
# AFCEA 2012

## ZVEI – Die Elektroindustrie

ISBN 978-3-934401-15-0

**Behörden Spiegel-Gruppe**
**in Zusammenarbeit mit AFCEA Bonn e.V.**

# Mehr Papa im Monat

**BWI – Strategischer Partner der Bundeswehr für Informations- und Kommunikationstechnik**

## Dank HERKULES können Angehörige der Bundeswehr sicher von zu Hause aus arbeiten.

BWI und Bundeswehr haben die technischen Rahmenbedingungen geschaffen, damit Familie und Dienst bei der Bundeswehr besser vereint werden können. Dadurch können Bundeswehrangehörige von zu Hause oder von unterwegs aus so arbeiten, als seien sie vor Ort in der Dienststelle. Die Voraussetzungen dafür bildet der Remote Access Service (RAS) der BWI. Als einheitliche Lösung für das mobile Büro ermöglicht der RAS einen sicheren und leistungsfähigen Zugang zum Netz und zu den IT-Anwendungen der Bundeswehr. Diese IT-Lösung ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen und erlaubt die verschlüsselte Übertragung eingestufter Daten über das Internet.

Weitere Informationen unter: www.bwi-it.de

BWI

Bonn, Mai 2012

Sehr geehrte Damen und Herren,

die Broschüre “AFCEA 2012”, die durch den Behörden Spiegel wie in den Vorjahren zusammen mit AFCEA Bonn e.V. herausgegeben wird, erscheint zur AFCEA-Fachausstellung, der zentralen Fachmesse für die Informations- und Kommunikationstechnik der Bundeswehr – aber auch zunehmend der Behörden und Organisationen mit Sicherheitsaufgaben. Die Angehörigen aus dem Bundesministerium der Verteidigung und aus den zahlreichen Dienststellen der Rheinschiene von Köln bis Koblenz informieren sich jedes Jahr im Mai in Bonn-Bad Godesberg über die Weiterentwicklung der IT/ITK. Die über 100 Aussteller fokussieren dazu ihr Angebot auf diesen speziellen Besucherkreis.

Partner für die Broschüre “AFCEA 2012” ist der ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V. mit seinem Sitz in Frankfurt am Main. Die Wahl dieses Partners erfolgte nicht ohne besonderen Grund. Erst kürzlich hat der Fachverband Sicherheit des ZVEI seine Organisation umgestellt. In drei neuen Leitmärkten und mit neuen Fachkreisen konzentriert er sich in den Bereichen Sicherheit und Verteidigung auf die neuen Schwerpunkte in der Informations- und Kommunikationstechnik.

Die vorliegende Broschüre beschreibt Veränderungen – vor allem in der Bundeswehr. Die Bundeswehr erhält eine neue Struktur, die das Bundesministerium der Verteidigung, ihre Ämter und Dienststellen und die Verbände betrifft. Es ist nicht die erste Anpassung an neue Rahmenbedingungen und es wird auch nicht die letzte bleiben – es ist aber die bisher einschneidendste. Die Verlagerung der Inspekteure der Teilstreitkräfte aus dem BMVg an neue Standorte macht dies deutlich. Die Änderungen im Rüstungsbereich der Bundeswehr – und damit auch in der IT – sind nicht weniger bedeutend.

Die Fachausstellung von AFCEA Bonn e.V. ist daher in diesem Jahr von besonderem Interesse. Nach dem Dresdner Erlass des Bundesministers der Verteidigung vom 21.03.2012 ist sie die erste große Gelegenheit für die Industrie und die Verbände mit neuen Ansprechpartnern über geänderte Strukturen und vor allem über veränderte Prozesse zu diskutieren. Das Thema “Mobile Computing im/für den Einsatz” bietet dazu den äußeren Rahmen. Ich wünsche daher der Fachausstellung besonderen Erfolg. Sie ist für alle wichtig – für die Besucher und für die Aussteller.

R. Uwe Proll
Herausgeber

www.behoerdenspiegel.de

**Impressum:** Sonderheft Behörden Spiegel “AFCEA 2012” **Redaktionelle Leitung:** Reimar Scherz, Behörden Spiegel, Telefon 0228 / 970 97-83 **Herausgeber** (presserechtlich verantwortlich): R. Uwe Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Berlin/Bonn **Anzeigen:** Beatrix Lotz, Helga Woll **Herstellung:** Spree Service- und Beratungsgesellschaft mbH, Berlin **Satz und Layout:** Birte Schulz, Behörden Spiegel **Fotos:** Autoren, AFCEA Bonn e.V., ZVEI, Behörden Spiegel Archiv **Druck:** Heider Druck GmbH, Bergisch Gladbach **Heftpreis:** 7,50 Euro  www.behoerdenspiegel.de

# AFCEA 2012

## 1. AFCEA Bonn e.V. – unter neuen Rahmenbedingungen



## 2. ZVEI – Sicherheit und Verteidigung

## 3. AFCEA-Fachausstellung

# Die neuen Herausforderungen annehmen!

## Generalmajor Erich Staudacher, Vorsitzender AFCEA Bonn e.V.

*Generalmajor Erich Staudacher*

Wenn Sie, lieber Leser, dieses Jahr unser traditionelles Begleitheft für das AFCEA-Jahr und die AFCEA-Fachausstellung aufschlagen, wird Ihnen der Topos “neu” in vielfältiger Form begegnen. Am meisten dürfte dieser in Verbindung mit der “Neuausrichtung der Bundeswehr” Ihre Aufmerksamkeit erhaschen.

Für AFCEA Bonn e.V. steht natürlich die “Neuausrichtung der Bundeswehr”, mit all ihren Auswirkungen auf IT, Führungsunterstützung, Vernetzung, Automatisierung im Mittelpunkt unseres Interesses. Nach 2011 als einem Jahr der Überraschungen, der auch zum Teil ungeplanten personellen Veränderungen, in der Umfang und Dimension der Neujustierung aller Stellschrauben sich erst allmählich in den Details herauszuschälen begann, weicht nun in 2012 der Zauber des Neuanfangs – “Alles ist Möglich” – den Mühen der Ebene – “Hart im Raume stoßen sich die Realitäten”. So nimmt z.B. der neue Rüstungs- und Nutzungsprozess, auch die Beschaffung und Nutzung von IT umfassend, im manchmal zähen Widerstreit der Meinungen nun Kontur an.

*AFCEA-Fachausstellung 2011: interessante Gespräche mit Bürgermeister Helmut Joisten*

Im Hintergrund entwickelt sich auch eine neue Unternehmenskultur in der Bundeswehr, die bei weiterhin klaren Verantwortlichkeiten und im Vertrauen auf den Leistungswillen die Zusammenarbeit der Nutzer mit den Ressourcenbereichen fördern will. Es soll nicht mehr die Situation eintreten, dass mit Verweis auf die eigene Unzuständigkeit jedes Problem dem Gegenüber zugeschoben wird und Lösungen nur auf Ebene der gemeinsamen Führung möglich sind. Zielvereinbarung, Leistungsvereinbarung und Integriertes Projektteam sind die neuen Schlüsselbegriffe.

Ausgelöst durch den bevorstehenden Umzug weiterer Teile des Bundesministeriums der Verteidigung nach Berlin gilt es, künftig dem “Gesprächsort” Berlin mehr Bedeutung zuzumessen. Wir von AFCEA Bonn e.V. müssen nüchtern feststellen, dass unsere bisherige Konzentration auf die Rheinschiene allein nicht mehr trägt. Also heraus aus eingefahrenen Gleisen! Seien Sie, liebe Freunde, bitte nicht überrascht, wenn wir in einem ausgeweiteten Verständnis von “Regionalität” als Bonner Chapter nun auch in Berlin ansprechbar sein werden. Dies bedeutet keineswegs die Vernachlässigung der treuen und wertvollen Partner zwischen Koblenz und Köln. Auch freuen wir uns auf die Gesprächspartner im neuformierten Führungsunterstützungskommando in Bonn und im Kommando Sanität in Koblenz. Aber mit Blick auf die ministerielle Entscheidungsebene und das Planungsamt in Berlin sowie einiger Teilstreitkräftekommandos im Umfeld ist die Tätigkeit von AFCEA Bonn e.V. in räumlicher Hinsicht auszuweiten. Aber nicht nur! Es gilt auch, die thematische Bereicherung zu erkunden, die z.B. mit der engeren Verknüpfung der bislang organisatorisch getrennten Bereiche IT und Waffensysteme im neuen BAAINBw nun möglich ist.

Zudem erleichtert uns ein solcher Neuansatz, auch Themen gemeinsamen Interesses und standardisierte, ressortübergreifende Lösungsansätzen zwischen der BOS-Welt und der Bundeswehr besser zu vermitteln, ganz im Sinne der Blickerweiterung von “defence” hin zu “security”. Eine sich rapide entwickelnde Bedrohungslage im und mittels des Internets verhilft dem manchmal schon etwas in Vergessenheit geratenen Begriff der Vernetzten Sicherheit zu neuer Aktualität. “Cyber security” ist in aller Munde. Wir von AF-


*GenMaj Staudacher eröffnet die AFCEA-Fachausstellung 2011*

CEA Bonn e.V. haben uns entschlossen, nicht mit einem entsprechenden Jahresthema zu einer ermüdenden Anhäufung einander ähnlicher Events beizutragen, sondern diesem Phänomen in allen Facetten durch kontinuierliche Berücksichtigung im Verlauf unserer diesjährigen Veranstaltungen näher zu rücken. Damit wollen wir nicht dem "Hype" Vorschub leisten. Vielmehr ist es unser Ziel, die in allen Verfahren, Ausrüstungen und Systemen notwendige Berücksichtigung von IT-Sicherheit, Datenschutz und Reaktionsfähigkeit im Cyber-Raum mit Sachverstand zu fördern.

