dass eine weitere Offenlegung der Budgets die nationale Sicherheit nachhaltig beeinträchtigen könnte. Seit der Terrorattacke vom 11. September 2001 – so darf angenommen werden – wurden diese Budgets massiv aufgestockt.

Weitere Betreiber des ECHELON-Systems sind:
– *Government Communication Headquarters* (GCHQ) in Grossbritannien[16]
– *Communication Security Establishment* (CSE) in Kanada[17]
– *Defence Signal Directorate* (DSD) in Australien[18]
– *Government Communications Security Bureau* (GCSB) in Neuseeland[19]

Systeme vergleichbar ECHELON

Man kann davon ausgehen, dass auch andere Länder über Systeme verfügen, um an Daten zu gelangen und sie auszuwerten. Man kann aber annehmen, dass keines dieser Systeme auch nur annähernd die Grössenordnung und Effizienz wie ECHELON hat. Das hat erstens mit den fehlenden finanziellen Mitteln und zweitens mit der Verfügbarkeit von genügend Rechenleistung zu tun.

Frankreich hat beispielsweise dank seinen ehemaligen Kolonien selbst eine weltumspannende Länderbasis für ein solches

Man kann davon ausgehen, dass auch andere Länder über Systeme verfügen, um an Daten zu gelangen und sie auszuwerten. Man kann aber annehmen, dass keines dieser Systeme auch nur annähernd die Grössenordnung und Effizienz wie ECHELON hat.

System. ECHELON ist offensichtlich für Frankreich kein Thema, in den Europäischen Kommissionen beispielsweise wurde ECHELON nie durch französische Vertreter thematisiert. Das Land hat eigene Satelliten und Trägerraketen sowie eine eigene Industrie zur Entwicklung und Herstellung der Infrastruktur. Der französische Nachrichtendienst *General Directorate for External Security* (DGSE), im Verteidigungsdepartement angesiedelt, ist u. a. zuständig für die strategische Informationsgewinnung *(electronic intelligence, counter intelligence)* ausserhalb des französischen Territoriums.[20] Antennenstationen sind in den meisten französischen Interessensgebieten dokumentiert, ihr genauer Zweck aber nicht bekannt.

Wie können wir uns schützen?

Oberster Grundsatz aller Benutzer im Umgang mit elektronischen Mitteln und Möglichkeiten muss die Aufmerksamkeit *(awareness)* gegenüber der täglich realen Bedrohung und gegenüber trügerischer Sicherheit sein. Ein Unterschied besteht

Oberster Grundsatz aller Benutzer im Umgang mit elektronischen Mitteln und Möglichkeiten muss die Aufmerksamkeit *(awareness)* gegenüber der täglich realen Bedrohung und gegenüber trügerischer Sicherheit sein.

zwischen dem militärischen und dem zivilen Umfeld. Zwar verfügt die Schweiz über eine ausgezeichnete Sicherheit in den militärischen Netzen. Das grösste Risiko stellt allerdings der (immer noch) geduldete Gebrauch von Mobiltelefonen in militärischer wie ziviler Umgebung dar.

Bei der Zusammenarbeit zwischen Armee und zivilen Behörden im Bereich der öffentlichen Sicherheit gibt es zudem bedenkliche Lücken. Das liegt begründet in der föderalistischen Struktur mit den 26 kantonalen Hoheiten und – fast ist man versucht zu sagen – mit 26 Lösungen. Die Sicherheitslücke rührt daher, weil es der Bund nicht schafft, das flächendeckende Sicherheitsnetz POLYCOM zu betreiben und im Sinne eines *back bone* die bestehenden kantonalen Polycom-Inseln und das Polycom-Netz der Grenzschutzorganisationen in einem einzigen Netz zu integrieren. Es bleibt zu hoffen, dass die erkannte Lücke mit Blick auf das sportliche Grossereignis UEFA EURO 2008 geschlossen werden kann.

Im zivilen Umfeld geht es in erster Linie um Industriespionage. Der EU-Bericht zu ECHELON dokumentiert einige Fälle. Beispielsweise installierte der französische Geheimdienst in den Flugzeugen der Air France in den Erstklasssitzen Mikrofone, um die Unterhaltungen der reisenden Geschäftsleute aufzuzeichnen. Dies wurde bis 1994 praktiziert, danach entschuldigte sich die Fluggesellschaft öffentlich. Der Fall des Volkswagen-Managers José I. Lòpez ist ein weiterer. Seine Videokonferenzen wurden von der NSA mitgeschnitten und der Firma *General Motors* zugespielt.

Letztlich geht es in allen Fällen um Informationssicherheit. Nachdem bewiesen ist, dass unser Wissen systematisch abgehört, gefiltert und ausgewertet wird, muss man sich einige Fragen stellen. Was bedeutet dies für unsere Behörden, Organisationen, Unternehmen und für mich als Privatperson? Wie werden wir als Bürger, Unternehmen, Mitglied oder Mitarbeiter informiert, sensibilisiert und ausgebildet, um sicherzustellen, dass das schützenswerte Wissen auch wirklich geschützt wird? Und vor allem stellt sich die Frage, wessen Aufgabe ist es zu informieren, zu sensibilisieren und auszubilden? Dies erfordert eine Analyse der Bedrohung, des Risikos und der Schwachstellen. Das muss zu Sicherheitsvorkehrungen führen, die aus infrastrukturellen, organisatorischen, technischen und personellen Massnahmen bestehen. Sie dienen dem Ziel, Vertraulichkeit, Integrität, Verlässlichkeit und Verfügbarkeit der Information wahren zu können. Der übergeordnete Rahmen dieser Vorkehrungen bildet die *security policy* einer Organisation. Die Mitarbeiter müssen nach den Richtlinien dieser *security policy* ausgebildet werden, und deren Umsetzung muss kontrolliert, nötigenfalls auch durchgesetzt, werden. Das hat letztlich mit Führung zu tun und nicht mit blossem Einsatz weiterer Technik. Ein Experte hat dies wie folgt formuliert:

If you* think *that technology can solve your security problem, then you don't understand the problem and you don't understand the technology. ●

[15] http://www.heise.de/ct/98/05/082
[16] http://www.fas.org/irp/world/uk/gchq/
[17] http://www.cse-cst.gc.ca/en/home/peer_organization-e.html
[18] http://www.dsd.gov.au/
[19] http:// www.govt.nz
[20] http://www.fas.org/irp/world/france/defense/dgse/

Network Enabled Operations (NEO): L'approche suisse de la transformation

Der Autor stellt uns kurz die C4ISTAR-Vision des Planungsstabes der Armee vor und erläutert anschliessend die gewählte Umsetzungsstrategie mit den erforderlichen doktrinalen Begleitmassnahmen.

Christian Bühlmann*

L'armée suisse ne peut échapper à la tendance générale à la transformation que poursuivent les Forces armées occidentales. En effet, les engagements contemporains ne peuvent être réalisés que par une intégration de forces modulaires, de systèmes d'armes, voire des partenaires nationaux (dans le cadre d'une coordination multiniveaux) ou étrangers (engagements multinationaux im Rahmen eines entsprechenden Mandates) pour créer rapidement des effets décisifs. L'intégration de capteurs, d'effecteurs, d'outils de traitement et de services dans un même système de conduite conduit à une multiplication des forces sans précédent, par

- une augmentation de la vitesse d'exécution due à la disponibilité d'informations et à l'auto-synchronisation et par
- la maximisation de l'enveloppe d'efficacité des effecteurs par la mise en réseau de capteurs et des effecteurs.

Dans cette optique, l'Etat-major de planification de l'armée (EM plan A) a défini une vision C4ISTAR qui vise à remplir les tâches des Forces armées suisses de manière efficiente, en fusionnant à temps et au juste niveau les informations importantes en une représentation complète et unifiée de la situation.

La stratégie d'implémentation C4ISTAR prévoit,
– dans une première phase (2004–2008), de réaliser l'aide au commandement intégrée afin d'assurer l'échange d'informations à temps et au juste niveau au sein du groupe Défense et,
– dans une seconde phase (2008–2011) de rendre l'armée capable de générer et de distribuer au juste niveau et à temps une *«Joint Recognised Picture»*. Ces prestations seront rendues possibles par l'acquisition de nouveaux senseurs, l'augmentation ou le maintien de la valeur de combat des senseurs actuels ou des effecteurs disponibles, ainsi que par leur fusion au sein de l'aide au commandement intégrée.

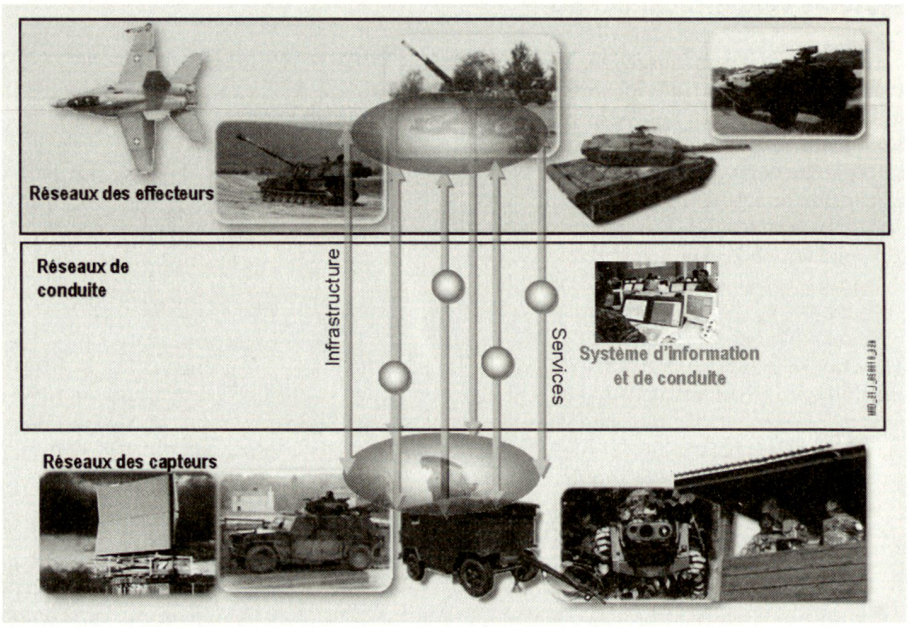
En parallèle, il s'agira de créer à tous les niveaux les capacités pour la planification et la conduite réseaucentrique par un développement évolutif de l'aide au commandement intégrée et de garantir l'interopérabilité.

Cependant, cette approche technologique (de type *Network Centric Warfare, Network Enabled Capabilities)* n'est pas suffisante, car elle risque de ne mener qu'à une **attribution** plus efficace. Elle doit être complétée par un concept doctrinal orienté sur les effets, baptisé ***Network Enabled Operations (NEO),*** pour obtenir, par la manœuvre, une **efficience** décisive à travers l'ensemble des types d'opération des Forces armées.

Du point de vue doctrinal, ce concept doit
– **considérer** l'ensemble des tâches de l'armée, d'où le passage à une approche de type «senseur à effets» plutôt que *«sensor to shooter»*,
– conduire à **gagner** la supériorité dans la décision et l'action,
– aider à **saisir** les chances par une doctrine manœuvrière concentrant les effets et délocalisant les effecteurs, plutôt qu'adopter une attitude défensive,
– **maintenir** l'aptitude à fonctionner avec une technologie dégradée par le développement de la conduite par objectifs.

En conclusion, on peut affirmer que
1. Le concept des NEO doit, à moyen et plus long terme, former le moteur de la transformation des Forces armées suisses.
2. Les NEO viseront à générer des effets décisifs amenant aux objectifs stratégiques à travers l'ensemble des tâches de l'Armée.
3. Le succès des NEO résidera dans
– la supériorité de la décision et de l'action,
– une approche manœuvrière de l'application ou de la menace d'application de la force,
– un changement de **culture** au sein de l'armée.
4. Une nouvelle approche doctrinale est indispensable pour mettre en œuvre les NEO.

Malgré l'importance des développements techniques, le rôle de l'homme demeurera capital pour le concept des NEO: C'est dans et par l'esprit que les engagements sont gagnés. ●



Gagner en efficience: L'approche Network Enabled Operations (NEO).

*Lt col EMG Christian Bühlmann, chef du domaine de la recherche et du développement en matière de doctrine militaire, Etat-major de planification de l'armée.

Das operativ/taktische ISTAR-System der Schweizer Armee zur Erstellung der erkannten Bodenlage

Im folgenden Artikel erläutert der Autor die zurzeit laufende Konzeptstudie zur Erstellung der erkannten Bodenlage. Dabei werden zuerst die notwendigen Voraussetzungen erläutert, und es wird anschliessend ein Soll-Ist-Vergleich angestellt, bei welchem auch die ISTAR-Defizite herausgeschält werden. Danach geht der Autor detailliert auf die Erfordernisse zur Umsetzung ein.

André Kotoun*

Im Zuge der Planungen zur Schweizer Armee (A XXI) beauftragte der Chef des Planungsstabes der Armee eine Arbeitsgruppe mit der Erstellung einer Konzeptionsstudie «Aufklärung».

Am 18. März 2005 wurde die Konzeptionsstudie «Aufklärung» durch den Streitkräfteplanungsausschuss genehmigt. Im folgenden Artikel sollen die wichtigsten und schwergewichtig die Teilstreitkraft HEER (TSK HEER) betreffenden Resultate vorgestellt und erläutert werden.

Ausgangslage

Anforderungen an die Nachrichtenbeschaffung

Die Militärstrategie der Schweizer Armee hat in den vergangenen Jahren mehrere Paradigmenwechsel durchlaufen. So wurde die statische und flächendeckende, vorwiegend autonom geführte Abwehrkonzeption der Armee 61 ab 1995 durch das teilmobile und nur noch teilweise flächendeckende Konzept der dynamischen Raumverteidigung (Armee 95) abgelöst. Mit der seit 2004 gültigen Konzeption (A XXI), wird dem Wandel des Bedrohungsspektrums Rechnung getragen. Dynamik, Komplexität und die verminderte Bedeutung des geografischen Raumes sind dabei die prägenden Merkmale.

Im Zuge dieser Entwicklung sind die Anforderungen an das Nachrichtenbeschaffungswesen der Armee drastisch angestiegen. Die Ursache liegt darin, dass die Truppendichte beträchtlich abnimmt und die militärischen Verbände nicht mehr statisch eingesetzt werden, sondern sich in Bereitschaftsräumen für mehrere mögliche Einsätze bereithalten. Dies zieht für alle betroffenen Führungsebenen einen erhöhten Reaktionszeitbedarf nach sich. Dieser entsteht, weil die betroffenen Verbände Zeit benötigen, um aus diesen Bereitschaftsräumen heraus rechtzeitig die der Absicht entsprechenden Einsatzräume zu erreichen.

Dies bedingt eine wesentliche Erweiterung der Interessenräume und damit verbunden, eine entsprechend vervielfachte Zunahme der Anzahl der eigentlichen Nachrichtenbeschaffungsräume.

Das aber bringt einen grossen zusätzlichen Sensorbedarf beziehungsweise einen stark erhöhten Bedarf nach zusätzlicher Reichweite und Vergrösserung des Betrachtungsraums der eingesetzten Sensoren mit sich. Auch steigert die Null-Fehler-Toleranz der Medien und der Politik in allen militärischen Operationen den Bedarf an präziser, dauernder und umfassender Aufklärung, zusätzlich zur Sicherstellung von hoher Präzision und damit verbunden der Vermeidung von Kollateralschäden.

Daraus ergibt sich, dass eine mit einem Strategie- oder Verteidigungskonzeptionswechsel verbundene Verringerung der Truppenstärke respektive Truppendichte immer mit einem beträchtlichen Mehrbedarf an Sensorik einhergeht *(Abbildung 1)*. Gleichzeitig erhöhen sich die Anforderungen an das Nachrichtenbeschaffungswesen als Ganzes. Diesem Umstand ist bei der Entwicklung einer zukünftigen Architektur des Nachrichtenbeschaffungssystems der Armee entsprechend Rechnung zu tragen.

Aus dieser Erkenntnis und abgeleitet aus dem Aufgaben- und Bedrohungsspektrum der Armee einerseits und den Vorgaben für die Fähigkeits- und Kompetenzausprägung der Armee andererseits, lassen sich nun grundsätzliche Anforderungen an das Nachrichtensystem gezielt ableiten *(Abb. 2)*.

In der Folge muss die Armee über die **Fähigkeit** verfügen:

- jederzeit, in Kooperation mit zivilen Partnern die für die militärische Führung subsidiärer Sicherungseinsätze im Inland benötigten Nachrichten über eine Gegenseite (asymmetrisch operierende, irreguläre Kräfte) rechtzeitig zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach kurzer (Tage) bis mittlerer (Wochen–Monate) Vorbereitungszeit, in Kooperation mit zivilen und militärischen Partnern die für die militärische Führung präventiver Raumsicherungsoperationen im Inland und im grenznahen Ausland benötigten Nachrichten über eine Gegenseite rechtzeitig zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach kurzer bis mittlerer Vorbereitungszeit, in Kooperation mit zivilen und militärischen Partnern die für die militärische Führung von PSO-Einsätzen im Ausland benötigten Nachrichten über eine Gegenseite rechtzeitig zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach kurzer bis mittlerer Vorbereitungszeit, selbstständig oder in Kooperation mit militärischen Partnern die für die militärische Führung (bis Stufe Einsatzbrigade) von dynamischen Raumsicherungs- und Verteidigungseinsätzen im In- und Ausland benötigten Nachrichten über einen Gegner und/oder eine Gegenseite rechtzeitig zu beschaffen, auszuwerten, zu bewerten und zu verbreiten.

