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

Autor(en): **Moschin, Andreas**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **171 (2005)**

Heft 12

PDF erstellt am: **28.03.2024**

Persistenter Link: https://doi.org/10.5169/seals-69955

Nutzungsbedingungen

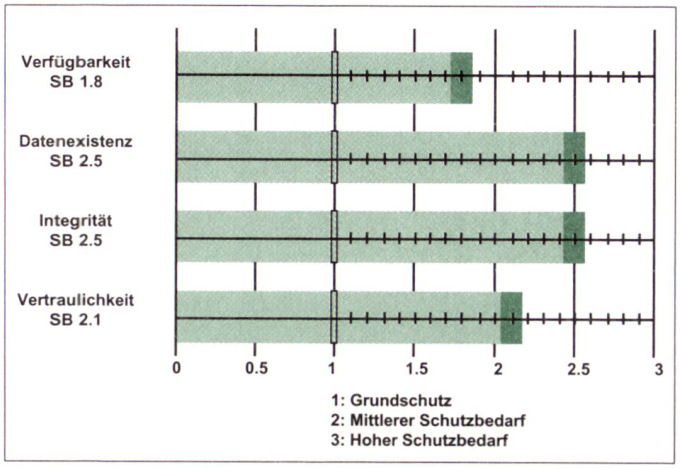
Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch



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.

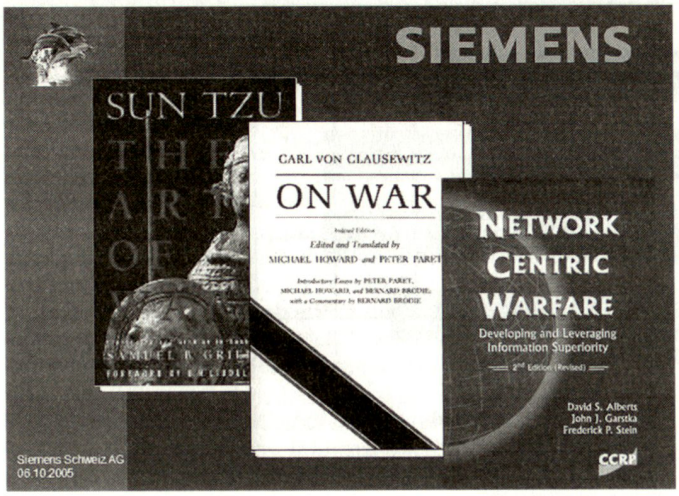
Die Wirtschaft hat den Nutzen der globalen Vernetzung längst erkannt. Sie setzt diese Erkenntnis auch um. Informationsmanagementsysteme ermöglichen die globale Verbreitung und Nutzung von Informationen. In multinationalen Unternehmen ist das «state of the art». In technologischer Hinsicht bringt der 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.

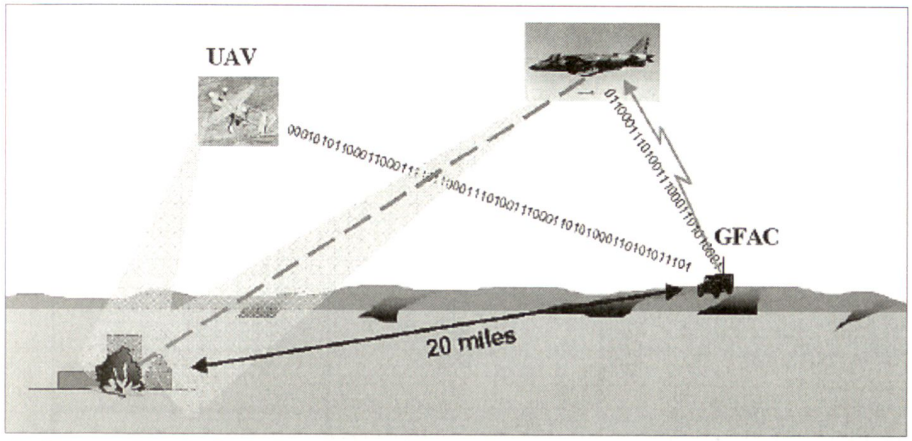
[3] Lionel Giles, «Sun Tzu die Kunst des Krieges.» Droemersche Verlagsanstalt, 1988.