Ein Zweites: Das vergangene Jahr hat mit dem arabischen Frühling die geopolitische Landschaft tiefgreifend verändert. Wir alle sind Zeuge der überraschenden Wirkung von sozialen Netzen bei innerstaatlichen Auseinandersetzungen. Hier hinein spielt der rasante Bedeutungsgewinn des mobilen Netzzugangs, des Loslösens der Datenverarbeitung und -verwendung von fixer IT-Infrastruktur, kurzum der ganze Reichtum der Möglichkeiten von "mobilem Computing". In den Augen vieler, gerade Jugendlicher, hat sich der ungehinderte Zugang zum Internet zu einer Art Grundrecht entwickelt. Mit gleicher Selbstverständlichkeit erwarten junge Menschen folglich eine entsprechend moderne Arbeitsumgebung, wenn sie den Streitkräften beitreten oder erkennen den Nutzen solcher IT-Entwicklungen im konkreten Einsatzumfeld, etwa von ISAF und Operation Unified Protector intuitiv.

Weil AFCEA sich seit 1946 den Herausforderungen und Erwartungen von Streitkräften und Sicherheitskräften inmitten der Gesellschaft und ihren Strömungen stellt, hat AFCEA Bonn e.V. daher "Mobile Computing" mit besonderem Blick auf die Einsätze zum diesjährigen Jahresthema gewählt. Wir sind sicher, dass wir damit für die Anwender wie für die Ent-

## Vorstand AFCEA Bonn e.V. 2012

### Geschäftsführender Vorstand

Vorsitzender
**Erich Staudacher**

Stellvertretender Vorsitzender und Leiter Programmbeirat
**Reimar Scherz**

Stellvertretender Vorsitzender und Sprecher Industriebeirat
**Joachim Mörsdorf**

Beauftragter für internationale Angelegenheiten
und Programmbeirat
**Hans-Ulrich Schade**

Geschäftsführer
**Rolf-Dieter Zeckai**

### Erweiterter Vorstand (Beisitzer)

Leiter AFCEA-Fachausstellung
**Friedrich W. Benz**

Industriebeirat
**Andreas Höher**

Industriebeirat
**Hartmut Jäschke**

Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
**Dietrich Läpke**

Programmbeirat und Young AFCEANs
**Ralph Michel**

Presse- und Öffentlichkeitsarbeit,
Repäsentant im Young AFCEANs Advisory Council
**Jochen Reinhardt**

Programmbeirat
**Dr. Ansgar Rieks**

Internationale Angelegenheiten und
Regional Vice President (RVP) North West European Region
**Wolfgang Taubert**

Schriftführer
**Kurt D. Wachsmuth**

Nachwuchsförderung
**Dr.-Ing. Michael Wunder**

### Mitwirkende Vorstandsgäste

Programmbeirat
**Karin Börsch**

Programmbeirat und Young AFCEANs
**Katja Frintrop**

Programmbeirat
**Götz Stuck**

*Die Koblenzer Fachtagung IT – seit sieben Jahren ein Highlight des Programms von AFCEA Bonn e.V.*

scheider im militärischen wie zivilgesellschaftlichen Bereich eine interessante thematische Grundlage für Gespräche, Erfahrungsaustausch und Denkanstöße bieten können. In unseren Fachveranstaltungen, dem Symposium der Fachausstellung, der Koblenzer Fachtagung und anderen Ereignissen tragen hierzu wie bisher die Vertreter aus Forschung und Wissenschaft, Amtseite, Industrie und Fachverbände maßgeblich bei. Mein besonderer Dank gilt daher an dieser Stelle vor allem unseren treuen Partnern von BITKOM, ZVEI, der Fraunhofer-Gesellschaft und dem Behörden Spiegel.

Wie Sie unserem Jahresprogramm entnehmen können, ist uns wiederum der Kontakt zur BOS-Gemeinde von besonderer Bedeutung. Ihn halte ich für weiter ausbaufähig, gilt es doch durch einen Informationsaustausch ohne gedankliche oder formale Schranken das gegenseitige (Kennen-)lernen zu fördern und vor allem beim Transfer von Lösungsansätzen behilflich zu sein. Denn das Rad muss ja nicht an mehreren Stellen gleichzeitig erfunden werden. Sicherlich gibt es Unterschiede in den spezifischen Anwendungen der IT-Unterstützung im militärischen und BOS-Bereich. Viele Gespräche aber haben mir verdeutlicht, wie sehr sich doch auch die Bedürfnissen ähneln. Vor allem die Streitkräfte aller Nationen tun gut daran, im Zeitalter schrumpfender Budgets den Blick “über den Zaun” zu richten auf Entwicklungen bzw. Realisierungen im zivilen Anwenderumfeld.

Verstärken werden wir unsere Bemühungen, jüngere Mitglieder und Freunde zu gewinnen und ihnen Mitwirkungsmöglichkeiten im AFCEA-Rahmen auch zur Präsentation von Ideen zu bieten. Im Fokus stehen für uns dabei Studierende höherer Semester und junge Berufsanfänger in Firmen und Behörden. Wir sind im Zusammenwirken mit den Hochschulen der Region bestrebt, unsere Möglichkeiten zur Würdigung herausragender Leistungen auszuweiten.

Im schulischen Bereich suchen wir immer noch nach effektiven Möglichkeiten der Unterstützung, die eben nicht nach dem Gießkannenprinzip erfolgt. Uns ist bewusst, dass die Förderung der naturwissenschaftlichen Bildung und des Interesses an der IT, das über die Nutzung vorgefertigter Software-Tools hinausgeht, weiterhin der Hilfe bedarf. Schließlich gilt es auch, das Bewusstsein für Risiken und Gefahren des Internets bei Heranwachsenden immer wieder zu schärfen. Vorschläge, wie AFCEA Bonn e.V. hier zusätzlich zu den etablierten Förderern nützlich sein kann, nehmen wir dankbar entgegen.

Last but not least darf ich Sie auf unser überarbeitetes Design hinweisen. Alle Auftritte von AFCEA Bonn e.V., vor allem die neu gestaltete Webseite, haben ein moderates “Face Lifting” erfahren. Wir wollen unsere Eigenständigkeit als Bonner Chapter in moderner, aber nicht übertriebener Form hervorheben, ohne unsere Verbindung zur weltumspannenden Gemeinschaft von AFCEA International in Frage zu stellen. Gerade globales Denken in gemeinsamen Werten mit regionalem Handeln zu verbinden war und ist die Stärke von AFCEA.

Lassen Sie mich herzlich Danken allen Freunden und Förderern von AFCEA Bonn e.V., die unsere bisherige erfolgreiche Arbeit überhaupt erst ermöglichten. Anschließen möchte ich auch meinen Dank an die vielen freiwilligen Mitwirkenden von AFCEA Bonn e.V., die die guten Ideen und Themen in die Tat der Veranstaltungen umsetzen. Einigen von ihnen, unseren Vorstandsmitglieder, werden Sie in den nun folgenden Artikel begegnen.

Aber die Wichtigsten adressiere ich zum Schluss, nämlich Sie, die geschätzten Leser. Ihr Interesse ist unsere Daseinsberechtigung, Ihr Beifall oder Ihre Kritik unser Ansporn. Ich wünsche Ihnen viel Vergnügen bei der Lektüre und freue mich auf Ihre Anregungen!

# Neuausrichtung des Bundesministeriums der Verteidigung (BMVg) und deren Bedeutung für die Prozesse und die Informationstechnik (IT)

Brigadegeneral Dr. Ansgar Rieks, Vorstand AFCEA Bonn e.V.

*Brigadegeneral Dr. Ansgar Rieks*

Die Neuausrichtung der Bundeswehr (Bw) mit ihren weitreichenden Auswirkungen beinhaltet auch eine Änderung ihres bisherigen Führungsverständnisses und ihrer zivilen und militärischen Führungsstrukturen. Davon betroffen ist auch ihr "strategischer Steuerkopf", das BMVg, wo eine bislang "allgemeine Verantwortungsdiffusion" (vgl. Bericht der Strukturkommission vom 26. Oktober 2010, S. 34) beseitigt und Verantwortungen klarer, zum Teil neu, definiert wurden. Ergebnis: Neue Strukturen, neue Prozesse, neue Klarheit, Kompetenz und Verantwortung in einer Hand und Konzentration auf die ministeriellen Kernaufgaben fördern gemeinsames, integriertes Denken, konsequentes Handeln und eine effektive Aufgabenerfüllung. Die operative Umsetzung wird in die Verantwortung der Behörden und Dienststellen der Bw übergeben.