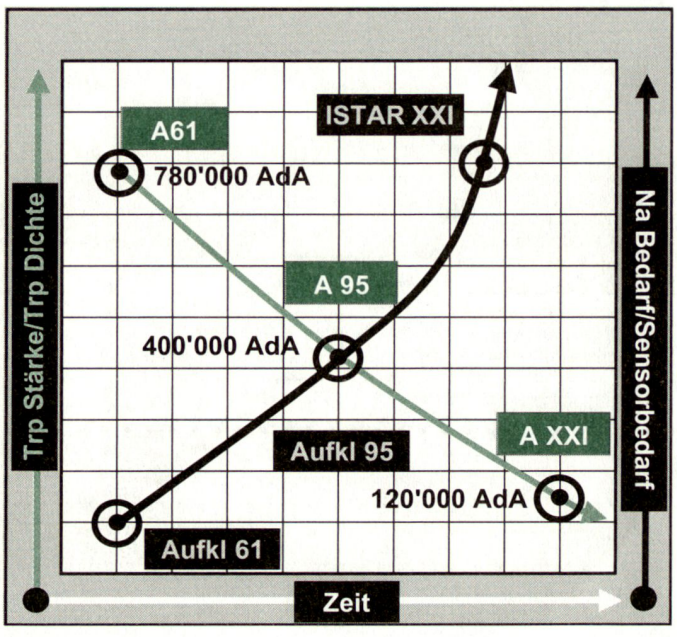


Abbildung 1: Entwicklung des Sensorbedarfs. Truppendichte vs Sensorbedarf A 61/A 95/A XXI.

* André Kotoun, stv. C HE Doktrin, PL LandOp und PL ISTAR LAND im Bereich Heeresdoktrin, Teilstreitkraft Heer.

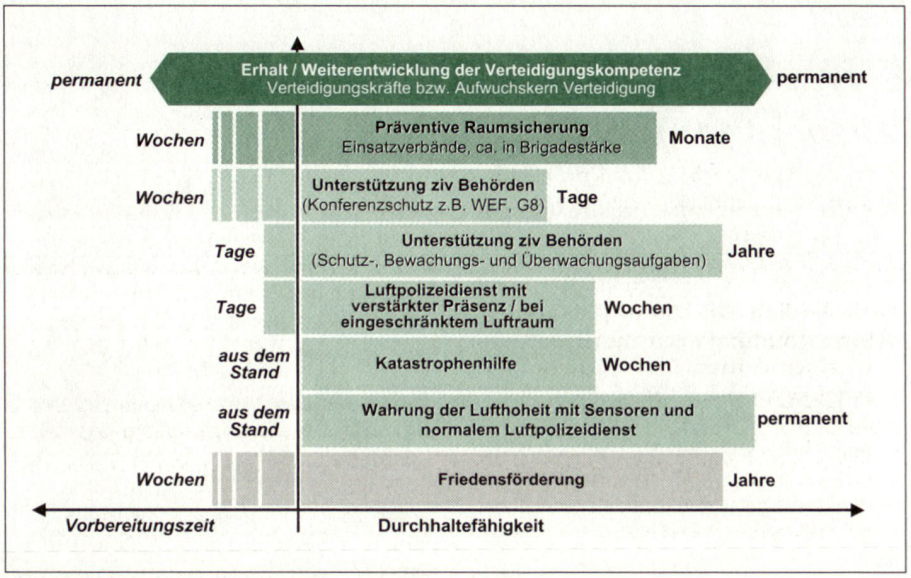


Abbildung 2: Fähigkeits-/Kompetenzausprägung der Armee.
Maximale, gleichzeitig erbringbare Leistungen der Armee ab 2008/2011 (ohne Einsatz der Reserve).

Die Armee muss darüber hinaus über die **Kompetenz** verfügen:

- jederzeit in Kooperation mit zivilen und militärischen Partnern die für die militärische Führung (Stufe operativer Einsatzverband) von dynamischen Raumsicherungs- und Verteidigungsoperationen im In- und Ausland benötigten Nachrichten über einen Gegner und/oder eine Gegenseite rechtzeitig zu beschaffen, auszuwerten, zu bewerten und zu verbreiten.

Hinzu kommt, dass das zukünftige ISTAR-System (Intelligence, Surveillance, Target Acquisition, Reconnaissance-System) der Schweizer Armee – als Teil des künftigen Führungs- und Wirkungsverbundes der Armee – sicherstellen muss, dass identifizierte Schlüsselziele automatisiert oder teilautomatisiert nach kürzester Zeit bekämpft werden können (Aufklärungs-Wirkungs-Verbund).

Dies hat zur Folge, dass die Entwicklung des zukünftigen ISTAR-Systems der Schweizer Armee in engster Abstimmung mit dem Aufbau des ersten digitalen Führungsverbundes (Command, Control, Communication, Computers, Information-System (C4I-System) erfolgen muss.

Die Schweizer Armee im Allgemeinen und die TSK HEER im Besonderen stützen sich dabei inskünftig in der Planung und Weiterentwicklung auf eine dem Denkmodell der Gefechtsfeldsysteme basierte Architektur *(Abbildung 3)*.

Aus der Analyse der Nachrichtenbedürfnisse der verschiedenen Führungsebenen in den verschiedenen Operationstypen ergibt sich die grundsätzliche Erkenntnis, dass:

- die unterschiedlichen Bedrohungsformen auch unterschiedlich ausgeprägte und konditionierte Nachrichtenbeschaffungsinstrumente erfordern;
- keine Bedrohungsform innerhalb des Bedrohungsspektrums mit nur einer Art von Sensor umfassend aufgeklärt werden kann.

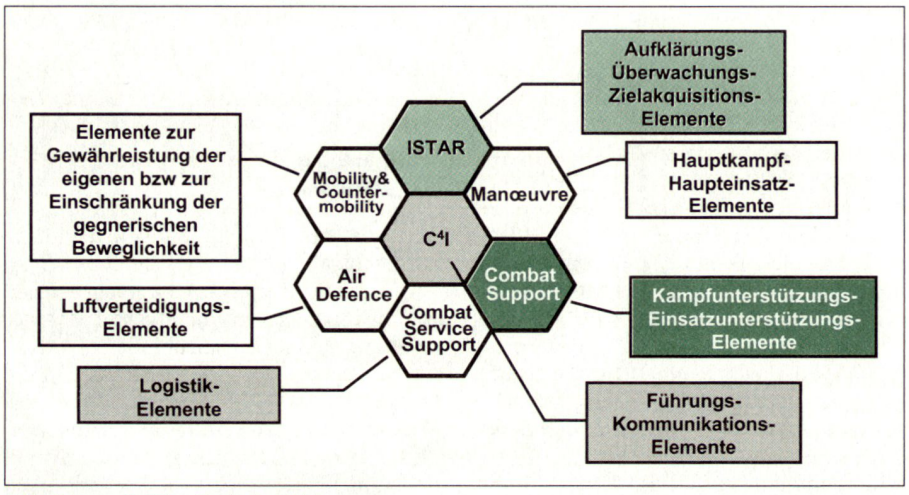


Abbildung 3: Die Gefechtsfeldsysteme.

Folglich soll das künftige ISTAR-System so modular aufgebaut sein, dass man den in den verschiedenen Operationstypen eingesetzten Einsatzverbänden (Territorialregionen und Einsatzbrigaden) aufgabenorientiert ausgeprägte ISTAR-Teilsysteme (ISTAR-Bataillone) beistellen kann.

Das zukünftige ISTAR-System muss somit über auf die unterschiedlichen Nachrichtenbedürfnisse der verschiedenen Führungsebenen und der verschiedenen Kräfte (Sicherungskräfte, Verteidigungskräfte, Unterstützungskräfte) abgestimmte und über aufgabenorientiert ausgeprägte ISTAR-Teilsysteme verfügen. Diese sind zwingend als organische Verbände zu konzipieren, da ansonsten eine Einbindung in das C4I-System de facto unmöglich wird. Pro Operationstyp (beziehungsweise Führungsebene) ist also ein spezifisch optimierter Typ von ISTAR Bataillon zu schaffen.

Resultate des SOLL-/IST-Vergleichs

Basierend auf den oben aufgeführten Erkenntnissen wurden die bestehenden ISTAR-Mittel und -Fähigkeiten der Schweizer Armee einer SOLL-/-IST-Analyse unterzogen.

Vorhandene ISTAR-Fähigkeiten

Die Schweizer Armee ist (Stand Oktober 2005) in der Lage:

- Nach mittlerer Vorbereitungszeit, in Kooperation mit zivilen Partnern die wichtigsten für die militärische Führung subsidiärer Sicherungseinsätze benötigten Nachrichten über eine Gegenseite, partiell in der geforderten Zeit und teilweise genügender Qualität, zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach langer (Monate–Jahre) bis sehr langer Vorbereitungszeit, in Kooperation mit zivilen militärischen Partnern Teile der für die militärische Führung präventiver Raumsicherungsoperationen benötigten Nachrichten über eine Gegenseite, teilweise in der geforderten Zeit und teilweise genügender Qualität zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach kurzer bis mittlerer Vorbereitungszeit, in Kooperation mit zivilen und militärischen Partnern die für die militärische Führung von PSO-Einsätzen im Ausland benötigten Nachrichten über eine Gegenseite teilweise in der geforderten Zeit zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- nach sehr langer Vorbereitungszeit, autonom, Teile der für die militärische (bis Stufe Einsatzbrigade) Führung von dynamischen Raumsicherungs- und Verteidigungseinsätzen – ausschliesslich im Inland und im grenznahen Ausland – benötigten Nachrichten über einen Gegner und/oder

eine Gegenseite, zu kleinen Teilen in der geforderten Zeit, zu beschaffen, auszuwerten, zu bewerten und zu verbreiten;
- jederzeit, autonom Teile der für die operative/militärstrategische Führung von dynamischen Raumsicherungs- und Verteidigungsoperationen im In- und Ausland benötigten Nachrichten über einen Gegner und/oder eine Gegenseite, teilweise in der geforderten Zeit, zu beschaffen, auszuwerten, zu bewerten und zu verbreiten.

Fehlende ISTAR-Fähigkeiten

Zum heutigen Zeitpunkt fehlen der Armee folgende, für die Wahrnehmung ihrer Aufträge notwendigen ISTAR-Fähigkeiten:
- die Fähigkeit und die Kompetenz zur systematischen und teilautomatisierten Auswertung, Bewertung und Verdichtung von durch in verschiedenen Aufklärungsspektren beschafften Nachrichten;
- die Fähigkeit und die Mittel zur Vernetzung der verschiedenen dem ISTAR-System zugehörigen Sensoren, Auswertungsorganen und Effektoren und damit in vielen Bereichen die Fähigkeit zur zeitgerechten Nutzung der Aufklärungsergebnisse;
- Teilfähigkeiten und Mittel zur Aufklärung von Gegenseiten;
- die Fähigkeit und die Mittel zur proaktiven Aufklärung eines Gegners (vor allem in friedensfördernden Einsätzen);
- die Fähigkeit zur multispektralen Aufklärung;
- die Fähigkeiten und die Mittel für einen boden- und luftgestützten Aufklärungs-Wirkungs-Verbund.

Absicht für die Entwicklung des ISTAR-Systems der Armee

Es geht in den kommenden Jahren darum:

in einer ersten Phase *(Schaffung der Grundlagen/Kompetenzbündelung)*
zunächst
- eine breit abgestützte Joint-ISTAR-Projektorganisation einzusetzen und die Konzeptionsstudie zu vertiefen;

damit
- eine kontinuierliche, zielgerichtete Planung und Weiterentwicklung der ISTAR-Fähigkeiten der Armee zu gewährleisten;

in einer zweiten Phase *(Modernisierung und Ausbau der bestehenden Fähigkeiten)*
- die bestehenden ISTAR-Fähigkeiten zu modernisieren und zu ergänzen, die ISTAR-Akteure durch Integration in das C4I-System der Armee zu vernetzen sowie die Interoperabilität mit ausländischen Streitkräften sicherzustellen;

gleichzeitig
- für die Aufklärung in der TSK HEER in den verschiedenen Teilaufträgen und auf den verschiedenen Führungsebenen spezialisierte Verbände und Organisationseinheiten zu schaffen und bei der Luftwaffe die entsprechenden Sensoren in die Einsatzverbände zu integrieren;

in einer dritten Phase *(Aufbau der wichtigsten fehlenden Fähigkeiten)*
zunächst auf taktischer Stufe
- einen luftgestützten Aufklärungs-Wirkungs-Verbund sowie die Fähigkeit zur bodengestützten, proaktiven (gewaltsamen) Aufklärung aufzubauen;

dann
- die Kompetenz zur satellitengestützten Aufklärung und zur luftgestützten multispektralen Aufklärung mit integrierter Führungsfähigkeit gegen mobile zeitkritische Ziele zu entwickeln.

Umsetzung

1. Phase: Schaffung der Grundlagen/ Kompetenzbündelung (2005–2007)

Schaffung vertiefter und erweiterter Grundlagen

Die Konzeptionsstudie «Aufklärung» gibt nur eine grobe Richtung für das Vorgehen bei der Entwicklung des ISTAR-Systems vor. Die bei der Erstellung der Konzeptionsstudie gewonnenen Erkenntnisse müssen daher mittels Folgestudien überprüft und vertieft werden.

Kompetenzbündelung

Die entscheidende Massnahme für den Aufbau der ISTAR-Fähigkeit ist die organisatorische Bündelung der verschiedenen mit ISTAR befassten Elemente und Organisationseinheiten der Armee.

2. Phase: Umbau/Modernisierung der bestehenden Fähigkeiten (2007–2009)

Bei diesem Entwicklungsschritt geht es um folgende Massnahmen:
- Qualitative Verbesserung der Nachrichtenauswertung und Nachrichtenbewertungsfähigkeit durch Anpassung der Ausbildung der ND-Spezialisten (Nachrichtenoffiziere, -unteroffiziere und -soldaten, Auswerteoffiziere und -spezialisten) an die tatsächlichen Bedürfnisse;
- Umbau der bestehenden Aufklärungsbataillone in spezialisierte ISTAR-Bataillone (1 ISTAR-Bataillon Typ A für die Stufe TSK HE resp. für eine operative Task Force. 2 ISTAR-Bataillone Typ B für die Sicherungskräfte des Heeres. 2 ISTAR-Bataillone Typ C für die Verteidigungskräfte des Heeres);
- Einbindung aller ISTAR-Akteure in die C4I-Architektur der Armee;
- Modernisierung des Aufklärungsdrohnensystems 95 durch Beschaffung eines neuen Sensorpakets und deren Anbindung an die ISTAR-Bataillone Typ B und C;
- Verbesserung der elektronischen Selbstschutzfähigkeiten der Luftwaffe;
- Re-Role der Fallschirmaufklärerkompanie.

Verbesserung der Nachrichtenauswertung und Nachrichtenbewertungsfähigkeit

Basierend auf einer noch vorgängig zu erstellenden Studie zur Datenfusion, Datensimulation, Interoperabilität und Ausbildung ist ein den modernen Anforderungen gerecht werdendes Ausbildungskonzept für alle ND-Spezialisten (Profi und Miliz) zu entwickeln und umzusetzen.

Schaffung von ISTAR-Bataillonen (ISTAR-Teilsysteme)

Es geht darum, die bestehenden Aufklärungsbataillone an die Anforderungen, welche ein multispektrales, netzwerkgestütztes, terrestrisches Nachrichtenbeschaffungssystem stellt, anzupassen.

Die Schaffung folgender ISTAR-Truppenkörper ist dabei aus heutiger Sicht vorgesehen:

1 ISTAR-Bataillon Typ A

Auf die (reaktive) Aufklärung primär eines modernen, das Gefecht der verbundenen Waffen führenden Gegners, sekundär einer Gegenseite und die Nachrichtenauswertung und Nachrichtenverbreitung zu Gunsten der TSK HEER und/oder eines operativen Einsatzverbandes spezialisierter Modulbaustein.

2 ISTAR-Bataillone Typ B

Auf die (reaktive) Aufklärung einer Gegenseite und die Nachrichtenauswertung und Nachrichtenverbreitung zu Gunsten einer Territorialregion oder einer Einsatzbrigade (Sicherungskräfte) spezialisierter Modulbaustein.

2 ISTAR-Bataillone Typ C

Auf die (reaktive) Aufklärung eines modernen, das Gefecht der verbundenen Waffen führenden Gegners und die Nachrichtenauswertung und Nachrichtenverbreitung zu Gunsten einer Einsatzbrigade (Verteidigungskräfte) spezialisierter Modulbaustein.

Kampfwertsteigerung ADS-95 und Anbindung an die ISTAR-Bataillone

Die ADS-95 sind mittels angemessener Kampfwertsteigerung an die ISTAR-Bataillone Typ B und C anzubinden.

