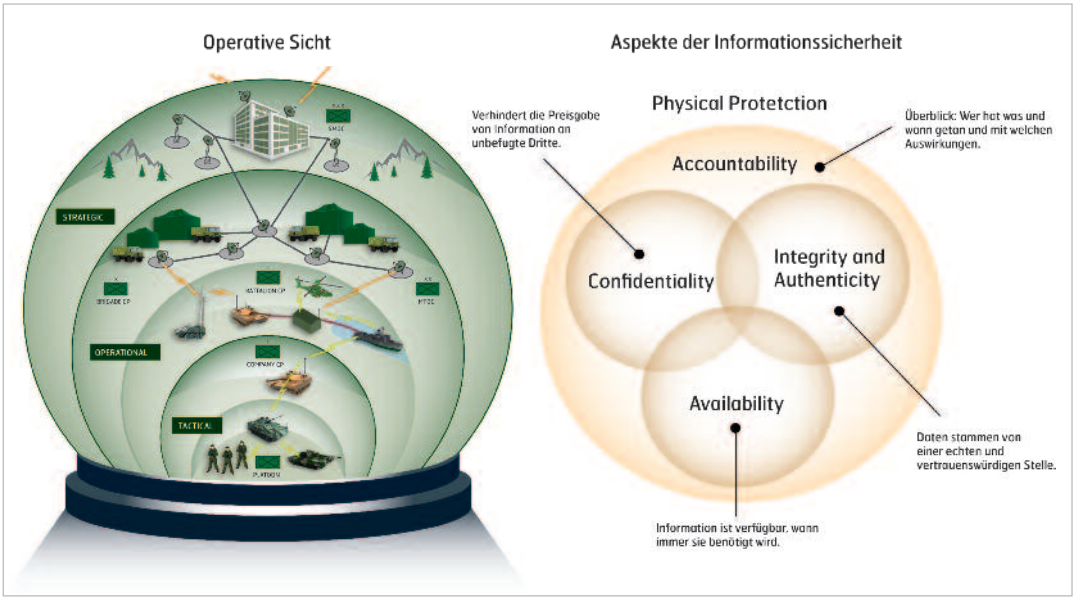
Gesicherte Information als Schlüsselgut vernetzter Einsatzführung

Moderne Streitkräfte passen sich den vermehrt asymmetrischen Bedrohungen an: Die strikte Aufteilung militärischer Verbände nach Räumen und Aufträgen weicht zugunsten operationsbezogener Einsatzverbände auf dynamisierten Gefechtsfeldern. Was ein Quantensprung in der Vernetzung von Führung und Kommunikation erst ermöglicht hat, birgt jedoch Risiken.

Jahn Koch

Teilstreitkräfte-übergreifende, effektbasierte Operationen, chirurgisch präzise ausgeführt in Ausnutzung maximaler Informationsüberlegenheit: Das verspricht der Einsatz moderner Führungsinformationssysteme unter dem Titel C4I. Die Königsklasse breiter militärischer Operationen ist angewiesen auf ein robustes Einsatznetzwerk mit erstklassigen Applikationen. Das Zeitalter des «Network Centric Warfare» (NCW) bietet zahlreiche Chancen, aber auch massive Sicherheitsrisiken von der Ebene des taktischen Erfolgs bis hin zu jener der internationalen Reputation. NCW ermöglicht durchgängige Kommandostrukturen und die Fähigkeit, den Einsatz «live vor Ort» auf allen Stufen darzustellen, zu steuern und zu unterstützen. Im Zentrum steht dabei das aus zahlreichen Sensordaten aufbereitete Lagebild (Common Operational Picture) – die Basis aller wesentlichen Einsatzentscheide und Anweisungen an den Verbund von Effektoren (Waffensystemen).