## Das BMVg auf neuem Kurs

Der Dienstpostenumfang des BMVg wird dabei von ca. 3.100 auf rd. 2.000 Dienstposten reduziert, die sich auf 26 Unterabteilungen und rd. 150 Referate verteilen (siehe Schaubild 1). Im Rahmen eines integralen Ansatzes werden die neuen Abteilungen des BMVg verstärkt zivil-militärisch "gemischt" besetzt. Die militärischen Organisationsbereiche (MilOrgBer) werden durch ihre Inspekteure nun außerhalb des Ministeriums geführt. Die Aufgabenbereiche der Abteilung Modernisierung wurden in andere Abteilungen integriert.

## Investieren in die Zukunft

Im Zentrum der Überlegungen für die Neuorientierung geht es darum, die Bundeswehr zukunftsfähig zu machen. Einige ausgewählte Entscheidungen hierzu sind:

Die bisherige Hauptabteilung Rüstung wurde neu strukturiert und firmiert nun unter "Ausrüstung, Nutzung und IT". Damit ist ihr neues Aufgabenprofil beschrieben.

Die neue Abteilung Planung entwickelt auf der Basis der Verteidigungspolitischen Richtlinien die Konzeption der Bw und setzt so den Rahmen für das Leistungsprofil der gesamten Bw. Die neue Prozessphilosophie des BMVg wird u.a. in einem Integrierten Planungsprozesses (IPP) stringent umgesetzt. Er bildet auf der Basis von Zukunftsentwicklung und Fähigkeitsmanagement einen Regelkreis aus mittelfristiger

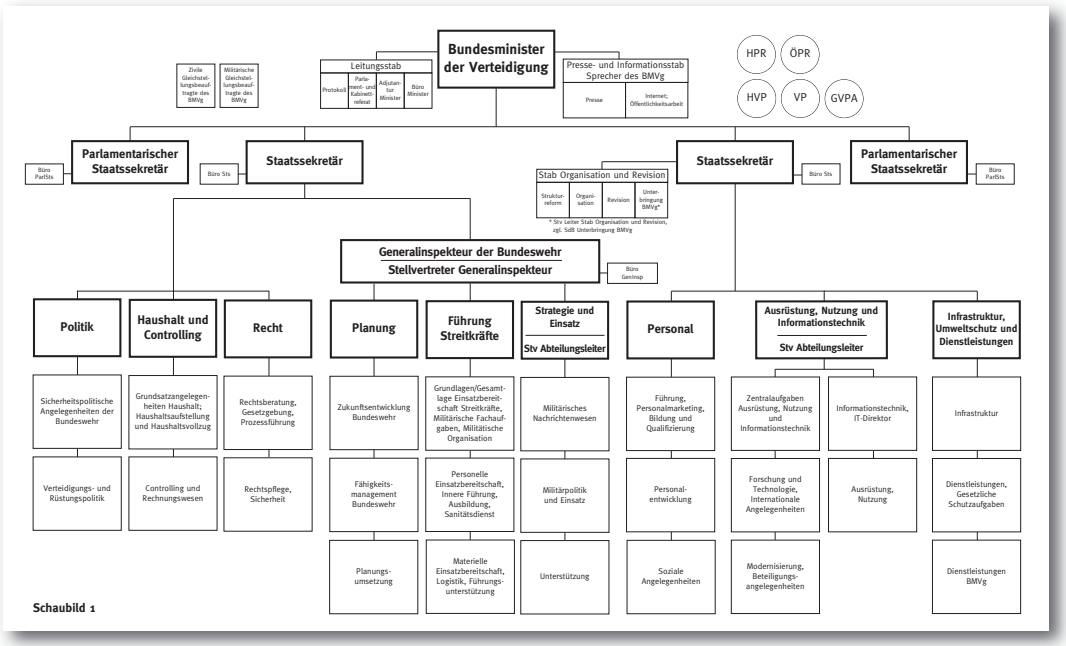
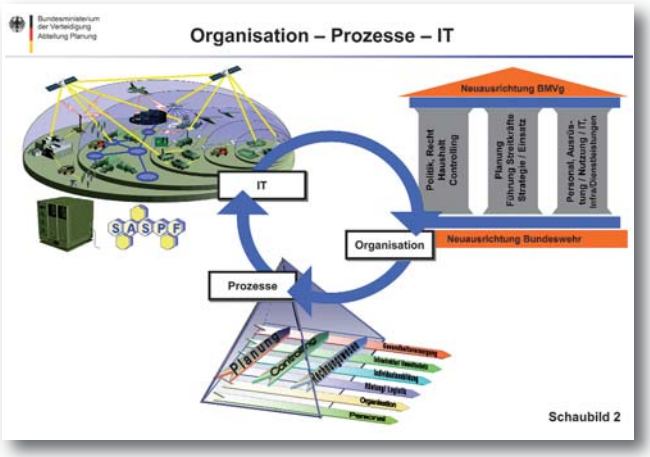



Schaubild 1

*Das neue Bundesministerium der Verteidigung mit 26 Unterabteilungen*




*Die besondere Rolle der IT*

Zielsetzung, Finanzbedarfsanalyse, Ressourcenplanung und Haushaltsaufstellung. Der IPP integriert ferner die durch die Abteilung Haushalt/Controlling verantwortete Zielvereinbarung, Haushaltsführung und Zielnachhaltung. Der IPP führt somit die bisher getrennten Bereiche der Bw-Planung, der Haushaltsplanung und des Controlling zusammen und fördert die enge Zusammenarbeit mit allen Organisationsbereichen. Dadurch werden auch die weiteren Prozesse, wie z.B. der Ausrüstungs- und Nutzungsprozess eng angebunden. Dies beseitigt unnötige Schnittstellen, erhöht die Leistungsfähigkeit – auch durch konsequente Einbeziehung der Einsatzauswertung – und verbessert die Effizienz. Zugleich verdeutlicht dieses integrative Zusammenwirken von Nutzern, Planern und Bedarfsdeckern, mit klar definierter Verantwortungsübergabe, das an Schnelligkeit, Effizienz und Flexibilität ausgerichtete neue "Denken und Handeln vom Einsatz her".

## Neue IT – Effizienz und Sicherheit

Im Rahmen der Neuausrichtung der aufbau- und ablauforganisatorischen Grundstruktur des BMVg und der Bw gilt es auch, innovative und unterstützende Technologien mit dem neuen Prozessdenken zu verbinden (siehe Schaubild 2). Für das BMVg heißt dies, dass die Neukonzeption von Verantwortung, Prozessen und Strukturen absehbar auch eine Umstellung von IT erfordert. Benötigt werden z.B. neue Funktionalitäten im Controlling und generell eine effektive Nutzung bzw. Anwendung der bereitgestellten IT. "E-Mail-Traffic" und "E-Mail-Wildwuchs" nach dem Motto "BMVg-weit verteilt ist gescheit" muss einer zielgerichteten intelligenten Nutzung Platz machen. Integratives Arbeiten fordert klar strukturierte Netzwerke. Eine darauf ausgerichtete IT auf Basis einer garantierten hohen Datenqualität mit Blick auf "Einheitlichkeit und Richtigkeit" unterstützt zielgerichtete Auftragserfüllung. Es ist offensichtlich, dass nicht nur Hard- und Software, sondern vor allem auch die Nutzer und ihr Verhalten eine entscheidende Stellgröße für die Neuausrichtung sind. Neue Medien, Entwicklungen im Bereich des Internets, Telearbeitsplätze, E-Government, Flexibilität durch Cloud Computing und damit verbundene dynamische IT-Infrastrukturen versprechen zwar vieles komfortabler und effizienter zu machen, bedürfen jedoch auch einer ganzheitlichen Sicherheitsstrategie, die den Gefahren der Cyber-Bedrohung Rechnung trägt.

Moderne IT ist eine wichtige Ressource für das BMVg und für die gesamte Bw, insbesondere auch im Einsatz. Grundlage hierfür ist ein führungsebenenübergreifender, national und multinational interoperabler und sicherer Informations- und Kommunikationsverbund, der IT-Services zur Verfügung stellt. Auf diesem Weg können erforderliche Prozesse, z.B. aus den Bereichen Führung, Logistik und Administration, auf allen Ebenen durchgängig von der Basis Inland, beginnend im BMVg, über das Einsatzführungskommando, bis in die Einsatzgebiete unterstützt werden. Die deutsche Teilhabe am Afghanistan Mission Network (AMN) ist das Beispiel für eine gelungene multinationale Einbindung und Interoperabilität nationaler Systeme. AMN stellt einen erheblichen Fähigkeitsgewinn dar, kann als "Blaupause" für künftige Einsätze dienen und ist ein substanzieller Schritt hin zur Vernetzten Operationsführung.

## Integrativer Ansatz

Die strukturelle Neuausrichtung wird, im BMVg beginnend, über alle Ebenen umgesetzt. Dabei muss an dem etablierten Ansatz der integrativen Prozessausrichtung festgehalten werden. Im Rahmen der Weiterentwicklung wird daher auch ein Schwerpunkt auf die ergänzend zu implementierenden Werkzeuge und Instrumente von Planung, Haushalt und Controlling sowie Ausrüstung, Nutzung und IT gelegt werden müssen, um sowohl die neuen BMVg- als auch Bw-Strukturen wegweisend in die IT- und Prozesslandschaft zu integrieren.