Die Kampfwertsteigerung soll es möglich machen, Objekte auf grössere Distanzen und mit besserer Auflösung aufzuklären und zudem die ISTAR-Bataillone Typ B und C dazu befähigen, Schlüsselziele über den Aufklärungs-Wirkungs-Verbund, mit

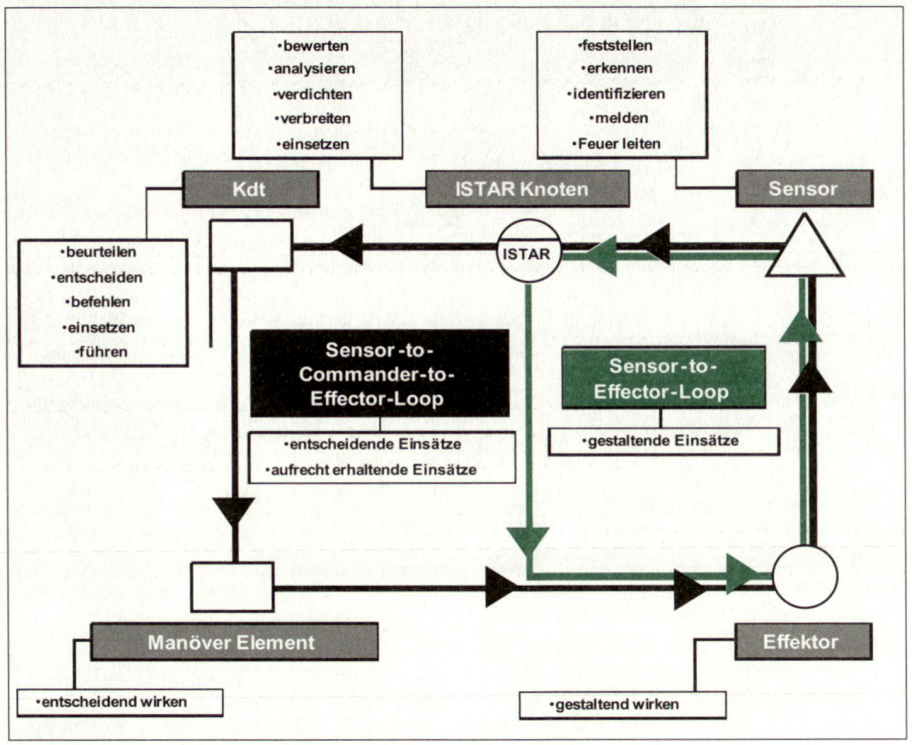


Abbildung 4: Aufklärungs-Wirkungs-Verbund (Prozess).

luft- oder bodengestützten Mitteln, zeitgerecht und teilautomatisiert bekämpfen zu können.

Electronic Support Measures (ESM) für die fliegenden Systeme der Luftwaffe

Für die Systeme der Luftwaffe ist die Bedrohung durch bodengestützte Fliegerabwehrwaffen (zum Beispiel durch Einmannlenkwaffen) ein zunehmend grösserer Risikofaktor. Gleichzeitig steigen aber die technischen Möglichkeiten zum elektronischen Selbstschutz.

Die heute in der Schweizer Armee vorhandenen Beschaffungssysteme vermögen unter anderem aus Gründen der Empfindlichkeit und teilweise des Flugprofils des Systemträgers den Anforderungen nur teilweise zu genügen. Ziel ist deshalb die Beschaffung zweier ab F/A-18 einsetzbarer ESM Pods, welche die Lücken in diesem Bereich schliessen sollen.

Re-role der Fallschirmaufklärerkompanie

Die Fallschirmaufklärerkompanie verfügt über einen exzellenten Stand an Ausbildung und ist international mit Profiverbänden vergleichbar. Ihre auf den Kalten Krieg ausgelegten Fähigkeiten sind aber heute nur noch teilweise von Bedeutung.

Daher soll hier eine grundsätzliche Umorientierung von deren Rolle geprüft werden.

Denkbar sind unter anderem Einsätze als:

- Zielaufklärer in der Tiefe des Raumes (als Sensoren des luft- bzw. des bodengestützten Aufklärungs-Wirkungs-Verbundes);
- Erkundungs- und Aufklärungsdetachement im Vorgang von Auslandeinsätzen.

3. Phase: Aufbau der wichtigsten fehlenden Fähigkeiten (2009–2011)

Netzwerkbasierter Aufklärungs-Wirkungs-Verbund (Boden und Luft)

In diesem Massnahmenpaket geht es um den Aufbau eines netzwerkbasierten Aufklärungs-Wirkungs-Verbundes *(Abbildung 4)* auf taktischer Ebene. Dieser umfasst sowohl einen bodengestützten als auch einen luftgestützten Aufklärungs-Wirkungs-Verbund, welche wiederum untereinander verbunden sein müssen.

Die Schaffung eines solchen Aufklärungs-Wirkungs-Verbundes bedingt den Aufbau entsprechender Strukturen, welche zum Teil erheblich von den heutigen Organisationsstrukturen der Armee abweichen.

Es wird darum gehen, die auch fürderhin hierarchisch organisierte militärische Führungsstruktur mit einer ahierarchisch organisierten ISTAR-Struktur *(Abbildung 5)* zu verknüpfen und in Einklang zu bringen.

Dazu werden den Stabszellen des Führungsgrundgebiets 2 (ND) der verschiedenen Führungsebenen (Bataillon bis TSK) über C4I-Schnittstellen (Interface) ISTAR- resp. ISR-Knoten beigestellt. Diese sind ihrerseits mit aufgaben- und führungsebenenspezifisch zusammengestellten Sensorpaketen, im Falle der Einsatzbrigaden und Territorialregionen, auch mit Effektorpaketen vernetzt.

Die so entstehenden ISTAR- bzw. ISR-Cluster (welche weit gehend den oben beschriebenen ISTAR-Bataillonen und den mit diesen fallweise verbundenen Effektoren entsprechen) werden ahierarchisch vernetzt, sodass von jedem ISTAR- bzw. ISR-Knoten aus auch auf die Sensor-, Auswerte- und Effektorleistungen der anderen Cluster praktisch zeitverzugslos zugegriffen werden kann. Damit können alle militärischen Akteure dazu befähigt werden, die durch die eigenen Sensoren beschafften Nachrichten zeitgerecht mit den Lagebildern der vorgesetzten Stellen, der Nachbarn sowie der Unterstellten zu einem akkuraten Lagebild zu verdichten. Dies

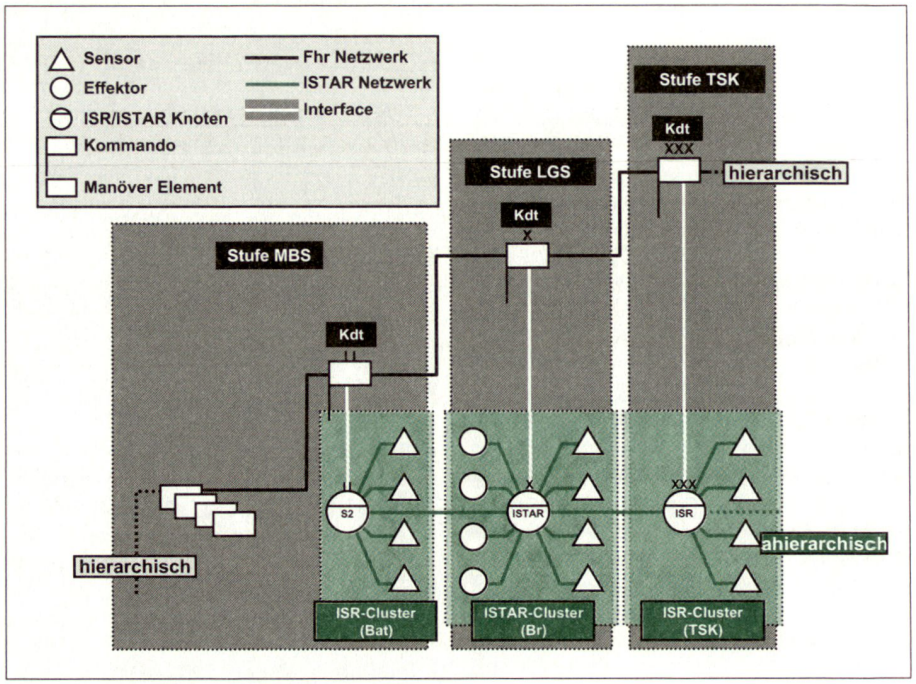


Abbildung 5: ISTAR-Struktur (Auszug TSK HEER).

wiederum erlaubt den militärischen Entscheidträgern, permanent ein hohes und genaues Lagebewusstsein zu entwickeln.

Bodengestützter Sensor zu Effektor-Kreislauf

Hierbei geht es primär darum, den heute schon bestehenden, bodengestützten, noch rudimentären Aufklärungs-Wirkungs-Verbund:

- durch Integration oder Verknüpfung mit dem Führungsinformationssystem der TSK HEER (FIS HE) in die ISTAR-Struktur zu integrieren;
- mit den noch nicht eingebundenen Sensoren der TSK HEER und zusätzlichen Effektoren zu ergänzen.

Luftgestützter Aufklärungs-Wirkungs-Verbund

Ziel ist der Aufbau des folgenden Fähigkeitskreislaufs:

- Aufklärung von Schlüsselzielen in der Tiefe des taktischen Einsatzraums durch boden- oder luftgestützte Sensoren;
- zeitverzugslose Übermittlung der Zieldaten zum luftgestützten Waffenträger (F/A-18 und/oder Neues Kampfflugzeug (NKF);
- Planung des Wirkungseinsatzes im Flugzeug bzw. in der Munition innert weniger Minuten;
- autonome Bekämpfung des Ziels innert weniger als 10 Minuten nach Zielaufklärung;
- Wirkungsaufklärung mit möglichst zeitverzugsloser Übermittlung der Resultate an den luftgestützten Waffenträger oder direkt an die Waffe.

Aufwuchskern proaktive (gewaltsame) Aufklärung

Aufklärung im Rahmen von dynamischen Raumsicherungs- und Verteidigungsoperationen, aber auch im Rahmen von PSO-Einsätzen, muss zunehmend in Räumen erfolgen, die von Anbeginn weg durch eine Gegenseite und/oder einen Gegner kontrolliert werden. Entsprechend geht es bei diesem Entwicklungsschritt darum, durch Schaffung eines Panzeraufklärungsbataillons der Armee, im Sinne eines Aufwuchskerns, die Kompetenz zur proaktiven (gewaltsamen) Aufklärung zu verschaffen.

Satellitengestützte Bildaufklärung

In diesem Bereich soll in zwei Schritten vorgegangen werden. In einem ersten Schritt werden Satellitenbilder aus für die schweizerischen Interessen relevanten Krisenregionen durch die Armee eingekauft (commercial off the shelf). Mit diesen Daten kann Folgendes erreicht werden:

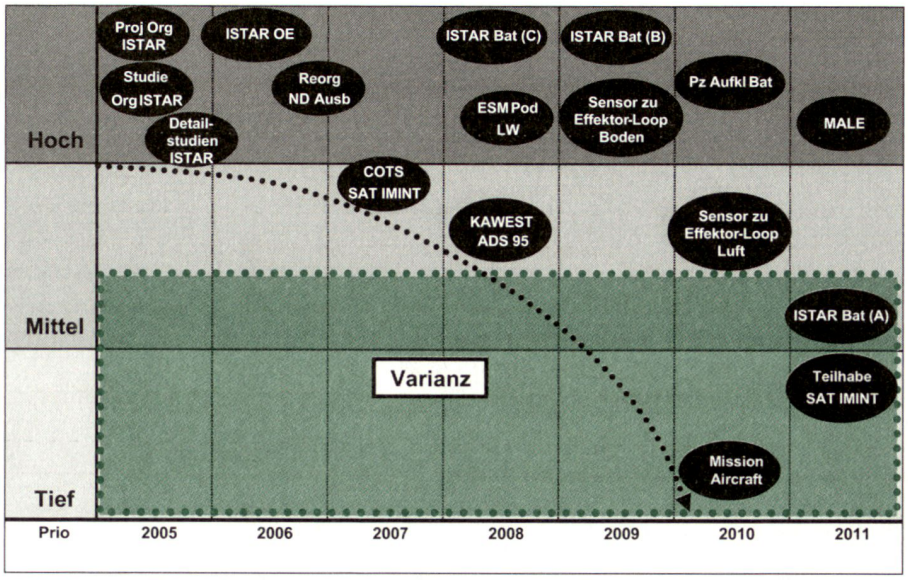


Abbildung 6: Priorisierung/zeitliche Abfolge der ISTAR-Vorhaben, Varianz.

- Schrittweise Erfassung der tatsächlichen Bedürfnisse der Armee in diesem Bereich;
- Ausbildung und Entwicklung der Auswertefähigkeit für durch Satelliten beschaffte Nachrichten.

Der zweite Schritt würde der Kauf einer eigenen Beschaffungsfähigkeit im Bereich der satellitengestützten Bildaufklärung bilden. Dabei könnte eine Konstellation aus einem oder mehreren Kleinsatelliten alleine oder mit einer Partnernation beschafft und betrieben werden, oder die Armee kann sich in ein bestehendes Aufklärungssystem einkaufen.

Der zweite Schritt soll, gegen Ende des Betrachtungszeitraums, aufgrund der Erfahrungen aus dem ersten Schritt, der damit entwickelten Kundenbedürfnisse sowie aufgrund des dann aktuellen Stands der Technik und der Kooperationsmöglichkeiten entschieden und gegebenenfalls weiterverfolgt werden.

Luftgestützte Multisensorplattformen

Die Konzeptionsstudie «Aufklärung» hat ergeben, dass von den untersuchten Systemen das ADS-95 in seiner heutigen Form das am wenigsten geeignete System für die Erfüllung der auf Grundlage der Bild-Nachrichtenbedürfnisse der TSK HEER aufgestellten operationellen Anforderungen ist. Der nächste Ausbauschritt bis 2011 in diesem Bereich bildet daher die Einführung zweier sich ergänzender Multisensorplattformen, die die Schwächen des ADS-95 ausgleichen. Es sind dies eine mittlere Aufklärungsdrohne (Medium Altitude Long Endurance Unmanned Aerial Vehicle [MALE UAV]) und ein luftgestütztes Frühwarn- und Aufklärungsflugzeug (Mission Aircraft [MA]) oder alternativ dazu Aufklärungs-Pods auf Kampfflugzeugen.

Priorisierung und zeitliche Abfolge der Vorhaben, Varianz

Wie der Tabelle *(Abbildung 6)* entnommen werden kann, soll der Aufbau des ISTAR-Systems einerseits im Einklang mit der formulierten Absicht für den Aufbau des zukünftigen ISTAR-Systems der Armee und andererseits abgestützt auf der Wichtigkeit eines Vorhabens für das Gesamtsystem erfolgen.

Die angeführten Jahreszahlen stellen nicht eine Zeitplanung für die Bereitstellung der operationellen Fähigkeiten, sondern eine Abfolge der Beschaffungsschritte im Sinne einer Investitionsplanung (Rüstungsprogramme) dar.

Somit ist klar, dass das System als Ganzes, frühestens im Jahr 2015 einsatzbereit sein dürfte.

Da damit gerechnet werden muss, dass aufgrund von finanzpolitischen Vorgaben das System allenfalls nicht vollständig realisiert werden kann, müssen solche Entwicklungen in die Vorhabenplanung mit einbezogen werden.

Die Varianz liegt dabei nicht in einer grundsätzlich anderen Ausgestaltung des Systems, sondern primär im Verzicht auf die Realisierung von Teilprojekten, welche primär der Schaffung von operativen Aufklärungsfähigkeiten oder Aufklärungskompetenzen dienen.

Operation «MERKUR»: Die deutsche Luftlandung auf Kreta als Prüfstein des neuseeländischen Gefechtsnachrichtendienstes

Die Militärgeschichte als Analyseinstrument für aktuelle Systeme und Innovationen einer modernen Armee ist eine Herausforderung: *Geschichte für die Planung der Zukunft.* Ein dramatisches Beispiel aus dem Zweiten Weltkrieg wird mit C4ISTAR in Verbindung gebracht. Die Studie kommt zur wenig erstaunlichen, aber wichtigen Einsicht: Entscheidend bleibt der Entschluss des Kommandanten.

Hans Rudolf Fuhrer, Adrian Baschung*

Einleitung

Die Kämpfe zwischen den deutschen Luftlandetruppen und den britischen Verteidigern auf Kreta vom 20. bis zum 31. Mai 1941 gehören zu den wohl dramatischsten Ereignissen des ganzen Zweiten Weltkrieges. Auf beiden Seiten wurde unter schweren Verlusten erbittert gefochten. Mit dieser operativen Luftlandung unter dem Decknamen «MERKUR» öffnete die deutsche Luftwaffe ein neues Kapitel in der modernen Kriegführung. Sie diente später als Modell für den Aufbau und Einsatz von Luftlandetruppen bei vielen Armeen. Die deutsche Luftwaffe selbst konnte sich keine derartige Operation während des Krieges mehr leisten, da die Verluste an Mensch und Material auf Kreta enorm waren und weil im weiteren Verlaufe des Krieges die Lufthoheit verloren ging.

> Mit dieser operativen Luftlandung öffnete die deutsche Luftwaffe ein neues Kapitel in der Kriegführung.

Diese grosse Luftlandeoperation im Mittelmeer wollen wir dazu benutzen, um folgende Fragen zu beantworten:

- Wie beeinflussen Meldungen das Lagebild eines Kommandanten im Gefecht?
- Wie beeinflusst das Lagebild die Entschlussfassung eines Kommandanten im Gefecht?

Das System C4ISTAR, welches in dieser Ausgabe bereits vorgestellt wurde, soll am Beispiel Kreta gespiegelt und geprüft werden.

Im Vorfeld dieser Analyse müssen zwei Einschränkungen gemacht werden:

- Die Dimensionen des Luft- und Seekrieges über und um Kreta werden, bis auf die Zusammenfassung des Kampfes, ausgeklammert.
- Der Vorgang der Luftlandung an sich interessiert hier nicht. Der Fokus liegt auf der Seite des neuseeländischen Verteidigers.

*Hans Rudolf Fuhrer, Dozent für Militärgeschichte an der MILAK/ETHZ bis 30. Sept. 2005.