Durchgängiger Schutz für Einsatznetze: Die verschiedenen Aspekte der logischen Informationssicherheit. Grafik: Crypto AG

Gefahren lauern beim ungenügenden Informationsschutz

Kommunikation und ungehinderter Informationsaustausch sind das Schlüsselelement für NCW, aus dem früheren «need to know» hat sich eine Kultur des «need to share» entwickelt. Dabei ist der Schutz von sensiblen Informationen in Übermittlung und Ablage (Datenbanken) bedeutsamer denn je. Denn sie sind zahlreichen Gefährdungen ausgesetzt – angefangen bei den Möglichkeiten klassischer Elektronischer Kriegsführung über die umfangreichen permanenten Aufklärungsmittel grosser geopolitischer Player bis hin zu den Schwachstellen innerhalb der eigenen Organisation und zu deren Ausnutzung durch versierte Saboteure wie zum Beispiel den mutmasslichen Wikileaksinformanten Bradley Mannings. Gleichzei-

Moderne Streitkräfte setzen auf Hochsicherheitsmassnahmen, die gleich auf mehreren Verteidigungslinien aufbauen:

- Grösstmöglichen Informationsschutz dank eines massgeschneiderten Sicherheitssystems anstatt eines Konglomerats aus Massenmarktware mit dem blossen Zusatzfeature «Sicherheit»;
- Sichere Datentransfers (Confidentiality), Integrität und gesicherte Herkunft der Nutzdaten (Integrity/Authenticity) und Mission Control (Accountability);
- Sichere Kompatibilität und Interoperabilität der Netze, die bislang bestenfalls ungeschützt durchgängig betrieben werden konnten (homogene Sicherheit für heterogene Topologien);
- Den Einzug einheitlicher Sicherheitsstandards auch in organisch gewachsene Einsatznetze mit dem praktischen Nebeneffekt des Investitionsschutzes;
- Umfassende Services basierend auf etablierten Standards (z.B. die DoDAF Architecture Framework);
- Die konsequente Trennung von Fragen des Betriebs der ICT-Infrastruktur und von Fragen des Sicherheitsmanagements;
- Die souveräne, ausschliesslich nationale Kontrolle über die eingesetzte Verschlüsselung (und nicht deren Kontrolle durch den Lieferant) bzw. die Verwendung von «Joint Algorithms».

tig entscheiden ihre Geheimhaltung und ihre unverfälschte, ständige Verfügbarkeit nachhaltig über die Sicherheit der eigenen Streitkräfte und über jeglichen Missionserfolg. Sie auf höchstem Level zu schützen beinhaltet mindestens:

- Die Auslegung des gesamten Einsatznetzes auf der Grundlage einer umfassenden und schlüssigen Sicherheitsarchitektur mit geschützten Zonen und Zonenübergängen;
- Die Echtzeitunterstützung aller Führungsinformationsprozesse bei gleichzeitiger Wahrung der Vertraulichkeit, Rückverfolgbarkeit, Integrität und Zugriffskontrolle aller verarbeiteten sensitiven Daten;
- Die Schaffung einer undurchlässigen und homogenen Systemsicherheitsschicht auf der Transport-, Service- und Applikationsebene, gerade auch in heterogenen Systemlandschaften;
- Die sichere Sprach- und Datenverbindungen, insbesondere in den Bereichen Radio, Messaging, IP/VPN und an der Schnittstelle zu sämtlichen Backbonetechnologien.
- Die Identifikation und Authentifizierung aller an der Kommunikation beteiligten Geräte und Personen, um Nachvollziehbarkeit und Integrität gewährleisten zu können.

«Militärische Befehlshaber müssen sich darauf verlassen können, dass ihre Führungskommunikation unter keinen Umständen abgehört, beeinflusst, verfälscht oder an Unbefugte weitergegeben wird.»

Technische Lücken gefährden ganze Operationen

Die technische Stärke und die Achillesferse der netzwerkzentrierten Kriegsführung liegen erfahrungsgemäss nahe beieinander. Hochkomplexe Führungs- und Kommunikationssysteme wie etwa das Afghan Mission Network der NATO, vielfach zusammengesetzt aus den Komponenten unterschiedlicher Nationen, Hersteller und Beschaffungsgenerationen, bergen nicht nur die Gefahr inkompatibler Schnittstellen, sondern auch nicht zu unterschätzende Sicherheitslücken. Wenn solche Brüche die Geheimhaltung und die Authentizität einsatzrelevanter Daten kompromittieren, können die eigenen Informationen leicht in fremde Hände gelangen und zum Nachteil gegen die Beschaffer verwendet werden. Eindrücklich hat dies etwa 2009 das Beispiel unverschlüsselter sensibler Aufklärungsdaten aus US-Drohnen in Afghanistan belegt, die von Aufständischen über Monate mit einer zivilen 26-Dollar-Software abgefangen werden konnten und somit für die Einsatzkräfte wertlos wurden. ■

Hptm
Jahn Koch
lic. phil.
Customer Segment Manager
Defence, Crypto AG
6301 Zug