*BrigGen Dr. Rieks und Jochen Reinhardt bei der Scheckübergabe zur Schulförderung von AFCEA Bonn e.V.*

# Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) – neue Strukturen und Prozesse für die IT

Hans-Ulrich Schade, Erster Direktor IT-AmtBw, Vorstand AFCEA Bonn e.V.

*Hans-Ulrich Schade*

Nach den Eckpunkten zur Neuausrichtung der Bundeswehr vom Mai 2011 werden die Beschaffung von Ausrüstungsgegenständen für die Streitkräfte und die Angelegenheiten der Informationstechnik der Waffensysteme und der Führungsunterstützung gebündelt. Damit hat diese Neuausrichtung erhebliche Auswirkungen auf den sogenannten Ausrüstungs- und Nutzungsprozess.

Das zur Umsetzung der Neuausrichtung eingerichtete Projekt "Rüstung, Nutzung, Informationstechnik", das vom Abteilungsleiter Rüstung im Bundesministerium der Verteidigung (BMVg) geleitet wurde, befasste sich mit der Entwicklung eines neuen, einheitlichen Ausrüstungs-, Beschaffungs- und Nutzungsmanagements. Dazu war es erforderlich, den bestehenden Rüstungsprozess (Customer Product Management, CPM) mit dem Ziel zu optimieren, klare Verantwortlichkeiten und Entscheidungskompetenzen zu schaffen sowie insbesondere die derzeit existierenden Schnittstellen bei der Bedarfsermittlung, Bedarfsdeckung und Nutzung deutlich zu reduzieren.

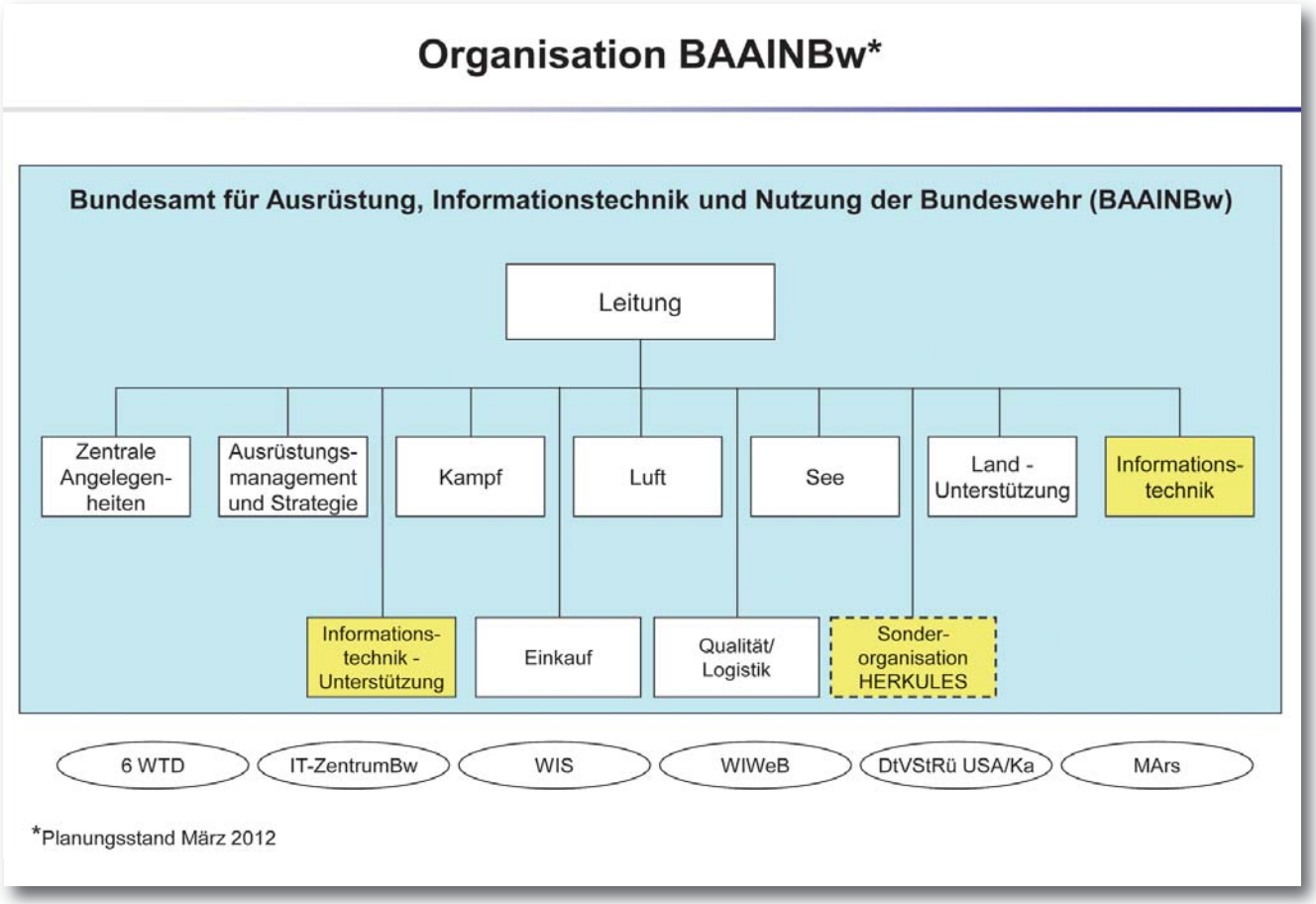
Der Leiter der Abteilung Ausrüstung, Informationstechnik und Nutzung (AIN) im BMVg trägt die durchgängige Verantwortung von der Erarbeitung materieller Lösungen (Produkte, Dienstleistungen) über deren Realisierung und Nutzungssteuerung bis hin zu deren Verwertung.

Das technische System-Know-how wird über den gesamten Lebensweg im neu einzurichtenden Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) vorgehalten, das durch die Zusammenführung des Bundesamtes für Wehrtechnik und Beschaffung (BWB) und des Bundesamtes für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) sowie durch die Integration von Nutzungsaufgaben aus den Organisationsbereichen entsteht. Zusammen mit der Rückkopplung aus dem Betrieb werden in dieser zivilen, gemischt zivil/militärisch besetzten Bundesoberbehörde die gewonnenen Erkenntnisse effektiv in die Neu- und Weiterentwicklung sowie Anpassung eingeführter Produkte eingebracht und umgesetzt. Dazu wurde dem Präsident/der Präsidentin des neuen Amtes die Materialverantwortung für die Einsatzreife für sämtliche Produkte und Dienstleistungen übertragen. Diese umfasst alle produktbezogenen Managementtätigkeiten, die eine sichere und bestimmungsgemäße Verwendbarkeit eines Produktes ermöglichen.

Das IT-AmtBw hat bereits in der Vergangenheit Nutzungsaufgaben im Bereich der Informationstechnik wahrgenommen. Die dort gewonnenen Erfahrungen sind in die Neuausrichtung eingeflossen. Organisatorisch findet die IT ihren Niederschlag in der Einrichtung der Abteilungen Informationstechnik und Informationstechnik-Unterstützung sowie der Sonderorganisation HERKULES des BAAINBw. Den Planungsstand März 2012 stellt die Abbildung dar.

Dabei sollen alle Aufgaben der Systeme der Informationsversorgung im Einsatz (Kommunikationssysteme, Führungsinformationssysteme und Aufgaben im Umfeld der IT-Sicherheit) in der Abteilung Informationstechnik und die Aufgaben aus den Bereichen der Fachinformationssysteme – einschließlich der Realisierung von SASPF – in der Abteilung Informationstechnik-Unterstützung wahrgenommen werden. Die IT-Ausstattung im Heimatland wird weiterhin Aufgabe der Sonderorganisation HERKULES sein.

Für die Informationstechnik bildet die von Staatssekretär Beemelmans am 16. Januar dieses Jahres in Kraft gesetzte IT-Strategie der Bundeswehr die an die neuen Strukturen und Prozesse angepasste konzeptionelle Grundlage für die Aufgabenwahrnehmung. Mit dieser Strategie wird abgeleitet und festgelegt, wie die Ziele der Bundeswehr unter Berück-




*BWB und IT-AmtBw werden das neue BAAINBw*

sichtigung der operativen und finanziellen Rahmenbedingungen bestmöglich durch IT unterstützt werden können. Sie stellt das Instrument zur strategischen IT-Steuerung in der Bundeswehr dar und ist regelmäßig – angepasst an den jährlichen Planungsrhythmus – zu überprüfen und fortzuschreiben. Die IT-Strategie hat Vorgabecharakter für die Ausgestaltung der IT in der Bundeswehr und setzt – ergänzend zur Konzeption der Bundeswehr (KdB) und im Rahmen des Integrierten Planungsprozesses (IPP) – unter Berücksichtigung der vorgenannten Rahmenbedingungen Vorgaben für Folgedokumente.