Adrian Baschung, cand. phil. Universität Fribourg; Adrian Baschung hat wesentliche Teile dieser Studie im Rahmen seines dreimonatigen Praktikums an der MILAK/ETHZ erarbeitet.

Der Luftlandeangriff auf Kreta vom 20. bis zum 31. Mai 1941

Ausgangslage

Nach dem Balkanfeldzug (6. April bis 11. Mai 1941) zeichnete sich die strategisch wichtige Lage der Insel Kreta mehr und mehr ab. Das deutsche Oberkommando ging zum einen davon aus, dass mit einer Inbesitznahme der Insel die Transportwege von Griechenland und Afrika nach Italien gesichert und die deutsche Lufthoheit bis an den Suezkanal ausgeweitet werden könnten.[1] Zum anderen hätten von hier aus Möglichkeiten bestanden, die britische Seelinie Gibraltar–Malta–Alexandrien zu stören, um zu verhindern, dass die Insel als Ausgangsbasis für britische Luftoperationen in Richtung der Ölfelder in Rumänien ausgebaut wurde.[2] Diese Ölfelder waren für die deutsche Energieversorgung kriegswichtig. Eine Schwächung der britischen Position im Mittelmeer war daher für die Achsenmächte Italien und Deutschland erstrebenswert.[3] Die Besetzung Kretas durch britische Truppen wollte die deutsche Armeeführung schon am 28. Oktober 1940 mittels einer Landung italienischer Mannschaften vorsorglich verhindern. Dies lehnte Mussolini jedoch ab.[4] Sein strategisches Fiasko beim Angriff auf Griechenland nutzte die britische Führung aus und besetzte am 1. November die Insel.[5]

Der Entscheid, Kreta aufgrund der britischen Seehoheit im Mittelmeer aus der Luft einzunehmen, fiel am 21. April 1941 im Führerhauptquartier. In Griechenland wurden die Vorbereitungen für den Überfall getroffen. Transport- und Landemaschinen wurden bereitgestellt und Luftlandetruppen per Eisenbahn und Lastwagen an die Ausgangspunkte gebracht. Diese aussergewöhnlichen Material- und Mannschaftstransporte wurden vom britischen Nachrichtendienst erkannt.[6] Er schloss daraus, dass Kreta Ziel einer Luftlandung sein würde.

Am 30. April 1941 wurde der bisherige Kommandant der 2. Neuseeländischen Division, General Bernard Freyberg, vom britischen Oberkommandierenden Nahost, General Archibald Wavell, zum Kommandanten auf Kreta ernannt. Sofort wurde mit dem Ausbau der Insel und der Planung der Verteidigung begonnen. Da die Deutschen den Luftraum über Kreta sperrten und die britische Flotte bedrängten, gelangten nur ungenügende Mengen an Material auf die Insel. Zudem waren die Truppen auf der Insel meist schlecht ausgerüstet. Viele Sol-

[1] Schreiber, Gerhard/Stegemann, Bernd/Vogel, Detlef: Das Deutsche Reich und der Zweite Weltkrieg. Der Mittelmeerraum und Südosteuropa, Stuttgart 1984, S. 487. Der Afrika-Feldzug hat dann klar gezeigt, dass Malta als Stützpunkt der Briten für die Kriegführung in diesem Raum entscheidender war als Kreta.

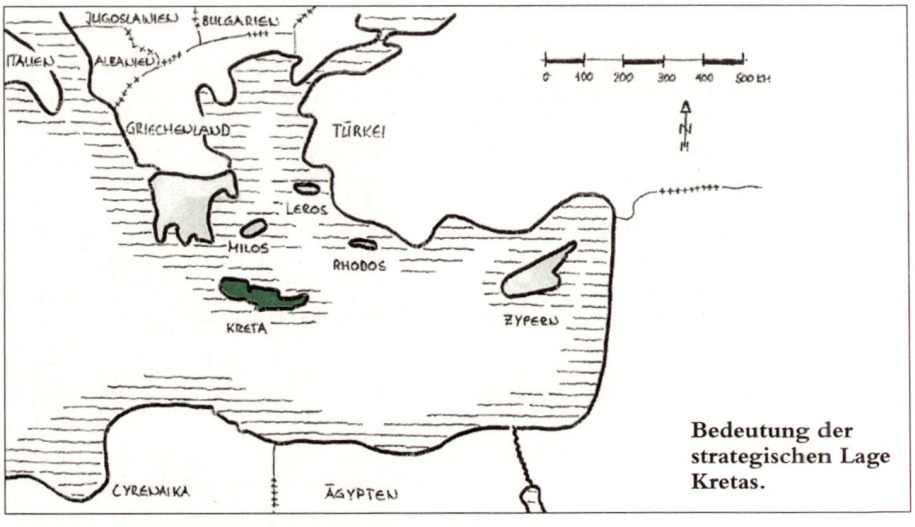
[2] Ebd. S. 485.

[3] Mühleisen, Hans-Otto: Kreta 1941. Das Unternehmen «Merkur». 20. Mai bis 1. Juni 1941, Freiburg i. Br. 1968, S. 10 f.

[4] Schreiber/Stegemann/Vogel, Das Deutsche Reich, S. 485 f.

[5] Ebd. S. 486.

[6] Churchill, Winston Spencer: Der Zweite Weltkrieg. Die Grosse Allianz, Bd. 3, Zürich 1950, S. 323 und Dach, Der Luftlandeangriff, Nr. 8, S. 40.



Bedeutung der strategischen Lage Kretas.

General Bernhard Freyberg
Kommandant der «Creforce», bestehend aus britischen, australischen, neuseeländischen und griechischen Truppen, Freischärlern und Paramilitärs.

Luftwaffengeneral Kurt Student
Oberbefehlshaber des durch Gebirgstruppen verstärkten XI. Luftlandekorps. Er leitete die Operation «MERKUR» von Athen aus.

daten gehörten zum ehemaligen britischen Griechenland-Expeditionsheer, welches sich im April 1941 vor dem deutschen Vormarsch in Griechenland in einer überstürzten Evakuierung nach Kreta retten musste. Dringend benötigtes Material und Waffen blieben dabei auf dem griechischen Festland zurück. Die Gesamtstärke der Inselverteidigung, der «Creforce», belief sich auf 42640 Mann.[7] Diese Streitmacht umfasste britische, australische, neuseeländische und griechische Truppen, zudem eine Anzahl von Freischärlern und Paramilitärs.[8]

Der «Creforce» warf die deutsche Luftwaffe das verstärkte XI. Luftlandekorps entgegen, bestehend aus Luftlande- und Gebirgstruppen, insgesamt 22040[9] Mann. Unterstützt wurden die Luftlandetruppen vom VIII. Fliegerkorps mit Jagd- und Bombereinsätzen. Der Oberbefehlshaber des XI. Luftlandekorps war Luftwaffengeneral Kurt Student. Er leitete die Operation «Merkur» von Athen aus.

Der Angriff

Am Morgen des 20. Mai 1941, um 06.00 Uhr (Die Zeitangaben beruhen auf der englischen Zeit, kontinentale Zeit + 1h), leitete das VIII. Fliegerkorps den Angriff auf Kreta mit je einer dreissigminütigen Bombardierung Malemes, Chaneas, Rethymnons und Heraklions ein.[10] Um 06.50 Uhr belegten Sturzkampfbomber (Stukas) die Absetzstellen und die schweren britischen Geschütze mit punktgenauer Bombardierung. Den Verteidigern wurde spätestens jetzt klar, dass die Invasion bevorstand.[11] Die Fallschirmjäger und Mannschaftsgleiter landeten in zwei Wellen: Die erste Welle setzte um 08.00 Uhr im Sektor Maleme-Chanea auf; die zweite erreichte am Nachmittag die Orte Rethymnon und Heraklion. Da die Gegenwehr der Verteidiger unerwartet stark ausfiel, verlegten die Fallschirmjägerkommandanten die Absetzstellen vom Strand ins Landesinnere und sprangen so zum Teil direkt in die Stellungen der Verteidigungstruppen,[12] was sie einen hohen Blutzoll kostete. Etliche Führungskräfte fielen aus. Dies und die starke Verzettelung der Luftlandetrupps verhinderte in der Folge eine geschlossene Operationsführung. Manches geplante Ziel konnte am ersten Kampftag nicht erreicht werden, beispielsweise die Einnahme der Rollfelder bei Maleme und Rethymnon.[13] Dennoch vermochten deutsche Fallschirmjäger bei der Brücke über den Fluss Tavronitis, westlich des Rollfeldes bei Maleme, und an den übrigen Absetzstellen Widerstandsnester zu bilden. Student beschloss daraufhin, das Schwergewicht auf Maleme zu verlegen, um am wichtigsten Punkt der Insel brachial den Hebel anzusetzen.[14]

Aber auch die Verteidiger hatten mit Problemen zu kämpfen. Verbindungen wurden durch Bombardierung und infanteristischen Beschuss beeinträchtigt, und die Verteilung der feindlichen Kräfte auf das ganze Gelände führte zu Verwirrung und Unübersichtlichkeit. Dennoch hielten die meisten Stellungen trotz des harten Ansturms der deutschen Elitetruppen. Die Landungen bei Rethymnon und Heraklion wurden sogar erfolgreich bekämpft.

Als wohl entscheidende Wende im Kampf um Kreta erwies sich die Aufgabe des wichtigen Kavkazie-Hügels, auch «Höhe 107» genannt, seitens des Neuseeländischen (NZ) Bataillons 22 (Bat 22)

> Als wohl entscheidende Wende im Kampf um Kreta erwies sich die Aufgabe des wichtigen Kavkazie-Hügels, auch «Höhe 107» genannt.

in der Nacht auf den 21. Mai. Dieser Hügel war für die Verteidigung des Schlüsselgeländes Maleme (Rollfeld-Flussübergang-Hauptstrasse) überaus bedeutend, was nicht genügend erkannt worden war. Maleme wurde vom Angreifer in der Folge dazu benutzt, von hier mittels einer Luftbrücke neues Material und Soldaten abzusetzen.[15]

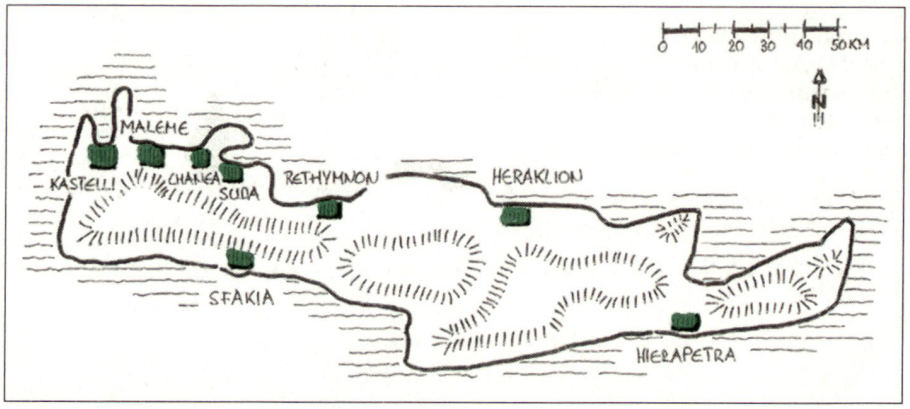
Als die prekäre Lage erkannt worden war, versuchten die Verteidiger, den verlorenen Raum wieder zurückzugewinnen. Bis in die späte Nacht des 21. Mai diskutierten Freyberg und seine Offiziere über die Angriffspläne.[16] Der Gegenangriff wurde am 22. Mai gegen 04.00 Uhr ausgelöst, blieb jedoch bald stecken. Es konnten keine bedeutenden Geländegewinne erzielt werden.[17] Überall auf der Insel konnten sich die deutschen Widerstandsnester behaupten. Somit existierte keine eigentliche Frontlinie.

Die Niederlage

Am 23. Mai zogen die britischen Verteidiger ihre Truppen bis nach Chanea zurück. Die deutschen Fallschirmjäger und Gebirgstruppen stiessen nach und zwangen die «Creforce» zum weiteren Rückzug. Am 25. Mai begannen die britischen Verteidigungslinien zu wanken. Freyberg meldete dies am Abend Wavell nach Kairo. Dieser und die Regierung in London erkannten die Notlage nicht und drängten darauf, dass die Insel gehalten werde. Am 26. Mai um 09.30 Uhr gestand Freyberg die Niederlage ein und meldete an Wavell, dass er eine Evakuierung der Insel einleiten werde.[18]

Die besiegten Verteidiger traten den Marsch an die Südküste an, um sich von dort nach Ägypten einschiffen zu lassen. In der Nacht vom 28. zum 29. Mai nahmen vier britische Zerstörer bei Sfakia über

[7] Mühleisen, Kreta 1941, S. 109.
[8] Baldwin, Hanson W.: Grosse Schlachten des Zweiten Weltkrieges, Düsseldorf/Wien 1968, S. 60.
[9] Mühleisen, Kreta 1941, S. 109.
[10] Dach, Der Luftlandeangriff, Nr. 11, S. 39.
[11] Baldwin, Die grossen Schlachten, S. 71.
[12] Dach, Der Luftlandeangriff, Nr. 11, S. 39.
[13] Mühleisen, Kreta 1941, S. 50.
[14] Baldwin, Die grossen Schlachten, S. 83.
[15] Ebd. S. 87.
[16] Ebd. S. 92.
[17] Ebd. S. 93.
[18] Baldwin, Die grossen Schlachten, S. 100 f.



Angriffseröffnung durch die deutschen Truppen. Die Lage der Absetzstellen. 1. Welle: Maleme–Chanea, 2. Welle: Rethymnon und Heraklion.

1000 Mann an Bord.[19] Die Evakuierung ging schleppend voran. Jedoch konnten bis zum 31. Mai rund 16500 Mann nach Ägypten gerettet werden. Etwa 5000 Mann britischer und Empire-Truppen sowie die griechische Besatzung blieben zurück auf der Insel.[20]

Die Garnison von Rethymnon kämpfte isoliert bis zum 30. Mai und musste anschliessend kapitulieren. Freyberg wurde in der Nacht auf den 31. Mai evakuiert. Auf den Pässen gegen Süden sperrten am 31. Mai noch Nachhuten, doch wurden sie umgangen und zur Aufgabe gezwungen. Die offizielle Kapitulation der «Creforce» beendete den Kampf um Kreta an diesem Tag.[21]

Die Verluste im Kampf um Kreta betrugen:[22]

- Verluste der britischen und Empire-Truppen mit ursprünglichem Bestand von zirka 32000 Mann (RAF, griechische, kretische und sonstige Truppen nicht eingerechnet):

Getötet oder vermisst	1671
Gefangen	1728
Verwundet	11609
Verlustsumme	**15008**

= zirka 47 % Verlust

- Verluste der deutschen Truppen mit ursprünglichem Bestand (nur Landungstruppen) von 22040 Mann:

Getötet	1915
Vermisst	1759
Verwundet	2004
Verlustsumme	**5678**

= zirka 25 % Verlust

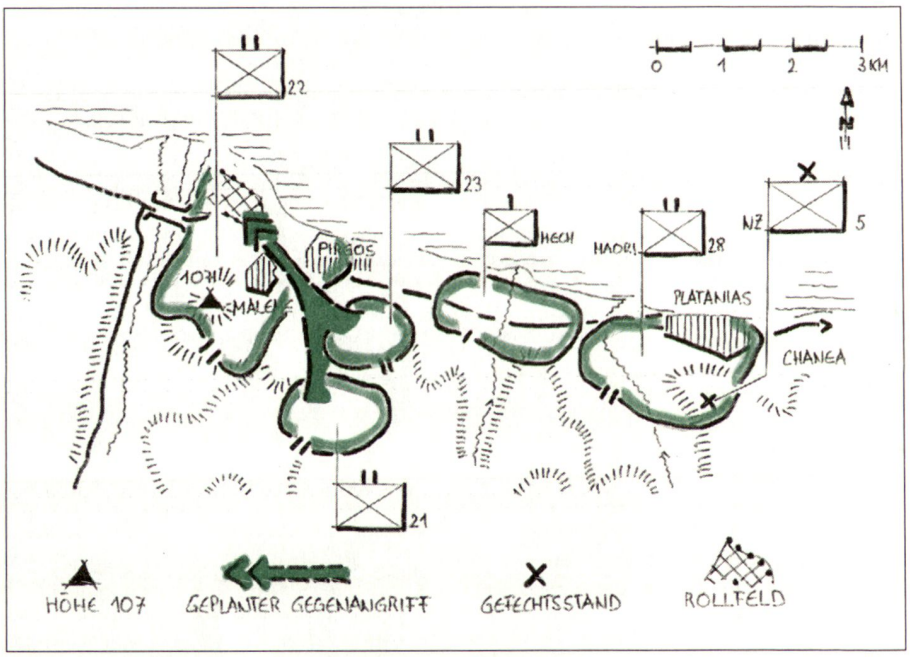
Maleme: Der Kampfraum der 5. Neuseeländischen Brigade

Wir konzentrieren uns nun für unsere nachrichtendienstliche Analyse auf das Schlüsselgelände Maleme – Platanias und wählen dafür den Zeitabschnitt vom 20. bis zum 21. Mai. Die verteidigende Truppe ist die 5. Neuseeländische (NZ) Brigade (Br). Diese Einschränkung hat drei Gründe: Erstens handelt es sich hierbei um ein Schlüsselgelände, zweitens ist die Quellenlage ausreichend, um Lagebeurteilung und Entschlussfassung der Kommandanten im Gefecht nachzuvollziehen. Drittens ist der Zeitrahmen (Intervall vom Beginn der Landung bis zum Entschluss zum Gegenangriff) klar definiert.