[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

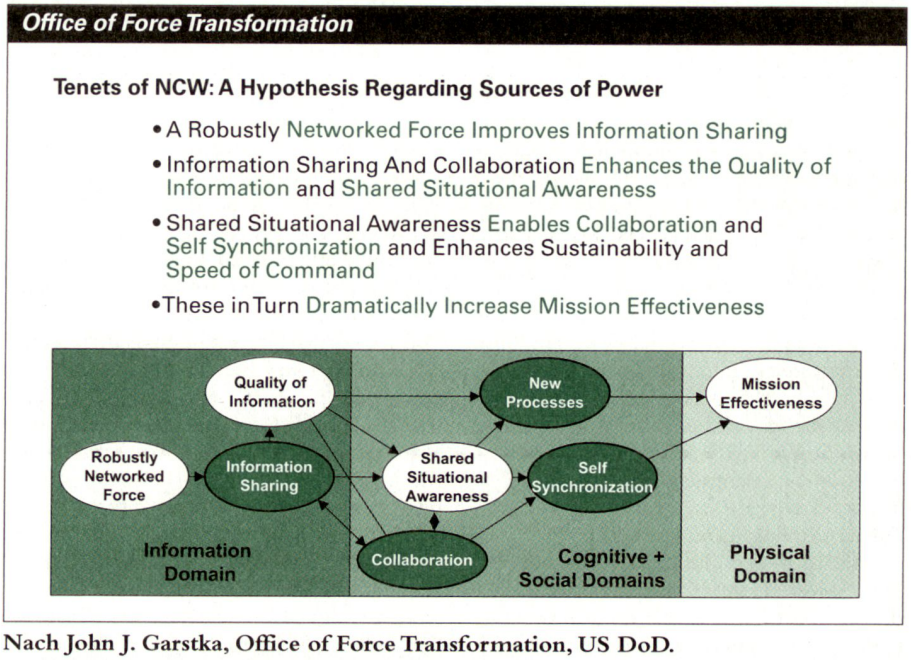
Office of Force Transformation, US DoD

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:

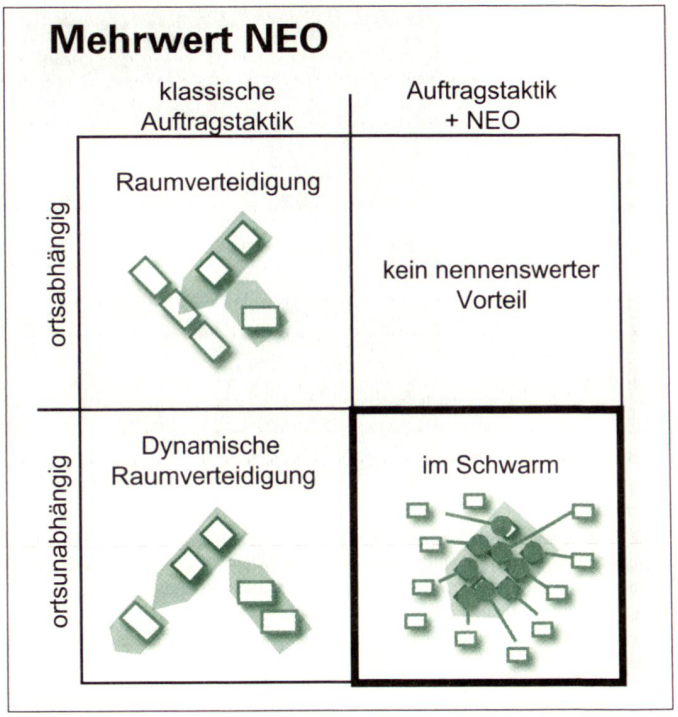
- **«Dominant Manouver»** (überlegene Bewegung): durch überlegene Geschwindigkeit und Beweglichkeit sowie der Fähigkeit, das Feuer von weit dezentralisierten Effektoren (land-, luft-, seegestützt, auch special operations forces) zu konzentrieren bzw. zu skalieren, wird Überlegenheit im Manöver erreicht.
- **«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.

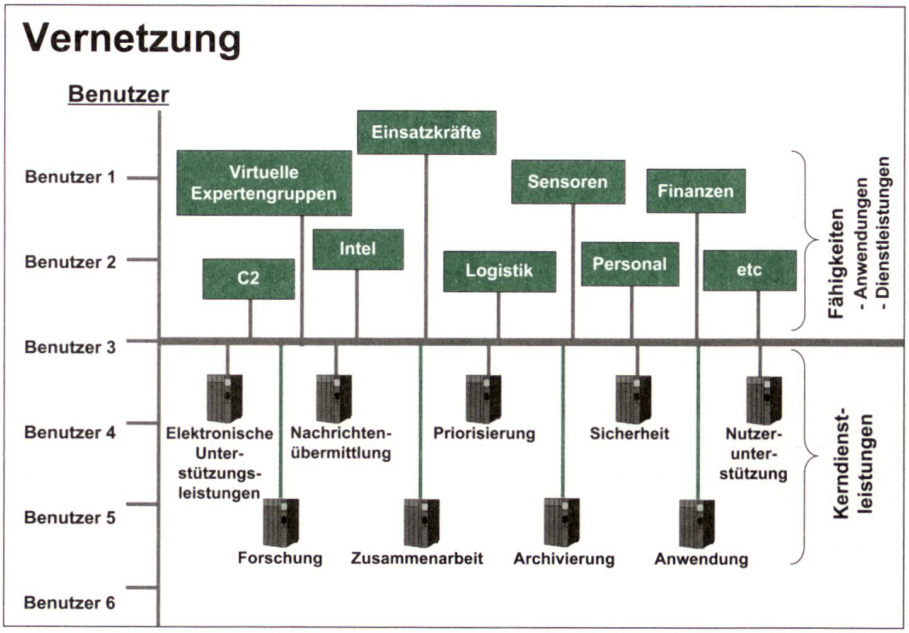
[10] Sebastian Schäfer. «Vernetzte Operationsführung».

[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. ●