Eindeutig im Vordergrund dieser Strategie steht weiterhin die Verbesserung der Befähigung der Bundeswehr zur Vernetzten Operationsführung. Außerdem gilt es unverändert, die Rationalisierung des Betriebes der Bundeswehr mit Hilfe der IT weiter voranzutreiben. Einer der Schwerpunkte liegt dabei auf der Harmonisierung und Standardisierung der IT-Systeme. Die Erfahrungen aus dem Einsatz zeigen deutlich, dass der eingeschlagene Weg der Reduzierung der Produktvielfalt und der Verbesserung der Interoperabilität weiter beschritten werden muss.

Die mit der überaus erfolgreichen deutschen Teilhabe am multinationalen Afghanistan Mission Network (AMN) gewonnenen Erkenntnisse hin zu einer serviceorientierten Architektur von Informationssystemen werden weiter konsequent umgesetzt, um die Flexibilität und Modularität der IT-Unterstützung auch in Zukunft zu erhöhen. Ziel ist es, den Streitkräften eine weitgehend einheitliche, hoch leistungsfähige und flexibel einsetzbare Ausstattung zur Verfügung zu stellen, die zudem jederzeit und an jedem Ort die Zusammenarbeit mit Verbündeten und Partnern ermöglicht.

Darüber hinaus beschreibt die IT-Strategie weitere Handlungsfelder, z.B. die Rolle des IT-Sicherheitsbeauftragten der Bundeswehr im BMVg in der Abteilung AIN und das Zusammenspiel mit seinem Stellvertreter in der Leitung des BAAINBw.

Das IT-System der Bundeswehr ist jedoch mehr als die Summe aller IT-Projekte. Ein taktisches Funkgerät, das die Erfordernisse von Trägerplattformen nicht berücksichtigt, ist ebenso nutzlos wie ein leistungsfähiges Führungsinformati-

onssystem, für das kein ausreichend ausgebildetes Personal zur Verfügung steht. Hier kann und wird die Zusammenführung der Ausrüstungs-, Informationstechnik- und Nutzungsaufgaben in einem Amt sowie die Ausbringung des IT-Direktors der Bundeswehr in der Abteilung AIN im BMVg positive Wirkung zeigen.

Die Organisation des neu aufzustellenden BAAINBw wird die neuen Rollen und Funktionalitäten im Bereich der IT abbilden und somit das Zusammenspiel mit den entsprechenden Akteuren im BMVg, im Ämterbereich, in der Industrie sowie in der Wissenschaft sicherstellen.

Insgesamt bietet die Verankerung der Informationstechnik der Bundeswehr in der neuen Abteilung AIN im BMVg sowie im BAAINBw für AFCEA Bonn e.V. neue Herausforderungen, aber auch Chancen. Die Informationstechnik bleibt auch künftig integraler Bestandteil des (Aus-)Rüstungsbereichs, der mit seinem erweiterten Aufgabenumfang besondere Bedeutung für eine zukunftsweisend ausgerichtete Bundeswehr haben wird. Hier wird sich ein weites, interessantes Feld der fachlichen Zusammenarbeit für AFCEA Bonn e.V. eröffnen.

*Gute Gespräche mit dem IT-AmtBw auf der Fachausstellung*

# Kooperationspotentiale bei der wehrtechnischen Forschung im Bereich Informations- und Kommunikationstechnik

Dr.-Ing. Michael Wunder, Vorstand AFCEA Bonn e.V.

*Dr.-Ing. Michael Wunder*

## Einleitung

Finanzieller und zeitlicher Druck, der sich aus den Einsatzszenarien der Bundeswehr und denen der Streitkräfte, der mit Deutschland in unterschiedlichen Konstellationen verbundenen Nationen ergibt, bestimmen zunehmend die Planungen im Bereich F&T. Dabei wird der Schwerpunkt von der angewandten Grundlagenforschung (F&T-Stufe 1) mit Vorhaben von eher langfristiger Bedeutung, wie der Nanotechnologie, Robotik oder Sensorik hin zu eher anwendungsnahen Technologien (F&T Stufe 2) verschoben, da hier schon immer der konkrete Einsatzbedarf der Streitkräfte und Sicherheitsorgane die Planungen bestimmte. Für den Bereich Informations- und Kommunikationstechnik (IKT) sind dabei vor allem Themen wie Abwehrmaßnahmen gegen IT-Bedrohungen (Cyber Defence) oder Anwendungen zur Entscheidungsunterstützung und zur Generierung relevanter Lageinformationen zu nennen.

In dieser Situation ist es selbstverständlich, auch bei der wehrtechnischen Forschung, die Setzung von Prioritäten und die bessere Ausnutzung von Kooperationspotenzialen in den Vordergrund zu stellen, ohne jedoch die nationalen Sicherheitsinteressen und die Fähigkeit zur Urteils- und Beratungsfähigkeit zu gefährden, eine Aufgabe, die im Wesentlichen von den wehrtechnischen Instituten und Dienststellen aufgrund ihrer Neutralität und Unabhängigkeit von Marktinteressen geleistet wird.

## Nationale Kooperation

Vorteilhaft für die IKT–F&T im Bereich Sicherheit und Verteidigung ist, dass der zivile Markt in großem Umfang die relevanten technologischen Basistechnologien hervorbringt. Diese sind auf Nutzbarkeit für wehrtechnische Zwecke, z.B. der Bedrohungsabwehr, zu prüfen und ggf. entsprechend durch anwendungsbezogene Weiterentwicklung anzupassen. Durch die Kooperation von Forschungsinstituten, denen die Identifikation und Erschließung relevanter Basistechnologien und deren Kombination und Reifung zu für die Sicherheit und Verteidigung nutzbaren Technologien zukommt und der Industrie, die den Transfer in Anwendungsprodukte und das Ausrollen übernimmt, lassen sich die Stärken beider Partner kombinieren. Eigenentwicklungen von Technologien sind dabei nur noch in den Fällen erforderlich, wo nationale Sicherheitsinteressen berührt werden oder wo es keinen ausgeprägten zivilen Markt gibt.

## Internationale Kooperation

Gab es bis vor einigen Jahren noch eine strikte Trennung zwischen militärischer und ziviler Sicherheitsforschung, die zum Teil historisch begründet und politisch gewollt war, so gibt es inzwischen eine Annäherung und damit eine sich beständig intensivierende Zusammenarbeit. Das liegt natürlich auch darin begründet, dass das Aufgabenspektrum der Streitkräfte aufgrund aktueller militärischer Szenarien in vielen Details ähnlich zu denen ziviler Sicherheitsorgane ist. Beispiele sind “Schutz von Infrastrukturen” oder “Schutz und Rettung von Personen”. Dies gilt natürlich nicht nur für den Bereich IKT, ist hier aber besonders augenfällig.

In Europa kann man diesen Willen zur Zusammenarbeit an dem Verhältnis zwischen der European Defence Agency (EDA) und der EU Kommission feststellen, die zunächst unabhängig voneinander agierten, nunmehr aber inhaltlich ihre F&T–Programme abstimmen und damit Synergieeffekte nutzen und Doppelarbeit vermeiden.

Die Europäische Kommission stellt für 2007-2013 mit dem 7. Forschungsrahmenprogramm (FRP) über 50 Mrd. Euro für Forschung bereit, davon 1,4 Mrd. Euro für Sicherheitsforschung. Über ein Viertel davon wird für reine IKT–Themen ausgeschüttet. Da aber auch in den anderen Forschungsfeldern, bei denen der Fokus bspw. auf Transport oder Ener-

*Die AFCEA-Studienpreisträger 2011 mit ihren Professoren und den Mitgliedern der Jury*

gie liegt, informationstechnische Fragestellungen eine große Rolle spielen, ist der IKT-Anteil insgesamt der größte. Die Forschungsförderung soll im 8. FRP ab 2014 für weitere sieben Jahre und dann mit einem auf ca. 80 Mrd. Euro aufgestockten Budget fortgesetzt werden.

Neben der EU–Ebene gibt es eine Reihe bilateraler und multilateraler Kooperationen mit europäischen Partnern. Hervorzuheben ist die Zusammenarbeit zwischen den sechs Nationen Deutschland, Frankreich, Großbritannien, Italien, Spanien, Schweden im Rahmen des sog. LoI6 – Letter of Intent. Diese Nationen finanzieren über 90% der europäischen Rüstungsforschung. Basierend auf gemeinsamen Planungen werden unter diesem formalen Dach der gegenseitige Informationsaustausch über aktuelle F&T-Vorhaben organisiert und gemeinsame Projekte durchgeführt.

Wichtigste Organisation der NATO für F&T im Bereich der Verteidigung ist die Research and Technology Organisation (RTO). Daneben werden auch im Rahmen der NC3O mit der bisherigen NC3A (hier steht eine Umorganisation der gesamten NATO Agencies bevor, die auch zu einer Zusammenlegung der NC3A mit anderen Agenturen beinhaltet; siehe dazu den Beitrag von Wolfgang Taubert auf Seite 19) als ausführender Institution F&T-Arbeiten durchgeführt, die weit über allgemeine Standardisierungsansätze hinausgehen.