Die Organisation der 5. NZ Br

Die 5. NZ Br, geführt von Brigadier James Hargest, unterstand der 2. NZ Division von Brigadier E. Puttick. Die Brigade hatte seit dem 19. Mai folgenden Auftrag:[23]

Einheit	Kommando	Auftrag
5. NZ Br	Brigadier Hargest	• Verteidigt Standort, speziell Rollfeld Maleme • Vernichtet *sofort* luftgelandete gegnerische (gn) Kräfte durch Gegenangriffe • Führt die *aktive* Verteidigung (spirited defence)[24]
Bat 21	Lieutenant-Colonel (Oberstlt) Allen	• Vernichtet luftgelandeten Gegner im Bat-Sektor • Hält sich bereit, Bat 22 durch einen Gegenangriff zu unterstützen
Bat 22	Lieutenant-Colonel Andrew	• Hält Rollfeld Maleme • Hält Höhe 107 • Überwacht Flussübergang Tavronitis
Bat 23	Lieutenant-Colonel Leckie	• Vernichtet luftgelandeten Gegner im Bat-Sektor • Hält sich bereit, Bat 22 durch einen Gegenangriff zu unterstützen
(Maori) Bat 28	Lieutenant-Colonel Dittmer	• Hält Platanias • Schützt Br HQ
Mechaniker Det	–	• Sperrt die Landstrasse zwischen Bat 23 und Bat 28

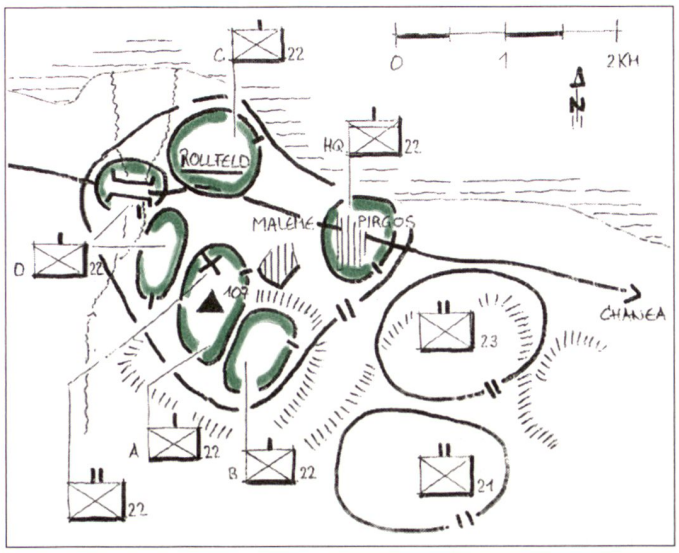


Räumliche Lage der 5. Neuseeländischen Brigade mit dem Gefechtsstand südlich Platanias.

Organisation des Bat 22[25]

Einheit	Kommando	Auftrag
Headquarters Kompanie (HQ-Kp)	Lieutenant (Oblt) Beaven	• Hält Pirgos • Sperrt Strasse nach Chanea
A-Kompanie (A-Kp)	Captain (Hptm) Hanton	• Hält Höhe und Plateau 107
B-Kompanie (B-Kp)	Captain Crarer	• Hält Gebiet östlich der Strasse Maleme–Vlakheronitissa • Hält Strasse Höhe 107-Vlakheronitissa
C-Kompanie (C-Kp)	Captain Johnson	• Hält Rollfeld • Hält Strand nördl. Rollfeld • Hält Ostufer bis Brücke über Tavronitis
D-Kompanie (D-Kp)	Captain Campbell	• Hält Ostufer des Tavronitis • Hält Brücke über Tavronitis
I sMG*-Zug MG-Bat 27	Second-Lieutenant (Lt) Brant	• Deckt Brücke Tavronitis und Teile des Flussbettes • Deckt südl. Teil des Rollfeldes
II sMG-Zug MG-Bat 27	Second-Lieutenant Luxford	• Deckt östl. Teil des Rollfeldes • Deckt Strand nördl. des Rollfeldes

* schwerer Maschinengewehr-Zug



Räumliche Ausgangslage des 22. Bataillons vor Angriffsbeginn mit dem Bataillonsgefechtsstand im Raum der Höhe 107.[26]

Meldefluss und Ereignisse in der 5. Brigade

Der Verlauf des Kampfes und die Kommunikation innerhalb des Verbandes vom 20. bis zum 21. Mai lässt sich in einer tabellarischen Darstellung wie folgt zusammenfassen:

Datum/Zeit	Meldung und Ereignis
20. Mai 1941	Beginn der Luftlandung auf Kreta nach Bombardierung.
08.15 Uhr	Sicht für britische Kommandanten (Kdt) wegen Rauch, Bombardierung usw. schlecht. Führung der Truppen (Trp) erweist sich als schwierig.
09.00 Uhr	Nachricht Freybergs an Wavell nach Kairo: Angriff hat begonnen![27] Bis 09.00 Uhr ist die Verbindung des Bat 22 (Andrew) zur 5. NZ Br (Hargest) nicht unterbrochen.[28] Die Verbindungen zu den Frontkompanien C, D und HQ brechen ab. 09.00 Uhr versucht Andrew, die Lage der D-Kp zu erkunden. Wegen Rauch und Staubwolken ist nichts auszumachen.[29] Eine kleine Gruppe von Fallschirmjägern (Paras) hält ein Haus südlich von Pirgos und unterbindet so den Meldefluss der HQ-Kp zum Bat Stab. Die Telefonverbindung zur 5. Br wird für einige Minuten unterbrochen; die Funkverbindung geht für 1 h verloren. Verbindungen (Telefon, Funk) zum Bat 21 und Bat 23 sind unterbrochen. Kommunikation mit Bat 23 nur mit Meldeläufern und Signalfeuern möglich. Verbindung mit Bat 21 völlig ausgefallen (Bat 21 hat keinen Funk). Bat 23 hat Verbindung (Telefon, Funk) zur 5. NZ Br und Meldeläuferkontakt mit Bat 21.
10.00 Uhr	Funkspruch Andrew an Hargest:[30] Bat 22 steht unter schwerer Attacke.
10.20 Uhr	Andrew beantragt Art Fe Unterstützung.[31]
10.55 Uhr	Funkspruch Andrew an Hargest: Lagebeurteilung: • Landung von etwa 400 Paras, 100 Nähe Rollfeld Maleme, 150 im Osten, 150 westlich des Flusses Tavronitis und an der Küste.[32] • Kontakt mit den Frontkompanien D-, C- und HQ-Kp abgebrochen. Bat steht unter schwerem Feuer.[33] • Anfrage, ob Bat 23 mit der HQ-Kp in Pirgos Kontakt aufnehmen kann.[34] Das Bat 23 schickt eine Patrouille nach Pirgos aus. Diese kann jedoch keinen Kontakt mit der HQ-Kp aufnehmen, da diese auf alle Bewegungen mit Feuer reagiert.
11.55 Uhr	Lagebericht von Leckie, Bat 23, an Hargest: «Situation on my area in complete control. Battalion in high spirits»[35]
12.00 Uhr	Lagebericht Andrew an Hargest: «Battalion being subjected to almost continuous bombing»[36] Kurz nach Mittag berichtet Andrew an die Brigade, dass sein Bat vom Tavronitis her unter Beschuss von leichter Artillerie und unter sMG Feuer stehe. Er vermutet, dass der Feind unter diesem Feuerschutz Gelände Richtung D-Kp gewinnen will.[37]
14.25 Uhr	Hargest an Leckie: «Will not call upon you for counter-attacking unless position very serious. So far everything is in hand and reports from other units satisfactory.»[38] Gegen den frühen Nachmittag trifft Andrew persönlich beim Gefechtsstand des Bat 23 ein. Dieser Umstand wird in keinem Kriegstagebuch erwähnt. Er geht auf die Schilderung von Major Thomason vom Bat 23 zurück, der LtCol Andrew persönlich kannte und ihn zum Bat Kdt weiterleitete. Andrew bittet um Unterstützung bei (Lt) Col Leckie, erhält jedoch keine.[39]
14.55 Uhr	Andrew an Hargest: «Battalion HQ has been penetrated.» Was gemeint ist, ist schwer zu sagen. Jegliche Angriffe auf Hügel 107 wurden bis zu diesem Zeitpunkt zurückgeworfen.[40]
15.55 Uhr	Andrew an Hargest: «Left flank has given way and the need for at least some reinforcement is now urgent.»[41] Bei Barber/Tonkin-Covell steht hier die Zeitangabe von 15.50 Uhr.[42] Gegen 16.00 Uhr (vielleicht auch schon früher) steht der BatStab unter Mörserfeuer aus Richtung des westl. Flussufers. Andrew verlagert den Gefechtsstand um 180 Meter Richtung B-Kp. Zur selben Zeit gliedern sich die Artilleriebeobachter und -offiziere auf dem Hügel 107 in die kämpfende Truppe ein, da sie den Kontakt zu ihren Geschützen völlig verloren haben.[43]
16.30 Uhr	Andrew verlangt bei der 5. Br einen Gegenangriff durch das Bat 23. Dieser Antrag wird abgelehnt.[44]

[19] Ebd. S. 103.
[20] Churchill, Der Zweite Weltkrieg, S. 359.
[21] Baldwin, Die grossen Schlachten, S. 106 f.
[22] Ebd. S. 108 f.
[23] Barber, Laurie/ Tonkin-Covell, John: Freyberg. Churchill's Salamander, Singapur 1989, S. 37 ff. und Stewart, Ian McD. G.: The struggle for Crete. 20 May-1 June 1941, Oxford, 1991, S. 122–129.
[24] Oberstlt i Gst. Mark, W.: Die Eroberung des Flugplatzes Malemes durch Luftlandetruppen. Kreta Mai 1941, In: Allgemeine Schweizerische Militärzeitschrift, 127. Jahrgang, Nr. 11, Frauenfeld 1961, S. 543.
[25] Davin, D. M.: Official History of New Zealand in the Second World War 1993–45. Crete. London 1953, S. 98 f.
[26] Nach Dach, Der Luftlandeangriff, Nr. 8, S. 46.
[27] Macdonald, Callum: The lost Battle. Crete 1941, London 1993, S. 170.
[28] Stewart, Ian McD. G.: The struggle for Crete. 20 May-1 June 1941, Oxford, 1991, S. 167.
[29] Ebd. S. 170.
[30] Ebd. S. 171.
[31] Barber, Laurie/ Tonkin-Covell, John: Freyberg. Churchill's Salamander, Singapur 1989, S. 56.
[32] Stewart, The struggle, S. 167.
[33] Comeau, Marcel G.: Operation Mercury, Somerset 1991, S. 179.
[34] Davin, Official History, S. 108.
[35] Comeau, Operation Mercury, S. 180.
[36] Ebd. S. 180.
[37] Davin, Official History, S. 109.
[38] Comeau, Operation Mercury. S. 180.
[39] Barber/Tonkin-Covell, Freyberg, S. 60.
[40] Comeau, Operation Mercury, S. 182.
[41] Ebd. S. 182.
[42] Barber/Tonkin-Covell, Freyberg, S. 171.
[43] Davin, Official History, S. 109.
[44] Dach, Hans von: Der Luftlandeangriff auf Kreta. Nach deutschen und englischen Kampfberichten, In: Der Schweizer Soldat, Nr. 11, Stäfa 1971, S. 67.

17.00 Uhr	Andrew an Hargest: «When can I expect the pre-arranged counter-attack?» Gegen 17.00 Uhr fordert Andrew Artilleriefeuer zur Unterstützung der sMG-Züge beim Flussbett an. Mittels Signalfeuer versucht er, das Bat 23 zum vorbereiteten Gegenangriff aufzufordern. Eine Antwort oder Hilfestellung erhält er nicht.[45]
17.15 Uhr	Hargest an Andrew: «The 23rd cannot carry out your request because it is itself engaged against paratroops in its area.» Hargest an die Division, jedoch nicht an Andrew: «Am ordering reinforcements to Maleme.»[46] Um 17.15 Uhr wirft Andrew seine zwei Panzer (Pz) und einen eigens zusammengestellten Infanteriezug (InfZug) dem deutschen Widerstandsnest bei der Brücke über den Tavronitis entgegen.[47] Die Paras haben keine schweren Waffen und den Pz somit nichts entgegenzusetzen. Der Gegenangriff scheitert jedoch, da die Pz wegen Pannen liegen bleiben. Der InfZug wird völlig aufgerieben.[48] Cap Johnson der Bat 22/C-Kp erstattet Bericht, dass der Gegenangriff gescheitert sei. Er könne bis zur Dunkelheit die Stellung am Rollfeld halten, müsse jedoch in der Nacht Verstärkung erhalten. 17.50 Uhr antwortet Andrew: «Hold on at all costs!» Johnson kehrt zur C-Kp zurück. Die Verbindung reisst erneut ab.[49]
18.00 Uhr	Andrew an Hargest: «I must withdraw unless reinforcements reach me soon.» Die Forschung geht davon aus, dass er nur einen lokalen Rückzug Richtung B-Kp im Sinn gehabt habe. Antwort Hargest (18.00): «If you must, you must.»[50] Gegen 18.00 Uhr schickt der Kommandant der Bat 23/B-Kp, Cap Gray, einen Meldeläufer zum Bataillonskommando (Bat Kdo). Gray hat von seinem Standort aus eine gute Sicht auf das Rollfeld Maleme und bemerkt die Heftigkeit der Kämpfe. Der Meldeläufer soll nach dem Status des Bat 22 fragen. Die Antwort des Bat Aufklärungsoffiziers ist, dass die Situation auf dem Rollfeld unter Kontrolle sei und noch Säuberungsaktionen liefen.[51]
18.05 Uhr	Hargest an Andrew: «Am sending you two companies, a companie 23rd battalion and b companie 28th (maori) battalion.»[52] Der Bat Stab des Bat 23 meldet der Bat 23/A-Kp unter Cap Watson, dass die Gesamtsituation auf der Insel Kreta klar sei. In einigen Sektoren jedoch sei die Situation «somewhat obscure».[53] Gegen 19.30 Uhr rückt die Bat 23/A-Kp über das Gebiet des Bat 21 zum Bat 22 vor, um dieses zu unterstützen. Andrew hat keine Ahnung, wo und wann die Verstärkung eintreffen wird. Er und seine Offiziere beschliessen zu warten. Als 19.25 Uhr immer noch keine Truppen angekommen sind, setzt er einen Funkspruch zur 5. NZ Br ab, erhält jedoch keine Antwort.[54] Am frühen Abend trifft ein Soldat der D-Kp beim Gefechtsstand des Bat 22 ein und berichtet, er sei der einzige Überlebende seiner Kompanie.[55]
20.30 Uhr	Andrew an Hargest: «I will have to withdraw to b Company ridge.»[56] Andrew erhält keine Antwort vom Brigade-Stab.
21.00 Uhr	Die A-Kp des Bat 23 trifft beim Bat 22 ein. Die B-Kompanie des Bataillons 28 (Maori) ist noch unterwegs. Die frische A-Kompanie wird zur Rückzugsdeckung an den alten Standort Andrews befohlen (Höhe 107). Im Bereich seiner B-Kompanie stellt Andrew fest, dass er ohne die C-, D- und HQ-Kompanie das Schlüsselgelände Rollfeld Maleme – Höhe 107 nicht länger halten kann. Er beschliesst, sich Richtung Bat 23 zurückzuziehen.[57]
22.00 Uhr	Hargest meldet Puttick, dass der Stand der Br «quite satisfactory» sei.[58] Gegen Mitternacht begibt sich Hargest zu Bett.
00.00 Uhr	Mit der A-, B- und der frischen A-Kp vom Bat 23 vollzieht Andrew den Rückzug vom Kavkazie-Hügel (Höhe 107). Das entscheidende Gelände in diesem Abschnitt ist von britischen Soldaten und Waffen geräumt.[59]
21. Mai 1941 01.00 Uhr	Die B-Kp des Bat 28 (Maori) trifft im Dorf Maleme ein.[60]
02.00 Uhr	Das Bat 22 trifft, zum Schock aller, beim 23ten Bat ein.[61] Die Verbindung zur 5. NZ Br ist gestört. Ein Meldeläufer wird entsendet. Der Kavkazie-Hügel liegt nun seit zwei Stunden frei. Cap Campbell, Kdt der Bat 22/D-Kp, bereitet die Evakuierung vor, nachdem er Höhe 107 verlassen vorgefunden hat.[62]
02.30 Uhr	Hargest wird geweckt. Man berichtet ihm, dass der Raum Maleme verloren sei. Dies ist nicht ganz korrekt, denn die D- und C-Kompanie halten zu diesem Zeitpunkt immer noch ihre Stellungen, welche sie bis Einbruch der Dunkelheit verteidigt haben.[63]
03.00 Uhr	Cap Campbell beginnt die D-Kompanie zurückzuziehen. Eine halbe Stunde später zieht sich die HQ-Kompanie aus dem Dorf Pirgos zurück.[64] Um 03.00 Uhr versammeln sich die Bat Kdt Allen (Bat 21), Leckie (Bat 23), Major Philp (Kdt Art Batterie 27) und Andrew zur Lagebesprechung.[65] Ein Gegenangriff, wie er in Freybergs Kampfplan vorgesehen ist, wird nicht eingeleitet. Man will den nächsten Tag über in dieser Verteidigungsstellung bleiben. Laut dem Aufklärungsoffizier Davin vom Bat 23 wäre genügend Zeit gewesen, um die Bataillone neu zu gliedern und sogar noch vor Tagesanbruch einen Gegenschlag Richtung Hügel 107 und Rollbahn zu führen.[66]
03.45 Uhr	Cap Johnson der Bat 22/C-Kp sucht Andrew auf Hügel 107 auf und findet die Stellungen verlassen. Er versucht daraufhin Kontakt mit den anderen Kompanien aufzunehmen.[67]
04.00 Uhr	Hargest erstattet dem Divisions-Kommandeur Puttick Bericht über den Rückzug bei Maleme.[68]
04.15 Uhr	Die C-Kp gibt die Rollbahn auf.[69]
05.00 Uhr	Andrew trifft beim Brigade-Stab in Platanias ein, um Hargest Meldung zu erstatten. Hargest billigt den Entschluss der Bataillons-Kommandeure, kehrt aber nicht mit Andrew zum Bat 23 zurück, sondern schickt Cap Dawson als Stellvertreter mit.[70]
06.00 Uhr	Die HQ-Kp trifft auf die D-Kp und sonstige Truppenteile. Die Kdt bemerken nun, dass Andrews «verlorene» Kompanien noch vorhanden sind.[71]
11.00 Uhr	Dawson meldet Hargest die abgeschlossene Reorganisation der Bataillone.[72]
11.15 Uhr	Puttick meldet Hargest, dass er beabsichtigt, das Bat 28 (Maori) zu entsenden und mit dem Rest der 5. NZ Br einen Gegenschlag am Abend (!) zu führen. Er leitet diese Absicht an Freyberg weiter, welcher diese in einer Lagebesprechung am Nachmittag diskutieren will.[73]
Nachmittag–Abend des 21. Mai 1941	An der Besprechung am Nachmittag des 21. Mai 1941 im Hauptquartier der Creforce in Chanea nehmen neben Freyberg sein Stabschef General Stewart, Brigadier Puttick, Inglis (4. NZ Br) und Vasey (Australische Br) teil. Es wird ein Gegenangriff beschlossen. Dieser soll vom Reserve Bat 20 der 2. NZ Div und dem Bat 28 geführt werden.[74] Der Angriff soll am 22. Mai um 04.00 Uhr ausgelöst werden.[75]

Lagebeurteilungen der Kommandanten

Wenden wir uns nun den Lagebeurteilungen der Kommandanten Andrew (Bat 22), Leckie (Bat 23) und Hargest (5. NZ Br) zu. Um – wie im Gefecht – das Lagebild synoptisch darzustellen, werden die Lagebilder der drei Offiziere in drei Phasen des Kampfes kurz beleuchtet. Die Unterteilung der Lagen ist wie folgt: **Phase I** wird den Beginn der Luftlandung am 20. Mai bis ungefähr Mittag (08.15–12.00 Uhr) umfassen. **Phase II** beinhaltet den Nachmittag und die Lageeinschätzungen zum Zeitpunkt des Rückzuges von Andrew von der Höhe 107 (20. Mai, 12.00 Uhr – 21. Mai, 02.00 Uhr). Der Zeitraum der letzten **Phase III** bedeutet die Stunden 02.30–06.00 Uhr des 21. Mai, als der entscheidende Gegenangriff der Brigade verpasst wird.

Lagebilder von Lieutenant-Colonel Andrew, Kdt Bat 22

Lieutenant-Colonel Andrew, Kdt Bat 22.

Phase I:

Lieutenant-Colonel Andrew hat mit Übersichtsproblemen zu kämpfen, die er als erfahrener Offizier erwartet hat. Nachrichten von seinen Frontkompanien sind nach 09.00 Uhr nicht mehr per Feldtelefon zu erhalten. Die Verbindungen sind aufgrund der Bombardierungen zu der HQ-, C- und D-Kp abgebrochen. Die Kommunikation zu den Bataillonen 21 und 23 bleibt nur noch mittels Meldeläufern und Signalfeuern teilweise aufrecht. Per Funk und Feldtelefon kann Andrew jedoch Verbindung zur Brigade fast durchgehend halten.

Trotz der fehlenden Meldungen kann Andrew in den ersten Stunden des Angriffs ein relativ klares Bild der Lage zeichnen:

Eigene Truppen
- Die Stellungen am Fluss und am Rollfeld halten trotz fehlendem Kontakt (dies war von der Höhe 107 aus grösstenteils zu erkennen).
- Sichtkontakt mit Pirgos ist eher schlecht. Daher wird das Bat 23 zur Kontaktaufnahme als Relais eingespannt.

Gegnerische Truppen
- Die ungefähre Stärke der feindlichen Kräfte und die Konzentrationspunkte sind bekannt (von der Höhe 107 aus gesehen).

Die Situation scheint unter Kontrolle. Andrews Einschätzung der Lage ist also relativ positiv.

Phase II:

Die weiterhin fehlenden Nachrichten und der wachsende Druck durch deutsche Angriffe, teilweise mit schweren Waffen,[76] veranlassen Andrew nach 12.00 Uhr sukzessive zu immer negativeren Einschätzungen der Lage. Dies belegen Funksprüche an den Brigadestab und die verschiedenen vergeblichen Verbindungsaufnahmen mit den übrigen Bataillonen. Da keine Meldungen von den Frontkompanien eintreffen und der Bataillonsgefechtsstand aus dieser Richtung beschossen wird, gewinnt Andrew den Eindruck, dass die Kompanien C und vor allem D am Einbrechen sind. Er beginnt, die Situation des Bataillons als schlecht einzuschätzen. Diese zunehmende Verschlechterung des Lagebildes wird dadurch bezeugt, dass Andrew zuerst nur Verstärkung für die linke Flanke verlangt hat und etwas später versucht, einen Gegenangriff durch das Bat 23 zu erwirken. Er stellt die Begehren bei Lieutenant-Colonel Leckie (Bat 23) selbst und mehrmals bei Brigadier Hargest (5. NZ Br). Jedesmal wird er abgewiesen. Hier kann man einen Wendepunkt in der Lagebeurteilung von Andrew bemerken, nämlich wie folgt:

Eigene Truppen
- HQ-Kp: Den ganzen Tag keine Meldungen. Landungen in diesem Gebiet wurden beobachtet und Andrew glaubt diese Einheit überrannt.
- A-Kp: Intakt
- B-Kp: Intakt; musste jedoch einen Angriff von Süd-Westen abwehren.
- C-Kp: Scheint zu hohe Verluste zu haben, um weiter halten zu können, obwohl sich Cap Johnson um 17.50 Uhr hinsichtlich der Verteidigung zuversichtlich gab.[77]
- D-Kp: Ein Soldat gibt an, der einzige Überlebende zu sein. Zudem wird Bat von dort beschossen. Daher schreibt Andrew auch die D-Kp ab.[78]
- Die Bataillonsreserve ist aufgebraucht und die erwartete Verstärkung durch das Bat 23 taucht nicht wie erwartet schnell genug auf, um sie einzusetzen. Andrew schätzt, mehr als 50% seiner Truppen verloren zu haben.[79]

Gegnerische Truppen
- Der Gegenangriff von 17:15 Uhr wird an der Brücke über den Tavronitis zurückgeschlagen und die Höhe 107 wurde tagsüber von dort beschossen.
- Bat 22 wird von Süd-West (B-Kp) angegriffen.
- Die Dörfer Pirgos und Maleme scheinen in Feindeshand.
- Der Gegner könnte:
- sich im Flussbett parallel zur Höhe 107 und von Pirgos her ungehindert bewegen und versuchen, sein Bataillon einzukreisen.[80] Der Angriff von Süd-Westen und feindliche Truppenbewegungen bei Pirgos deuteten jedenfalls darauf hin.
- die Höhe 107 einnehmen und von da auf die Truppenkonzentration im Gebiet der B-Kp wirken.[81]

[45] Barber/Tonkin-Covell, Freyberg, S. 172.
[46] Comeau, Operation Mercury, S. 182.
[47] Davin, Official History, S.110.
[48] Baldwin, Hanson W.: Grosse Schlachten des Zweiten Weltkrieges, Düsseldorf/Wien 1968, S. 81 f.
[49] Comeau, Operation Mercury, S. 182.
[50] Ebd. S. 183.
[51] Barber/Tonkin-Covell, Freyberg, S. 64.
[52] Comeau, Operation Mercury, S. 183.
[53] Barber/Tonkin-Covell, Freyberg, S. 70.
[54] Ebd. S. 67.
[55] Comeau, Operation Mercury, S. 183.
[56] Barber/Tonkin-Covell, Freyberg, S. 67.
[57] Comeau, Operation Mercury, S. 183 f.
[58] Stewart, The struggle, S. 178.
[59] Comeau, Operation Mercury, S. 184.
[60] Barber/Tonkin-Covell, Freyberg, S. 70.
[61] Ebd. S. 70.
[62] Comeau, Operation Mercury, S. 188.
[63] Ebd. S. 188.
[64] Ebd. S. 189.
[65] Ebd. S. 188.
[66] Davin, Official History, S. 185.
[67] Ebd. S. 189.
[68] Davin, Official History, S. 192.
[69] Ebd. S. 190.
[70] Davin, Official History, S. 186.
[71] Comeau, Operation Mercury, S. 190.
[72] Davin, Official History, S. 186.
[73] Comeau, Operation Mercury, S. 190.
[74] Barber/Tonkin-Covell, Freyberg, S. 81.
[75] Baldwin, Grosse Schlachten, S. 93.
[76] Davin, Official History, S. 109.
[77] Ebd. S. 111.
[78] Comeau, Marcel G.: Operation Mercury, Somerset 1991, S. 183.
[79] Davin, Official History, S. 111.
[80] Barber, Laurie/Tonkin-Covell, John: Freyberg. Churchill's Salamander, Singapur 1989, S. 68.
[81] Ebd. S. 113.

Fallschirmjägereinsatz auf Kreta 1941.

Der lokale Rückzug der A-Kp und des Bataillonsstabes nur in den Bereich der B-Kp erscheint Andrew aus diesen Gründen nicht vorteilhaft. Er erachtet einen weiträumigeren Rückzug als notwendig.

Phase III:

In dieser Phase ist es kaum mehr möglich, das Lagebild von Andrew nachzuzeichnen, da sich an seiner Situation wenig geändert hatte und die Kommandanten der Bataillone nun gemeinsam eine Lagebeurteilung vornahmen. Erst beim Eintreffen der Reste seiner verloren geglaubten Kompanien zeichnete sich ein neues Bild von der Lage seines Bataillons und dem Kampfraum Maleme ab.

In der neuseeländischen Geschichtsschreibung ist man der Meinung, Andrew habe sich, aufgrund des schlechten Zustandes seines Bataillons, nicht zu einem Gegenangriff entschliessen können.[82]

Lagebilder von Lieutenant-Colonel Leckie, Kdt Bat 23

Phase I:

Während des ganzen Tages ist die Beurteilung der Lage des Bat 23 und auch die des Bat 22, von Leckie aus, eine durchwegs positive.

Die Verbindungen mit dem Bat 22 sind seit Beginn des Angriffes zwar auf Meldeläufer und Signalfeuer beschränkt, jedoch können Beobachtungen Richtung Pirgos und Rollfeld Maleme die andauernden Kämpfe und die vermeintlich gute Lage des Bat 22 bestätigen.[83] Ebenfalls führen die erfolgreichen Abwehr- und Säuberungsaktionen des Bat 23 gegen Luftlandeeinheiten (ab 09.00 Uhr)[84] Leckies dazu anzunehmen, es handle sich beim Bat 22 ebenfalls bloss um Bekämpfung und Säuberung des Bataillonsgeländes:

Eigene Truppen
• Kaum Verluste; halten Stellungen.
• Bat 22 kämpft noch, hält aber Stellung
Gegnerische Truppen
• Können sich im Bataillonsraum nicht festsetzen.

Diese Lagebeurteilung spiegelt sich im Funkspruch gegen Mittag an Hargest.

Phase II:

Abgesehen von den Fallschirmjägern am Morgen hat das Bat 23 kaum Feindkontakt und wartet darauf, einen Gegenangriff auslösen zu können. Der Gefechtslärm aus der Richtung des Bat 22 hält zwar an, aber ohne Meldungen von dort kann sich Leckie nur ein beschränktes Bild mittels direkter eigener Beobachtungen machen.[85] Die Meldung vom Brigadehauptquartier um 14.25 Uhr bestätigt seine Auffassung oder vermittelt mindestens ein positives Lagebild über das Bat 22 und den Zustand der 5. NZ Br allgemein.

Selbst die direkten Anfragen von Andrew am Nachmittag und die Signalfeuermeldungen gegen Abend veranlassen Leckie nicht zu einer Änderung seiner positiven Einschätzung der Lage. Bemerkenswert ist hier, abgesehen vom persönlichen Erscheinen Andrews selbst, sicherlich das Ereignis um 18.00 Uhr, als der Meldeläufer der Bat 23/B-Kp nach dem Status des Bat 22 fragt und vom Bataillonsstab des Bat 23 zu hören bekommt, dass alles zum Besten stehe. Dies steht im krassen Gegensatz zur Beobachtung der schweren Kämpfe. Selbst die A-Kp, als Verstärkung zum Bat 22 geschickt, wird vom Bat 23 unzureichend informiert. Die Lage sei im Allgemeinen unter Kontrolle und nur in einigen Sektoren «etwas undeutlich». Leckie verlässt sich also in dieser Phase voll und ganz auf die Beurteilung der Brigade und interpretiert die Lage des Bat 22 von diesem Standpunkt aus als weiterhin nicht Besorgnis erregend.

Phase III:

Wie bei Andrew lässt sich in dieser Phase kein eindeutiges Lagebild Leckies erkennen. Fest steht, dass Leckie die Lage mit seinen Bat Kp Kdt am 21. Mai um 03.00 Uhr in seinem Hauptquartier analysiert hat und sich zu einer umfassenden Reorganisation, nicht aber zu einem Gegenangriff durchringen konnte.[86] Leckie war auch der Auffassung, dass die Höhe 107 und die Rollbahn Maleme verloren seien.

Lagebilder des Brigadier Hargest

Phase I:

Dass der Kontakt zu den Fronttruppen im Gefecht abzubrechen droht, ist bei jedem massiv geführten feindlichen Angriff zu erwarten. Auch Hargest ist auf *Verbindungsausfälle* innerhalb der Brigade gefasst.[87] Bis Mittag sind die Meldungen seiner Bat spärlich, jedoch gesamthaft positiv. Sie sind für den Brigadekommandanten aber aufschlussreich genug, um sich ein Bild der allgemeinen Lage zu machen. Diese Behauptung kann man durch die Tatsache stützen, dass der Brigadestab bei keinem der Bataillone, selbst nach starken Gefechten, Nachfragen zum Status gestellt und sich mit den wenigen Funk- und Telefonmeldungen begnügt hat, welche von der Front nach Platanias gelangt sind. Dass der Raum um das Rollfeld Maleme und die Höhe 107 wegen ihrer wichtigen Lage hart umkämpft sein würden, ist Hargest voll und ganz bewusst. Deshalb hat Freyberg die Stationierung der 5. NZ Br um das Schlüsselgelände persönlich überprüft.[88] Damit hat er allen Führungskräften, inklusive Hargest, die bedeutende Rolle des Einsatzraumes des Bat 22 nahe gelegt.

Die Lagebeurteilungen von Andrew und Leckie führten Hargest um Mittag zur folgenden Beurteilung:

Eigene Truppen
Bat 22:
• Landung von zirka 400 Fallschirmjägern
• Schwere Bombardierung
• Kontakte zu den Frontkompanien abgebrochen; Gegner wird jedoch abgewehrt
Bat 23:
• Landung von Fallschirmjägern im Bat-Raum
• Erfolgreiche Abwehr und Säuberung durch Bat
• Bat ist zum Gegenangriff bereit.
Gegnerische Truppen
Bereich Bat 22:
• Zirka 400 Fallschirmjäger im Raum; werden erfolgreich bekämpft
• Schwere Bombardierungen
Bereich Bat 23:
• Hunderte Fallschirmjäger getötet; Landungstruppen nahezu vernichtet

Die Brigade scheint das Gefecht unter Kontrolle zu haben.

[82] Davin, Official History, S. 185.
[83] Ebd. S. 123.
[84] Stewart, Ian McD. G.: The struggle for Crete. 20 May–1 June 1941, Oxford, 1991, S. 175.
[85] Stewart, The struggle, S. 175.
[86] Davin, Official History, S. 185.
[87] Stewart, The struggle, S. 177.
[88] Barber/Tonkin-Covell, Freyberg, S. 17.
[89] Davin, Official History, S. 135.
[90] Stewart, The struggle, S. 177.
[91] Davin, Official History, S. 135.
[92] Ebd. S. 137.
[93] Davin, Official History, S. 111.

Phase II:

Gegen Nachmittag beginnen sich die Meldungen vom Bat 22 dahingehend zu verdichten, dass der Kampf äusserst hart geführt wird. Während das Bat 23, ohne durch Feindeinwirkung behelligt zu werden, auf den Befehl zum Gegenangriff wartet, versucht Andrew seinen Vorgesetzten fortwährend von der Notlage seines Bataillons zu überzeugen. Er verlangt Artillerieunterstützung, dann infanteristische Verstärkung und schliesslich den vorbereiteten Gegenangriff durch das Bat 23.