Die F&T Aktivitäten der NATO RTO sind in mehreren Panels mit spezifischem Fokus organisiert. IKT spielt zwar bei allen Panels eine Rolle, die Bearbeitung der Kernthemen der IKT für militärische Anwendungen werden vom Information Systems Technology Panel (IST) organisiert. Allgemein identifizieren Panels die relevanten Forschungsaufgaben. Dazu werden die nationalen Vorgaben, aber auch vielversprechende Technologiepotentiale als Ergebnis eines sogenannten "Technology Watch" herangezogen. Die eigentliche Forschungsarbeit wird unterhalb der Panels von sogenannten Research and Technology Groups (RTG) geleistet. Deren F&T-Aktivitäten sind in der Regel auf drei Jahre angelegt und werden meist von Wissenschaftlern und Industriemitarbeitern betrieben. Insgesamt sind bei der RTO mehr als dreitausend Spezialisten in diesen Teams organisiert, die an aktuellen militärischen Forschungsthemen arbeiten, davon ca. 450 im Bereich ITK. Ergebnisse der Aktivitäten sind in der Regel international abgestimmte Konzepte, gemeinsame Entwicklungen oder Standards, die bspw. in STANAGS einfließen.

Das Synergiepotenzial in der RTO in ihrem vorwettbewerblichen Arbeitsbereich ist sehr hoch, da mit der Beteiligung an einer Aktivität der Zugriff auf alle Ergebnisse der jeweiligen Arbeitsgruppen möglich ist. Die Beteiligung ist freiwillig, finanziert durch die entsendenden Nationen. Unter diesen Voraussetzungen hat sich eine Arbeitskultur entwickelt, die ohne großen administrativen Aufwand hohen Nutzen für alle Beteiligten ermöglicht. Die RTO bietet für wehrtechnische Anwendungen eine einzigartige Plattform zum Informationsaustausch. Wesentlich ist dabei auch die in Bezug auf das Gesamtspektrum der IKT-Forschung relativ seltene Gelegenheit zum Vergleich eigener Arbeiten im internationalen Kontext und damit zur Standortbestimmung bei der wehrtechnischen F&T.

Bundesamt für Informationsmanagement
und Informationstechnik der Bundeswehr

AFCEA Bonn e.V.
*Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung*

# Mobile Computing und Cyber Defence – (k)ein Widerspruch

Die Bundeswehr nutzt bereits heute eine Vielzahl mobiler IT-Geräte. Zukünftig wird sie noch stärker als in der Vergangenheit an den sprunghaften Entwicklungen des kommerziellen Kommunikationsmarktes teilhaben und von den Vorteilen mobiler Endgeräte profitieren. Die Hersteller dieser Technologie unternehmen zwar Anstrengungen, diese Geräte gegen Missbrauch zu härten. Ob deren Maßnahmen auch ausreichend sind, bleibt zu untersuchen und zu diskutieren.
Wir wollen Sie gern zur **gemeinsamen Fachtagung von AFCEA Bonn e.V. und IT-AmtBw am 30. August 2012** zu einem Gedankenaustausch einladen und mit Ihnen über Mobile Computing und Cyber Defence sprechen. In diesem Zusammenhang möchten wir Sie auch anregen, darüber nachzudenken, wie verhindert werden kann, dass diese beiden Sachverhalte im Widerspruch zueinander stehen.
In dieser kritischen Betrachtung der Themenfelder Mobile Computing und Cyber Defence erhoffen wir uns Antworten zu finden auf Fragen wie: Welche Strategien und Möglichkeiten des Schutzes der Informationen in diesem Umfeld gibt es? Welche Erfahrungen haben NATO, EU und Bündnispartner? Gibt es erfolgreiche Beispiele außerhalb der Bundeswehr, z.B. bei Banken, Versicherungen und großen Firmen? Welche Lösungsansätze hat die Industrie?

Wir laden Sie hiermit zu dieser Veranstaltung mit internationaler Beteiligung herzlich nach Koblenz ein und erwarten Sie zu einem interessanten Programm und einem unterhaltsamen Abend mit der Möglichkeit zu vielen Gesprächen.

| | | |
|---|---|---|
| Ort: | Falckenstein-Kaserne, Saal des Heeres, Von-Kuhl-Str. 50, 56075 Koblenz | |
| Zeit: | Donnerstag, 30.08.2012 | 09:00 – 18:30 Uhr |
| | mit “Koblenzer Abend” | 18:30 – 21:00 Uhr |
| Teilnehmer: | Bundesministerium der Verteidigung; Kommandobehörden, Ämter, Dienststellen und Truppenteile der Bundeswehr; Behörden und Organisationen mit Sicherheitsaufgaben (BOS); Institute, Verbände; Universitäten und Fachhochschulen; Industrie mit Schwerpunkt Informations- und Kommunikationstechnik; internationale Gäste | |
| Fachl. Leitung: | Brigadegeneral a.D. Reimar Scherz, Vorstand AFCEA Bonn e.V.<br>Brigadegeneral Klaus F. Veit, Vizepräsident IT-AmtBw | |
| Programm: | + | aktuelle Informationen unter www.afcea.de und www.it-amtbw.de |
| Kostenbeitrag: | + | Eintritt: 75,- € |
| | + | Öffentlicher Dienst und AFCEA-Mitglieder: Eintritt kostenfrei; es wird jedoch ein Betrag von 15,- € für die Verpflegung erhoben. |

Klaus F. Veit, Brigadegeneral
Vize-Präsident IT-AmtBw

Erich Staudacher, Generalmajor
Vorsitzender AFCEA Bonn e.V.

AFCEA Bonn e.V., Borsigallee 2, 53125 Bonn, Tel.: 02 28 / 9 25 82 52, Fax: 02 28 / 9 25 82 53
IT-AmtBw, Ferdinand-Sauerbruch-Str. 1, 56073 Koblenz, Tel.: 02 61 / 4 00-41 01, Fax: -41 05

# Der neue Ausrüstungs- und Nutzungsprozess – eine Chance für die ITK-Branche

Joachim Mörsdorf, Stv. Vorsitzender AFCEA Bonn e.V., Sprecher Industriebeirat

*Joachim Mörsdorf*

Nach Aussage von Vertretern des Bundesministeriums der Verteidigung sind wir mitten in der größten Umstrukturierung und der deutlichsten Neuausrichtung der Bundeswehr seit ihrer Gründung. Die Aussetzung der Wehrpflicht und die damit einhergehende verstärkte Suche nach geeignetem Nachwuchs stellt eine völlig neue Herausforderung dar. Die wachsende Anzahl zunehmend komplexer und immer wieder für das Leben der Soldaten bedrohlicher Einsätze in aller Welt fordert neue Konzepte und neues Material. Ob es nun die größte Herausforderung ist oder "nur" eine der vielen bereits vollzogenen "Reformen": an herausfordernden Fragestellungen mangelt es der Bundeswehr derzeit wahrlich nicht.

Eine (Teil-)Antwort gibt der neu konzipierte Ausrüstungs- und Nutzungsprozess, in dem erstmals eine lebenszyklusübergreifende Bewertung von Rüstungs- und IT-Vorhaben erfolgen soll. Der bisherige Beschaffungsprozess war trotz grundsätzlicher Bewährung vor allem durch

- ein fehlendes Fähigkeitsmanagement über den gesamten Prozess,
- langwierige Abstimmungs- und Entscheidungsprozesse,
- hierdurch steigende Beschaffungskosten,
- zersplitterte Verantwortlichkeiten und Kompetenzbereiche,
- sowie Intransparenz und schwerfällige Kommunikationsstrukturen

geprägt.

Bereits in der Stellungnahme zur Erarbeitung des Berichts der Strukturkommission hat die Wirtschaft den bestehenden Prozess kommentiert und umfangreiche Verbesserungsvorschläge gemacht. Der Abteilungsleiter Ausrüstung/IT/Nutzung (AIN) hat kritische Punkte aufgenommen und im Vergleich zum alten Prozess zahlreiche weitere Verbesserungen eingearbeitet.

Dies bedeutet insbesondere

- die klare Festlegung der Verantwortlichkeiten und Zuständigkeiten im Gesamtprozess inklusive der Führung über Zielvereinbarungen,
- der grundsätzliche Vorzug für Lösungen auf Basis handelsüblicher Produkte und bereits entwickelter Komponenten,
- die Einbindung der Wirtschaft in die Integrierten Projektteams (IPT) zur Realisierung eines Beschaffungsvorhabens.

Mit Blick auf die ITK ergeben sich für die Industrie folgende Schwerpunkte:

- Anwendung des Beschaffungsprozesses nicht mehr in den Systemsäulen, sondern system- und projektübergreifend; d.h. konsequente Umsetzung eines funktionalitäts- und diensteorientierten Ansatzes.
- Verstärkte Nutzung von Off-the-shelf-Technologien; d.h. insbesondere Nutzung bestehender militärischer oder ziviler Off-the-shelf-Technologien bzw. Komponenten, wo immer diese zumindest gleichwertig oder aber durch die wesentlich frühere, wirtschaftlichere und risikofreiere Verfügbarkeit bei ausreichender Funktionalität bereits sinnvoll nutzbar sind.
- Aufbau eines kooperativen Beschaffungsprozesses statt eines "Zwei-Frontenverhältnisses" Auftraggeber-Auftragnehmer, d.h. insbesondere
  - Engere Zusammenarbeit von Auftragnehmer und Bundeswehr (u.a. BMVg, BAAINBw, Planungsamt) über den gesamten Projektverlauf,
  - Proaktives Führen von Dialogen mit Lieferanten seitens der Bundeswehr,
  - Aktive Informationsversorgung der deutschen Wirtschaft durch speziell hierfür vorgesehene deutsche Vertreter in internationalen Organisationen sowie spezifischer Exportunterstützung,
  - Erhöhung der auftraggeberseitigen Managementkompetenz.