Weshalb Hargest durch diese alarmierenden Meldungen nicht sein Lagebild vom Morgen des 20. Mai an den Fortgang des Gefechtes angepasst hat, ist unklar. Betrachtet man die Meldung von 17.15 Uhr, so deutet die Ablehnung des geplanten Gegenangriffs des Bat 23 auf eine klare Fehlbeurteilung der Lage hin. Die offizielle neuseeländische Geschichtsschreibung geht sogar davon aus, dass sich Hargest zu diesem Zeitpunkt über den feindlichen Brückenkopf beim Tavronitis nicht bewusst war.[89]

Die falsche Lagebeurteilung kann jedoch auch auf die frühe Meldung von der Landung von 400 Fallschirmjägern zurückgeführt werden.[90] Da Andrew über keine weiteren Landungen berichtet hat, könnte diese erste Meldung alle weiteren Einschätzungen Hargests dahingehend beeinflusst haben, dass sich Andrew lediglich mit 400 deutschen Elitesoldaten abmühte und somit die Lage des Bataillons in der Hitze des Gefechtes zu übertrieben schlecht beurteilte. Daher schien ihm die Lage nicht als derart bedrohlich, um seine Brigadereserve auszulösen und sie zum Gegenangriff auf Maleme einzusetzen. Hargest hat vor allem mit einer maritimen Landung gerechnet und wollte das Bat 23 als Küstenverteidigungsverband bereit halten.[91] Dennoch scheint es einen kleinen gedanklichen Ruck bei Hargest gegeben zu haben, als er gegen 17.15 Uhr der Division mitteilt, dass er Verstärkung nach Maleme schicken werde. Weshalb er es vermeidet, diesen Umstand Andrew mitzuteilen, bleibt ein Geheimnis.

Erst mit der Meldung Andrews gegen 18.00 Uhr, dass der Gegenangriff des Bataillons 23 misslungen sei, ändert sich die Lagebeurteilung des Brigadiers dahingehend, dass er die Lage beim Bat 22 als «schlecht» beurteilt und eine Verstärkung befiehlt.[92] Mit der Entsendung nur zweier Kompanien, eine noch über eine weite Strecke, zeigt sich erneut ein zu positives Lagebild des Brigadiers. Es lässt sich so zusammenfassen:

Eigene Truppen
Bat 23:
- Status unverändert, gut

Bat 22:
- Harte Kämpfe und Verluste, waren aber eingerechnet und voraussehbar
- Ein Gegenangriff innerhalb des Bat 22 wurde abgeschlagen –> Bat-Reserve vernichtet
- Andrew drängt auf Gegenangriff des Bat 23, noch zuwarten
- Andrew beabsichtigt, sich lokal zurückzuziehen, sieht Lage zu pessimistisch

Gegnerische Truppen
Bereich Bat 22:
- Schwerpunkt bei Maleme-Rollbahn (zirka 400 Fallschirmjäger)
- Vermutlich Brückenkopf beim Fluss Tavronitis gebildet
- Bedrängt Bat 22 mit MG- und Mörserfeuer

Für eine falsche Lagebeurteilung bei Maleme spricht auch die Meldung an die Division gegen 22.00 Uhr, dass die Situation in der Brigade *«quite satisfactory»* sei.

Phase III:

Aufgrund der Nachricht des Meldeläufers des Bat 23, welche Hargest am 21. Mai gegen 02.30 Uhr im Bett erhält, muss er sein Lagebild dem Verlauf der Kämpfe angepasst haben:

Eigene Truppen
Bat 21:
- Am alten Standort

Bat 22:
- Hat sich von der Höhe 107 und dem Rollfeld Maleme zwischen das Bat 21 und 23 zurückgezogen. Der Raum Maleme ist verloren.

Bat 23:
- Am alten Standort

Gegnerische Truppen
- Haben wahrscheinlich wichtige Punkte bei Maleme (Rollfeld/Höhe 107) eingenommen.

Der neueste Bericht von Andrew um 05.00 Uhr und die Meldung der Reorganisation von Bat 22 gegen 11.00 Uhr hat das Lagebild Hargests vollends realistischer gemacht:

Eigene Truppen
Bat 21/22/23:
- Reorganisiert
- Absicht: Halten besetztes Terrain bis Befehl zum Gegenangriff
- Verloren geglaubte Kompanien des Bat 22 (D/HQ) ebenfalls eingetroffen (hätten ohne Rückzugsbefehl wahrscheinlich standgehalten).

Gegnerische Truppen
- Haben die aufgegebenen Positionen des Bat 22 sicher eingenommen.

Kurze Analyse und Wertung der Entschlussfassungen

Die Analyse der Entschlussfassung der drei ausgewählten Kommandanten versucht insbesondere die Bedeutung der Meldungen zu eruieren und deren Einfluss zu werten.

Der Entschluss von Lieutenant-Colonel Andrew, Kdt Bat 22

Analyse

Betrachtet man den Meldefluss innerhalb des Bat 22 und das Lagebild des Kommandanten, so wird sein Entschluss zum Rückzug nachvollziehbar. Er beruht vor allem auf zwei wichtigen Erkenntnissen, die Andrew aus den Meldungen zieht:

1. Ausbleibende Nachrichten von seinen Frontkompanien und der Beschuss der Höhe 107 aus dieser Richtung bedeuten für ihn den Zusammenbruch und Verlust dieser Einheiten.

2. Beobachtete Feindbewegungen deuten auf einen Zangengriff hin, mit dem Ziel, sein Bataillon einzuschliessen und vom Rest der Brigade zu trennen.

Den Kampf konnte Andrew also nur noch weiterführen, wenn entweder ein Gegenangriff zu seinen Gunsten durch das Bat 23 geführt würde oder wenn rechtzeitig Verstärkung einträfe. Ersteres blieb aus, und die Verstärkung kam sehr spät und war zu schwach, um die Front in der Nacht auf den 21. Mai mit frischen Truppen aufzufüllen.

Somit konnte der Rückzug des Bataillons im Schutze der Nacht – erst ins Gebiet der B-Kp, dann zwischen die Bat 21 und 23 – die einzige Rettung der verbleibenden Truppen von Andrew darstellen. Bei einem feindlichen Angriff am nächsten Tag hätte das Bataillon in dieser vermeintlich dezimierten Stärke wahrscheinlich nicht standhalten können.[93]

Der Entschluss erwuchs also grösstenteils aus der Einschätzung der nicht gemeldeten Verluste und der gefährlichen feindlichen Möglichkeit. Beide Einschätzungen waren mangels verlässlicher Frontinformationen verzerrt und teilweise falsch. Obwohl die Drahtverbindungen zur C-, D- und HQ-Kp früh abbrachen und Kontaktversuche mit Meldeläufern aufgrund des feindlichen Feuers unmöglich waren, schafften es einzelne Männer dennoch durchzukommen. Sogar der Kommandant der C-Kp, Captain Johnson, meldete sich am 20. Mai gegen 18.00 Uhr. Johnson ging zurück und suchte gegen 03.45 Uhr erneut Verbindung. Auch Cap Campbell von der D-Kp suchte Kontakt mit dem Bataillonsstab. Da der Hügel jedoch verlassen war, zog er sich mit seiner Kompanie ebenfalls zurück.

Absetzen von Fallschirmjägern.

Wertung

In der fehlerhaften Beurteilung der Lage liegt der hauptsächliche Kritikpunkt an Andrews Entschluss. Er versuchte wohl, Verbindung mit den Fronteinheiten herzustellen, kam aber wegen des Beschusses nicht durch. Das Informationsdefizit verleitete ihn zu einem vorschnellen und verhängnisvollen Rückzug. Vielleicht wäre es besser gewesen, tagsüber zu warten und die Verbindungen mit den «verlorenen» Kompanien in der Nacht zu suchen.[94] Dieses Vorgehen wählten die Kompaniekommandanten C und D und hatten damit Erfolg. Zeit wäre ja noch vorhanden gewesen, da Andrew auf die in Aussicht gestellte Verstärkung wartete.[95] Andrew tat den Schritt der aktiven Verbindungssuche erst nach seiner Entschlussfassung. Am 20. Mai gegen 21.00 Uhr schickte er Meldeläufer zu den Kompanien C, D und HQ, um ihnen den Rückzug des Gefechtsstandes und der A-Kp Richtung B-Kp mitzuteilen.[96]

Denken und Handeln des Kommandanten waren problematisch: Zunächst schreibt er aufgrund fehlender Nachrichten seine Frontkompanien ab, lässt ihnen dann per Meldeläufer ausrichten, er ziehe sich aufgrund ihres Verlustes zurück, anstatt ihren momentanen Status abzuklären und auf dieser Basis seinen Entschluss zu fassen. Daher muss kritisiert werden, dass er das Schlüsselgelände im Brigadenabschnitt aufgab, ohne eine Kontaktaufnahme zur Front in der Nacht versucht zu haben. Seine Lagebeurteilung trug der Situation ungenügend Rechnung, um den Rückzugsentscheid rechtfertigen zu können. Stattdessen verliess er sich völlig auf wage Eindrücke, die er aus Beobachtungen und aus vereinzelten und zum Teil zweifelhaften Meldungen, wie der eines flüchtenden Soldaten der D-Kp, gewann.

Der Entschluss von Lieutenant-Colonel Leckie, Kdt Bat 23

Analyse

Lieutenant-Colonel Leckie stützte sich für seine Entschlussfassung grösstenteils auf die Meldungen der Brigade und auf eigene Beobachtungen.

Der eigene erfolgreiche Kampf gegen die deutschen Fallschirmtruppen könnte ihn darin bestärkt haben anzunehmen, dass Andrew genauso unproblematisch mit dem Gegner in seinem Einsatzraum fertig werden könne. Leckie war, im Gegensatz zu Andrew, in der Lage, sein Bataillon als Ganzes zu führen und konnte bereits früh den Erfolg seiner Gegenangriffe an Hargest melden.

Das Übrige tat wohl der Bericht Brigadier Hargests von 14.25 Uhr, der ihm die Gesamtsituation der Brigade, einschliesslich die Lage des Bat 22, als klar und kontrolliert beschrieb. Also entschloss sich Leckie, den Gegenangriffsbefehl von oben abzuwarten und nicht aus eigener Initiative zu handeln. Daran änderte sich auch nichts, als Andrew persönlich bei ihm auftauchte und um Hilfe ersuchte. Selbst alarmierende Meldungen aus einer seiner Kompanien, dass man gegen Abend immer noch harte Kämpfe beim Rollfeld beobachtet habe, vermochten ihn nicht umzustimmen. Der Entschluss zu warten stand fest.

Wertung

Die Meldungen aus seinem eigenen Bataillon hätten Leckie gegenüber den Meldungen aus dem Brigadehauptquartier bereits etwas misstrauisch machen müssen. Leckie war dem Bat 22 am nächsten stationiert und hatte mit seiner B-Kp einen recht guten Einblick in die Geländekammer des Rollfeldes bei Maleme. Auch das persönliche Vorsprechen Andrews hätte ihn stutzig machen müssen, denn Andrew galt als erfahrener Frontoffizier und verlangte sicher nur aus triftigen Gründen Hilfe.[97]

Dass die vereinbarten und mehrmals eingeübten Meldesignale (Signalfeuer) des Bat 22 vom Bat 23 übersehen wurden, muss wohl der Unübersichtlichkeit des Kampfes zugeschrieben werden. Tragisch war, dass sie beim Zusammenbruch der Telefonverbindungen die einzige Möglichkeit für das Bat 22 waren, beim Bat 23 direkt Verstärkung anzufordern.[98] Innerhalb des eigenen Bataillons war die Verbindung aufrecht geblieben. Das Bat 23 hatte aber am Nachmittag nichts weiter zu tun, als auf den Befehl zum Gegenangriff zu warten. Diese Eventualität eines Gegenangriffs hätte Leckie zu einer aktiveren Nachrichtenbeschaffung bewegen sollen. Da sein Bataillon die Einsatzreserve der Brigade darstellte, wäre es für Leckie sicherlich von Vorteil gewesen, die Situation in seinem sekundären Kampfraum so genau als möglich zu kennen. Die Passivität hatte fatale Folgen.

Die Entschlüsse des Brigadiers Hargest

Analyse

Bei Hargest sollen nur zwei Entschlüsse analysiert werden: Erstens die Verweigerung des Gegenangriffs des Bat 23 zu Gunsten des Bat 22 um 17.15 Uhr und zweitens die Passivität am folgenden Tag um 05.00 Uhr, nachdem er Maleme bereits verloren glaubte.

Es bleibt nicht nachvollziehbar, warum sich Hargest nicht für einen Gegenangriff entscheiden konnte, dies trotz mehrmaligen Antrages von Andrew. Das Bat 23 war gegen Mittag frei, um als Reserve zu Gunsten des Bat 22 eingesetzt zu werden. Daher war die Aussage Hargests um 17.15 Uhr, das Bat 23 könne nicht eingreifen, da es immer noch im Kampf mit Fallschirmjägern stehe, schlicht falsch. Dass Hargest es gleichzeitig unterliess, Andrew mitzuteilen, er werde dennoch Verstärkung schicken, ist ebenso wenig verständlich. Eine solche Ankündigung hätte die Kampfmoral des Bat 22 steigern und Andrew etwas «Luft» zur Beurteilung der Lage verschaffen können.

Um diese Fehlentscheide nachvollziehen zu können, müssen die Lagebeurteilungen Hargests näher betrachtet werden. Erstens erwartete er einen harten Kampf um das Rollfeld bei Maleme und wollte nicht zu früh reagieren und seine Reserve nicht vorschnell aus der Hand geben. Zudem befürchtete er eine amphibische Landung im Anschluss an die Luftlandung. Zweitens lagen ihm keine Meldungen über weitere Luftlandungen bei Maleme vor. Die ungefähr 400 Fallschirmjäger sollten also kein unlösbares Problem für einen erfahrenen Offizier wie Andrew darstellen.

---

[94] Stewart, The struggle, S. 170 f.

[95] Macdonald, Callum: The lost Battle. Crete 1941, London 1993, S. 200.

[96] Davin, Official History, S. 111.

[97] Andrew wurde 1917 mit dem Victoria-Cross ausgezeichnet und war mit seiner «orthodoxen» Kampfidee für einen Verteidigungskampf aus einer befestigten Stellung heraus, wie er bei Maleme geschlagen werden sollte, bestens geeignet (Stewart, The struggle, S. 125). Er wird ebenfalls als ein «*hardbitten professional*» beschrieben, der bei seinem Gang durch alle Grade viele Erfahrungen sammeln konnte (Macdonald, The lost Battle, S. 258).

[98] Davin, Official History, S. 66.

Drittens setzte das Bat 23 bei seiner Feindberührung den deutschen Truppen derart hart zu, dass diese in deren Abschnitt nahezu vernichtet wurden. Weshalb sollte das Bat 22 mit einer noch besseren Ausgangslage hinsichtlich Bewaffnung, Geländeverstärkungen und Führung also solche Schwierigkeiten haben? Warum sollte er in dieser Situation die Brigadereserve bereits auslösen?

Wertung

Spätestens bei der Meldung gegen 18.00 Uhr, als der Gegenangriff des Bat 22 zurückgeschlagen worden war, wäre eine Reaktion seitens des Brigadekommandanten zu erwarten gewesen. Sein Lagebild beruhte jedoch auf zu wenigen und zu alten Meldungen, um situationsgerecht reagieren zu können. Diese veranlassten ihn sogar, den Status des Schlüsselgeländes Maleme als *«quite satisfactory»* zu bezeichnen. Fachkreise sind sich heute in einem Punkt einig: Um in diesem Moment des Kampfes ein Lagebild des bedrängten Bat 22 zu beschaffen, hätte sich Hargest selbst an die Front begeben müssen.[99] Die meisten kritisieren auch den Umstand, dass sich Hargest am 21. Mai der passiven Haltung seiner Bataillonskommandanten anschloss. Dies war eine klare Missachtung seiner eigenen Kampfabsicht und der Richtlinien zur Verteidigung von Freyberg: Luftlandetruppen sollten sofort und selbstständig durch Gegenangriffe vernichtet werden.[100] Betrachtet man die Auswirkungen dieser passiven Haltung auf den Abwehrkampf der Brigade, so kann von einer Katastrophe gesprochen werden.

Vergleich mit C4ISTAR

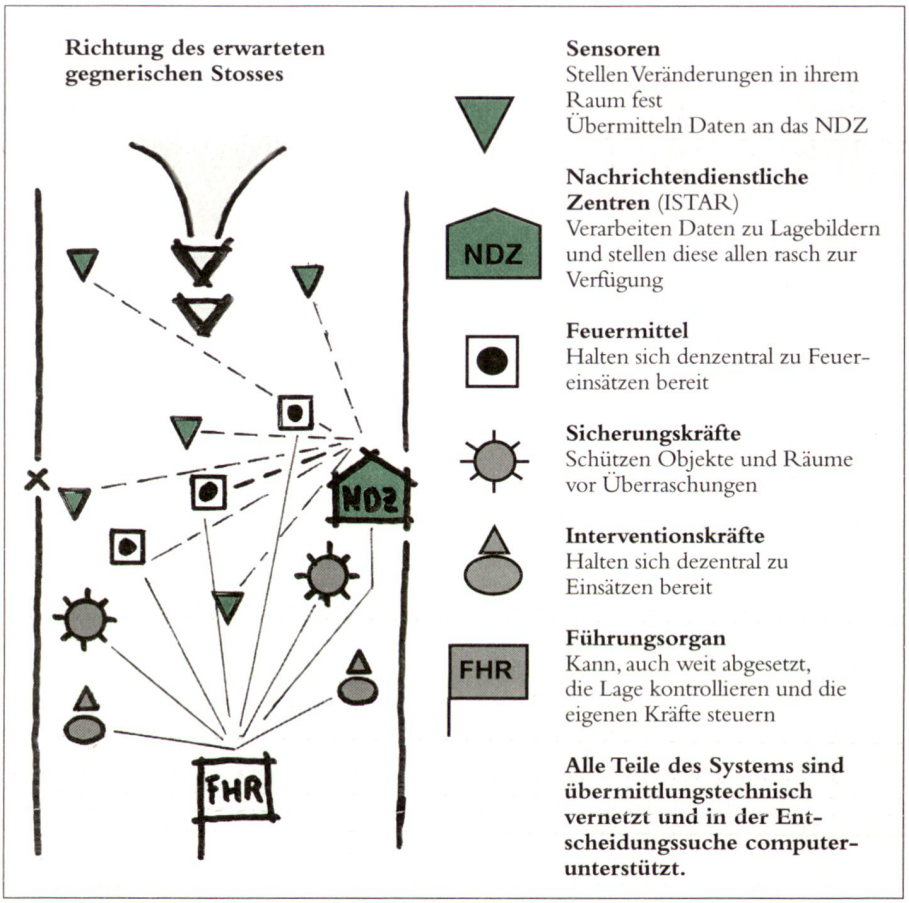
Wie könnten nun die Konsequenzen, die *«lessons identified»*, aus diesem historischen Beispiel für das Kommunikationssystem C4ISTAR lauten?