Mancher Leser mag sich bei diesen Aussagen verwundert die Augen reiben, wo doch wesentliche der o.g. Forderungen in den heutigen Prozessen bereits beschrieben sind. Genau hierin liegt die Chance der ITK-Branche und speziell der mit-


*Die Fachausstellungen von AFCEA Bonn e.V. – eine wichtige Plattform für die mehr als 70 Mitgliedsfirmen*

telständisch orientierten Unternehmen. Für die Industrie sind im Rü/Nu-Prozess liegende Neuerungen Tagesgeschäft, die darüber hinausgehenden Konsequenzen (vor allem die Abkehr von spezifischen Neuentwicklungen in Großvorhaben) werden Synergien und Raum für innovative Ideen schaffen.

Die Einbeziehung der Nutzung bereits in der Planung von Vorhaben und die dafür erforderlichen Aufwendungen werden vor allem den mittelständischen Anbietern neue Möglichkeiten geben, innovative Ideen nicht nur vorzuschlagen, sondern auch den Praxisnachweis durch Realisierung erbringen zu können.

Es besteht allerdings ein Widerspruch zwischen "grundsätzlicher Bewährung" des CPM und dem formulierten "schlechten Ergebnis". Auch im bisherigen CPM bestand die Möglichkeit der beschleunigten Umsetzung von Forderungen, wenn alle Beteiligten die gleichen Interessen hatten! Wenn in der Neufassung der Wille zur konsequenten Umsetzung fehlt, ist eine solche aus Sicht der Industrie unnötig. Um die notwendigen organisatorischen Änderungen reibungslos zu implementieren, erscheint ein umfangreiches Change Management angezeigt. Hier können Erfahrungen aus der ITK-Branche einfließen.

An dieser Stelle lohnt ein Blick auf die vielfältigen Aussagen von Staatssekretär Stéphane Beemelmans, wonach die neuen Strukturen im Ministerium und auch im BAAINBw durch eine konsequente Durchmischung von zivilem und militärischem Personal bestimmt werden. Die integrierten Projektteams sind damit "nur" eine Ableitung. Die Zusammenführung des Know-hows aller am gesamten Lebenszyklus-Prozess beteiligten Personen (Nutzer, Bedarfsträger, Bedarfsdecker, Dienstleister/-Realisierer) ermöglicht den Ausgleich wegfallenden Personals und Dienststellen und damit den Erhalt der "Qualität der Bundeswehr".

Aus Sicht der ITK-Industrie konstatieren wir, dass die IPT die wesentliche Grundlage sind, um den Rü/Nu-Prozess effektiv gestalten zu können. Dies setzt allerdings voraus, dass die IPT-Mitglieder frei in ihrer Entscheidung sind und Beratungsunterstützung annehmen dürfen.

Die Teilhabe der Wirtschaft in den integrierten Projektteams steht in Abhängigkeit von der Auslegung der rechtlichen Zulässigkeit. Dies ist im Hinblick auf die Beschränkungen des Vergaberechts nachvollziehbar, jedoch dem Gesamtprozess abträglich. Ohne eine stete Beteiligung des jeweiligen Dienstleisters als Bestandteil des Realisierungsteams erscheint eine reibungslose Prozesssteuerung schwer möglich. Darüber hinaus ist das Aufgreifen von Ideen der Wirtschaft für die Weiterentwicklung der Bundeswehr in einer frühen Phase, wie in der Abteilung Planung im BMVg und im Planungsamt vorgesehen, hilfreich und zielführend.

## Wird die Erneuerung des Rü/Nu-Prozesses ein Erfolg?

Transparenz muss natürlich gewollt sein. Mit Hilfe der IT-Unterstützung kann schnell ein effektives Vorhabencontrolling einschließlich Meilensteinplanung und darauf aufbauend ein zugleich wirtschaftlicher und aus Sicht der Nutzer effektiver Prozess zur Anwendung gebracht werden.

## Wie immer im Leben

Der neue Ausrüstungs- und Nutzungsprozess bietet Chancen und Risiken. Er wird nicht verhindern, dass das absehbar begrenzte Budget des EPl 14 in den kommenden Jahren eine Reihe von möglicherweise auch schmerzlichen Einschränkungen und Einsparungen zur Folge hat. Aber vielleicht macht der neue effiziente Prozess "mehr" möglich als der bisherige. Das wäre bereits ein großer Vorteil. Auch muss das Thema "Leistungsstörungen" (ist immer nur die liefernde Industrie "schuld" an Terminverzögerungen oder geringerer Produktleistung?) angegangen werden.

## Fazit

Die Rolle und Bedeutung der ITK im Prozessbild der Bundeswehr wird insgesamt – relativ und absolut – weiter wachsen. Es liegt (auch) an uns, der ITK-Branche, dem Prozess der Neuausrichtung mit Rat und Tat zum Erfolg zu verhelfen.

# Die aktuelle NATO-Reform – IT-Unterstützung heute und morgen

Wolfgang Taubert, Vorstand AFCEA Bonn e.V. und Regional Vice President AFCEA International

*Wolfgang Taubert*

Es ist Reformzeit – nicht nur bei der Bundeswehr. Die NATO ist die erfolgreichste militärpolitische Organisation der Neuzeit, aber äußere Zwänge nach höherer Effektivität und Effizienz gehen auch an ihr nicht vorbei. Im Jahre 2010 haben die 28 NATO Nationen und der NATO Generalsekretär die Richtung vorgegeben – kleiner, effektiver und effizienter (und ein wenig sparsamer natürlich) soll es werden. Dabei wurden alle drei wesentlichen Pfeiler der NATO adressiert – das politische Hauptquartier in Brüssel, die militärische Kommandostruktur und die NATO Agenturen. Der zeitliche Rahmen der Reform ist sportlich. Noch im Jahr 2012 sollen wesentliche Reformziele erreicht und neue Strukturen eingenommen sein.

Das politische Hauptquartier der NATO befindet sich in Brüssel. Hier agiert der Internationale Stab und der Internationale Militärstab zur Unterstützung des NATO Generalsekretärs sowie des NATO Militärausschusses. Dies entspricht im weitesten Sinne ministeriellen Funktionen. Eine funktionale Reorganisation des NATO Hauptquartiers ist geplant und eine personelle Reduktion um ca. 10% ist absehbar.

Die NATO verfügt heute über 11 militärische Hauptquartiere – 2 strategische, 3 operative und 6 taktische Kommandos. Zwei dieser Taktischen Kommandos (Component Commands) befinden sich in Deutschland – Headquarters Allied Force Command Heidelberg und Headquarters Allied Air Command Ramstein. Alles in allem verrichten über 13.000 Soldaten ihren Dienst in den Hauptquartieren der NATO. Die Reform sieht eine Reduktion der Hauptquartiere auf 7 vor, die Zahl der Soldaten wird dann bei ca. 8.800 Soldaten liegen. Das Headquarters Allied Force Command Heidelberg ist eines der zur zu Schließung vorgesehenen Hauptquartiere.

Die NATO Agenturen dienen der NATO und ihrer Mitgliedsnationen als unterstützende Elemente. Im weitesten Sinne verfügt die NATO über 15 Agenturen in den Bereichen Informationstechnik, Rüstung und Logistik. Die Agenturen setzen unter anderem alle relevanten Investitionen der NATO um. Sie unterscheiden sich vor allem in ihrem Finanzierungprinzip deutlich. Die Rüstungsagenturen werden direkt von den beteiligten Nationen (‹ 28) finanziert. Die meisten der logistischen und IT-Agenturen werden aus dem allgemeinen NATO-Haushalt finanziert (28 Nationen, “common funded”) – das entspricht im wesentlichen den Finanzierungsprinzipien einer deutschen Behörde – jährliche Mittelzuweisung. Zwei der NATO Agenturen verfügen über ein sogenanntes Kundenfinanzierungsmodell (“customer funded”) – die finanziellen Mittel liegen bei den Kunden (Hauptquartiere, Nationen) und werden bei Projektauftrag bzw. Projektende den Agenturen überwiesen. Diese wiederum begleichen alle ihre Ausgaben (Gehälter, laufender Betrieb, Dienstreisen, …) aus einem Aufschlag auf die Projektkosten. Das erlaubt Flexibilität und führt zu Leistungsdruck. Auf der anderen Seite führt mangelhafte oder unpünktliche Projektarbeit und folgerichtiges Ausbleiben von “Folgeaufträgen” zu Defiziten im Budget der entsprechenden Agentur. Die Konsequenzen sind (nicht nur theoretisch) die Kürzungen bei Personal und anderen Ausgaben.