Vorerst müssen jedoch die Voraussetzungen geschaffen werden, um nicht Unvergleichliches zu vergleichen.

Die Unterschiede zwischen den Möglichkeiten der Truppen im Modell des C4ISTAR und denen auf Kreta 1941 liegen auf der Hand:

	C4ISTAR	Kreta
	(modern: Brigade)	Luftlanderegiment[101]
Gegner	Bewaffnung und Mechanisierung auf höchstem Niveau	Kaum schwere Waffen und mechanisierte Truppen
	Zentral geführt	Versprengte Einheiten
Eigene	Ausreichende Bewaffnung und Mechanisierung	Bewaffnung und Mechanisierung nicht ausreichend[102]
	Kommunikation ausgebaut	Kaum Kommunikationsmöglichkeiten
	Verteidigung dynamisch	Verteidigung weit gehend statisch

Abgesehen von den evidenten Unterschieden können in einem ersten Schritt verschiedene Parallelen hergestellt werden, welche die Ereignisse auf Kreta zwischen dem 20. und 21. Mai 1941 und dem modernen C4ISTAR-System in Verbindung bringen können. Dazu werden folgende schematische Voraussetzungen geschaffen:



Vereinfachte schematische Darstellung C4ISTAR-System.

[99] Davin, Official History, S. 137 und Stewart, The struggle, S. 178.

[100] Barber/Tonkin-Covell, Freyberg, S. 73 f.

[101] Franz Kurowski nennt die Zahl von 1860 Fallschirmjägern, welche im Maleme-Sektor landeten (Kurowski, Franz: Sprung in die Hölle, S. 256.) Stewart übernimmt diese Zahl, vermerkt jedoch, dass noch etwa 300 Mann hinzugezählt werden müssten, da die Lastensegler-Einheiten nicht mitgezählt wurden (Stewart, The struggle, S. 161).

[102] Die Ausrüstung der Artillerie war auf britischer Seite mangelhaft und deren Führung kompliziert, da die Feuerkompetenzen kompliziert delegiert waren. (Dach, Der Luftlandeangriff, Nr. 8, S. 45).

1. Die stationären Frontkompanien (A–HQ) des Bat 22 nehmen im *Modell Kreta* die Funktion der Sensoren wahr.

2. Die Funktion der NDZ (Nachrichtendienstliche Zentren) wird auf den Bataillonsstab des Bat 22 übertragen. Dieser empfängt, filtert und meldet die Nachrichten an die Brigade (5. NZ) weiter, die hier das Führungsorgan ist. Wie beim C41 kann das Bataillon direkt Artilleriefeuer leiten, mittels der bei ihm stationierten Artillerieoffiziere und Minenwerferbeobachter auf der Höhe 107. Die zentrale Feuerleitung durch den obersten Kdt (FHR. 5. NZ Br) ist auch vorgesehen.

3. Die Auslösung der Reserveeinheiten, ist im Modell Kreta an Bat 21 und Bat 23 delegiert.

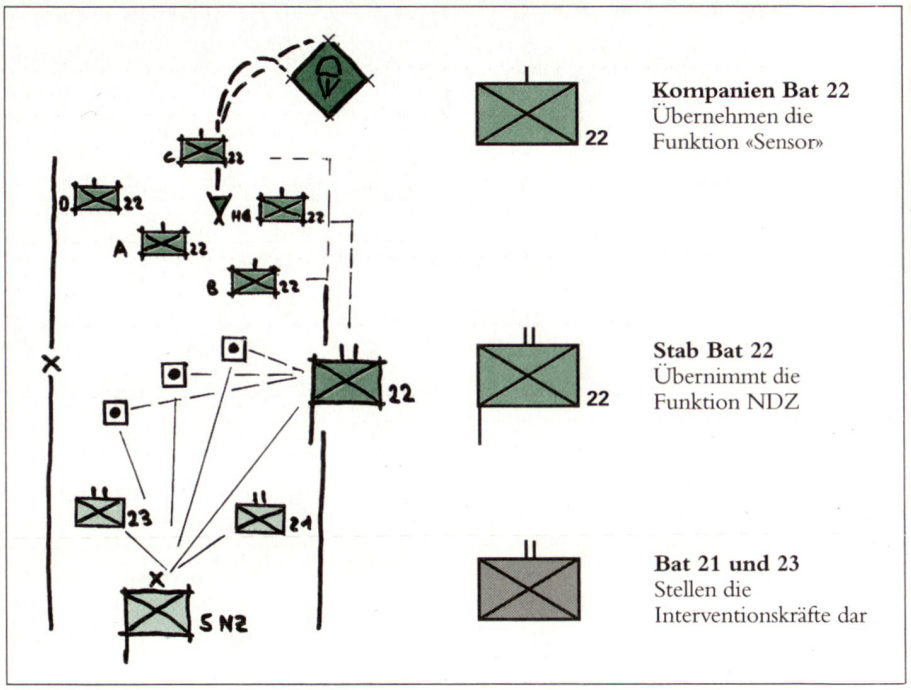
Systemerprobung mit Gefechtsbeispiel Maleme

Das Beispiel Kreta eignet sich also, um die Problematik an einer Gefechtssituation zu überprüfen, in welcher der Meldefluss schleppend und unzureichend läuft, dennoch Schlüsselmeldungen enthält.

Dies sind die Basissätze bei dieser Systemprobe:

- Die Verbindungen der Sensoren (Front-Kp) zum NDZ (Bat 22) sind wegen massiver Feindeinwirkung gestört (A).
- Nur ein vages, jedoch anfangs positives Lagebild wird durch das NDZ (Bat 22) an das FHR (Hargest) weitergegeben (B).
- Dieses Lagebild des NDZ wird wegen fehlender Verbindung zu den Sensoren zunehmend negativ (C).
- Welchen Entschluss trifft das Führungsorgan (D)?

Wie oben beschrieben, stützten sich die Kommandanten Andrew, Leckie und Hargest zum grössten Teil auf Meldungen, die unzureichend überprüft oder schon veraltet waren. Besonders auf Stufe Brigade gelangen Nachrichten vom Bat 22 (NDZ) zu Hargest (FHR), welche zwar spärlich sind, jedoch die Lage im Kampfgebiet als zunehmend prekär beschreiben. In der Folge hält das FHR an einem veralteten Lagebild fest, das nicht den laufenden Meldungen angepasst wird. Das Lagebild Hargests, das selbst in den alarmierenden Berichten Andrews keinen Anlass zu einem sofortigen Gegenstoss findet, hat für die ganze Inselverteidigung fatale Folgen. **Also lag der Misserfolg des Kampfes bei Maleme nicht nur bei der schlechten Kommunikation, sondern vor allem bei der fragwürdigen Interpretation der Meldungen und Fakten durch die verantwortliche «Führungsstufe» Brigade.**

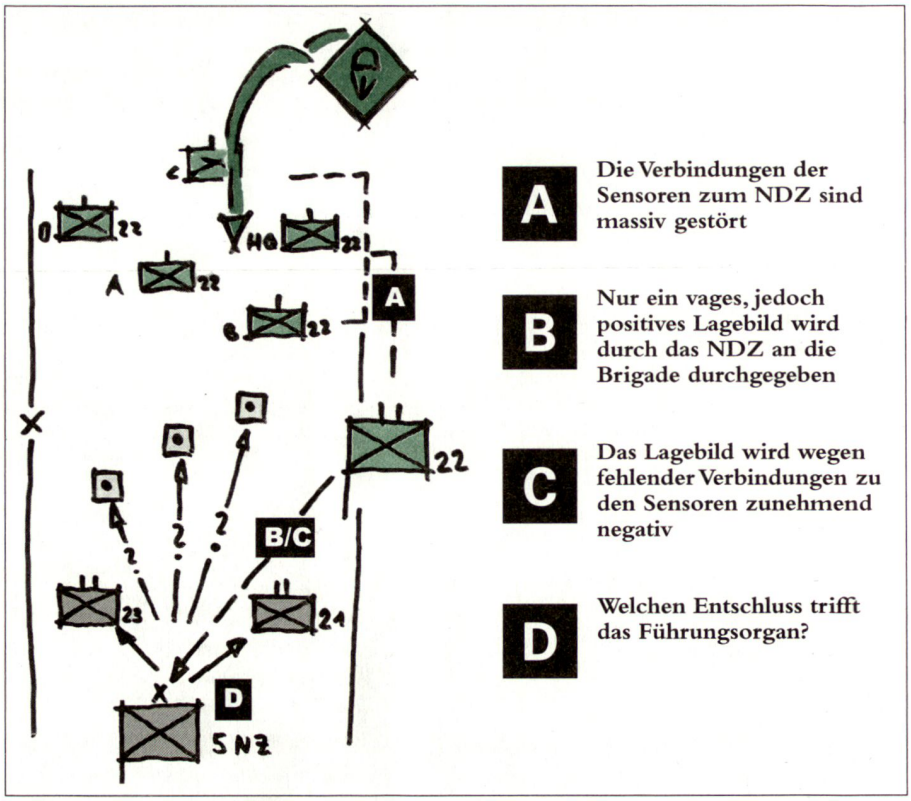


«C4ISTAR»-Modell Kreta.

Folgerungen aus der Systemprobe C4ISTAR-Kreta

Erst wenn man mit einem Gefechtsbeispiel ein solches Szenario auf der Basis eines modernen Kommunikationssystems, wie das C4ISTAR, durchspielt, lassen sich die wichtigen und entscheidenden Stellen in einem System aufzeigen.

Nachrichten sind ohne Zweifel von zentraler Natur. Das wurde am historischen Beispiel der Lage der 5. NZ Br bei Maleme am 20. und 21. Mai verdeutlicht. Die Verbindungen zwischen den Bataillonen und der Brigade waren dürftig, die Kommunikation unter den Bataillonen schlecht und innerhalb des Bat 22 katastrophal. Die Kommandeure waren auf kontinuierliche Meldungen von der Front angewiesen, um sich einen Überblick zu verschaffen. Dieser Mangel an Informationen führte zu Fehleinschätzungen und Zerrbildern, die schliesslich zu riskanten Entschlüssen führten. Besonders eindrucksvoll



Basissätze der Systemprobe.

zeigt sich diese fatale Aneinanderreihung von Ereignissen bei Andrew, welcher sich zu einem, für die ganze Inselverteidigung, folgenreichen Rückzug durchrang und wichtiges Gelände im Rahmen der Kampfführung preisgab. Daher ist für die Führung im Gefecht eine ausgebaute Kommunikation elementar.

Der Mangel an Informationen war jedoch nur zum Teil für die Niederlage in diesem Kampfsektor mit verantwortlich. Entscheidenden Einfluss auf das Gefecht hatte erstens die richtige Beurteilung der Lage durch die Kommandanten, im Sinne des Verdichtens von Informationen und Fakten zu Erkenntnissen und zweitens deren Entschlussfassung, welche aus der konsolidierten Lagebeurteilung resultieren sollte.[103] Geht man nach dem Führungsrhythmus, so steht man bei der Sammlung von Informationen lediglich am Anfang des Prozesses der Führungstätigkeiten, der von der Problemerfassung über die Lagebeurteilung, Entschlussfassung, Planentwicklung und Befehlsgebung führt.[104]

Hierzu sind anschauliche Beispiele im Sektor der 5. NZ Br zu finden. Einerseits haben wir Leckie vom Bat 23, welcher dringende Meldungen und alarmierende Beobachtungen aus der Richtung des Bat 22 mit einem Bericht von der Brigade aufhob und die Lage an der Front wie auch die persönliche Stellungnahme von Andrew falsch einschätzte. Weitreichender waren die Konsequenzen bei den Entschlüssen Hargests, der sich von negativen Frontmeldungen zu keiner Reaktion gezwungen fühlte, sei dies in Form persönlicher Präsenz an der Front oder in Form eines im Voraus geplanten und von Freyberg indirekt in den Handlungsrichtlinien befohlenen Gegenangriffes.

Schlusswort

Wie eingangs erwähnt, hat sich die Militärgeschichte als Analyseinstrument für aktuelle Fragen als tauglich erwiesen. Es ist daher vorstellbar, dass diese Anwendung auch in Zukunft zu Hilfe gezogen werden kann.

Die vorliegende Analyse hat gezeigt, dass ein hoher oder tiefer Rhythmus im Nachrichtenfluss sowie gute oder schlechte Qualität der Meldungen nicht die ausschlaggebenden Faktoren im Kampf auf Kreta gewesen sind. Entschieden haben schliesslich Köpfe. Diese intellektuelle oder intuitive Leistung wird dem Kommandanten auch in Zukunft von einem modernen System wie dem C4ISTAR nicht abgenommen werden.

Jedes Kommunikationssystem – auch das Sprachlabor – kann nur unterstützende Leistungen erbringen. Kann man also darauf verzichten? Diese Entscheidung steht noch aus. Notsituationen verlangen Prioritäten. Korpskommandant Fritz Prisi 1946 hat anlässlich der Diskussion um die angeblich fehlenden Operationspläne der Schweizer Armee bei Beginn des Zweiten Weltkrieges gesagt:

«Wenn ich die Wahl habe, dann investiere ich in Köpfe und nicht in Schubladen!»

Wie so oft heisst wohl die Lösung: sowohl als auch.

Literaturangaben

Baldwin, Hanson W.: Grosse Schlachten des Zweiten Weltkrieges, Düsseldorf/Wien 1968.

Barber, Laurie/ Tonkin-Covell, John: Freyberg. Churchill's Salamander, Singapur 1989.

Churchill, Winston Spencer: Der Zweite Weltkrieg. Die Grosse Allianz, Bd. 3, München/Zürich 1961.

Comeau, Marcel G.: Operation Mercury, Somerset 1991.

Dach, Hans von: Der Luftlandeangriff auf Kreta. Nach deutschen und englischen Kampfberichten, In: Der Schweizer Soldat, Nr. 8, Stäfa 1971.

Dach, Hans von: Der Luftlandeangriff auf Kreta. Nach deutschen und englischen Kampfberichten, In: Der Schweizer Soldat, Nr. 11, Stäfa 1971.

Davin, D. M.: Official History of New Zealand in the Second World War 1993–45. Crete. London 1953.

Hillgruber, Andreas/Hümmelchen, Gerhard: Chronik des Zweiten Weltkrieges. Kalendarium militärischer und politischer Ereignisse 1939–45, Düsseldorf/Regensburg 1978.

Kurowski, Franz: Sprung in die Hölle Kreta. Fallschirmjäger und Gebirgstruppen erobern eine Insel, Bayreuth 2001.

Macdonald, Callum: The lost Battle. Crete 1941, London 1993.

MILVOC-II: Wörterbuch militärischer Begriffe. Deutsch-Englisch, Zürich 1996.

Mühleisen, Hans-Otto: Kreta 1941. Das Unternehmen «Merkur». 20. Mai bis 1. Juni 1941, Freiburg i. Br. 1968.

Oberstlt. i. Gst. Mark, W.: Die Eroberung des Flugplatzes Malemes durch Luftlandetruppen. Kreta Mai 1941, In: Allgemeine Schweizerische Militärzeitschrift, 127. Jahrgang, Nr. 11, Frauenfeld 1961.

Reglement 51.20 d: Taktische Führung XXI (TF XXI), Schweizerische Armee, gültig ab 1.1. 2004.

Reglement 52.2/III: Symbole und taktische Zeichen, Schweizerische Armee, gültig ab 1.1.2002.

Schreiber, Gerhard/Stegemann, Bernd/Vogel, Detlef: Das Deutsche Reich und der Zweite Weltkrieg. Der Mittelmeerraum und Südosteuropa, Stuttgart 1984.

Schreiber, Gerhard: Der Zweite Weltkrieg, München 2002.

Stewart, Ian McD. G.: The struggle for Crete. 20 May-1 June 1941, Oxford 1991.

Internetadressen:

http://Library.kent.ac.uk/cartoons/collections/database.php [Stand 9.9.05].

http://www.nzetc.org/etexts/WH2-22Ba/WH2-22BaP009b.jpg [Stand 9.9.05].

http://www.bruisvat.nl/nummer8/kreta%201941.gif [Stand 9.9.05].

[103] Reglement 51.20 d: Taktische Führung XXI (TF XXI), Schweizerische Armee, gültig ab 1.1. 2004, S. 62 und 65.

[104] TF XXI, S. 58 ff.