In den letzten Jahren ist nicht nur die Zahl der NATO Mitgliedsnationen stark gestiegen. Auch die Anzahl der Agenturen ist auf 15 angewachsen, zumeist mit Mitarbeiterzahlen um oder unter 100. Im Rahmen der NATO Reform wurde das politische Ziel vorgegeben, die Anzahl der Agenturen auf drei zu reduzieren. Ziel ist die Einrichtung einer Rüstungsagentur, einer Logistikagentur und einer IT-Agentur. Die Logistik- und IT-Agentur sind im Zeitplan und werden zum 1. Juli 2012 ihren Betrieb aufnehmen.

Soviel zum Prinzipiellen – wie sieht nun die konkrete IT-Unterstützung der NATO aus und wo geht die Fahrt hin. Mehr als 50% der NATO Investitionen gehen in den erweiterten Bereich der Informationstechnik – C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). C4ISR ist der Stoff (besser Klebstoff – “glueware”), der die NATO technisch zusammenhält. Im wesentlichen definiert sich die NATO bekanntlich über die natio-

nalen Beiträge ihrer Mitglieder. C4ISR ist hierbei die große Ausnahme von der Regel.

Im Bereich der Informationstechnik agieren heute 3 NATO-Agenturen – NACMA, NC3A und NCSA.

## NACMA – NATO Air Command and Control Management System Agency

Die NACMA wurde 1991 gegründet und dient der Realisierung des Projekts NATO Air Command and Control System (ACCS). Dieses Projekt soll in Zukunft das Rückgrat der NATO Luftverteidigung bilden. Die NACMA befindet sich in Brüssel und verfügt über ca. 100 Stellen (alle zivil). Die NACMA ist eine "common funded" Agentur. Eine erste operationelle Nutzung von ACCS ist für die kommenden Jahre geplant.

## NC3A – NATO Consultation, Command and Control Agency

Die NC3A wurde 1996 gegründet und verantwortet die Realisierung aller NATO C4ISR Projekte (mit der Ausnahme von ACCS). Diese ca. 600 Projekte werden seit 2001 unter dem Regime der Kundenfinanzierung ("customer funded") für die NATO sowie Mitglieds-/Partnernationen abgewickelt. Die NC3A hat zwei Hauptstandorte Den Haag und Brüssel sowie 5 Außenstellen (darunter Kabul und Kandahar) und verfügt über ca. 750 Stellen (700 zivil, 50 militärisch). NC3A-Projekte sind beispielsweise – AMN (Afghanistan Mission Network) und ICC (Integrated Command and Control Software for Air Operations). Diese Vorhaben sind in hunderten NATO und nationalen Kommandos erfolgreich im operationellen Einsatz. Darüber hinaus gehören alle NATO Projekte in Bereichen wie CyberDefence und Raketenabwehr zum Portfolio der NC3A.

*General Major Koen Gijsbers – künftiger General Manager der "NATO Communications & Information Agency"*

## NCSA – NATO Communication and Information Systems Services Agency

Die NCSA wurde 2004 gegründet und dient dem Betrieb der Informationstechnik der NATO Hauptquartiere (stationär und Einsatz). Die Agentur verfügt über ca. 4.000 Stellen (überwiegend militärisch) und hat ihr Hauptquartier in Mons (Belgien). Die NCSA ist an allen Standorten mit NATO Hauptquartieren sowie in Einsatzgebieten (wie Afghanistan) präsent. Die NCSA ist eine "common funded" Agentur. Ihre Kernaufgaben liegen im Betrieb der stationären IT-Infrastruktur der NATO Hauptquartiere sowie der Unterstützung der Einsätze der NATO mit mobilen IT-Komponenten. Die gesamte Betriebsunterstützung der NCSA erfolgt rund um die Uhr.

*NATO C3 Agentur Den Haag*

*NATO Agenturmitabeiter bei ISAF*

Die Zielvorgabe für die künftige IT Unterstützung der NATO besteht in der Schaffung einer einheitlichen Agentur zur Unterstützung des gesamten Lebenszyklus von IT-Projekten. Die Aufspaltung in zwei Projekt- und eine Betriebsagentur hat sich als semioptimal erwiesen. Darüber hinaus plant die NATO das Prinzip des "customer funding" auf die neue Agentur zu übertragen. Die neue "NATO Communications & Information Agency" wird alle C4ISR Projekte der NATO realisieren und betreiben. Sie wird die NACMA und NC3A komplett und große Teile der NCSA umfassen. Ein Teil der NCSA, verantwortlich für die mobile Unterstützung von NATO Einsätzen, wird als "CIS Group" bei SHAPE verbleiben. Ein neuer General Manager wurde im Oktober 2011 in einem Wettbewerbsverfahren gefunden. General Major Koen Gijsbers (Niederlande) wird am 1. Juli 2012 seinen Dienst aufnehmen. Die neue Agentur wird drei Hauptstandorte haben – Brüssel, Den Haag und Mons.

Die NATO hat sich mit der aktuellen Reform als außerordentlich handlungsfähig erwiesen und dabei auch den politischen Rahmenbedingungen (Finanzkrise) den nötigen und vertretbaren Respekt gezollt. In relativ kurzer Zeit wurde eine NATO Reform im Kontext des neuen strategischen Konzepts entworfen und befindet sich mitten in der Umsetzung. Damit wird die NATO gestärkt und agiler aus dem Reformprozess hervorgehen. Ihre Rolle als der zentrale Eckpfeiler deutscher Sicherheits- und Militärpolitik wird somit weiter manifestiert.

Im Bereich der Informationstechnik wird die NATO effektiver und effizienter werden – das Anreizsystem eines "customer funding". Eine Lebenszyklus-Betrachtung sind hierfür Garanten. Für die Bundeswehr wird sich der Trend zu einer strategischen Partnerschaft fortsetzen. Es geht zunehmend weniger um ausschließliches Geben (Ressourcen) als um ein Geben und Nehmen. Das Partizipieren an und die Übernahme von strategischen Projekten wie AMN und ICC haben das Potenzial zur schnellen Bereitstellung interoperabler Fähigkeiten und nicht zuletzt zum Kostensparen.

# AFCEA Veranstaltungskalender 2012

23. Januar
**Fachveranstaltung:**
**Mobile Computing – lebensrettender Sanitätsdienst**

27. Februar
**Info-Veranstaltung Young AFCEANs: Leadership Forum**

09. März
**Forum CeBIT 2012:**
**Cyber Defence Bundeswehr – Vom Schutz des IT-Systems Bw zur Security Awareness**

16. März
**Mittagsforum: AFCEA-Mitgliedsfirmen stellen sich vor**

22. März
**Parlamentarischer Abend (Berlin):**
**Quo vadis NATO – die NATO im Reformmodus**

23. April
**Fachveranstaltung: Die IT der Bundeswehr unter geänderten Rahmenbedingungen**

09./10. Mai
**26. Fachausstellung**
**Symposium: Mobile Computing im/für den Einsatz**

05. Juni
**BOS-Tagung: Mobile Computing – Anwendungsmöglichkeiten und Sicherheitsanforderungen**

28. Juni
**Mitgliederversammlung AFCEA Bonn e.V.**

05. Juli
**Fachveranstaltung AFCEA/BITKOM/EinsFüKdoBw:**
**Mobile Computing für die Einsätze der Bundeswehr**

30. August
**Koblenzer Fachtagung IT 2012:**
**Mobile Computing und Cyber Defence – (k)ein Widerspruch**

12. September
**Forum ILA 2012 – UAV**

24. September
**Info-Veranstaltung Young AFCEANs:**
**Mobile Computing mit Facebook, Twitter und Co – im täglichen Dienst und im Einsatz**

11. Oktober
**Fachexkursion**

26. Oktober
**Mittagsforum: AFCEA-Mitgliedsfirmen stellen sich vor**

14. November
**Techhnologieforum Fraunhofer FKIE**

19. November
**Fachveranstaltung: Herausforderung Cyber-Sicherheit**


Bundesamt
für Sicherheit in der
Informationstechnik

**AFCEA Bonn e.V.** und das **Bundesamt für die Sicherheit in der Informationstechnik (BSI )**
führen eine gemeinsame Fachveranstaltung durch mit dem Thema

# Mobile Computing

## Anwendungsmöglichkeiten und Sicherheitsanforderungen

Auch bei Behörden und Organisationen mit Sicherheitsaufgaben würden Angehörige im Dienst am liebsten modernste Kommunikationsmittel und mobile Computer so nutzen, wie sie es aus dem privaten Umfeld bereits gewöhnt sind.

iPhone, iPad und ähnliche Produkte mit einer großen Zahl bereits verfügbaren Apps mit unterschiedlichsten Funktionen bieten vielfältige Anwendungsmöglichkeiten auch für Sicherheitsbehörden. Die komfortable Nutzung steht jedoch im Spannungsfeld mit Sicherheitsaspekten, die gerade im BOS-Bereich besondere Bedeutung haben.

Wir konnten eine Reihe kompetenter Referenten gewinnen, die diese Thematik aus unterschiedlichen Perspektiven behandeln werden. Die Veranstaltung wird wieder Gelegenheit zu intensivem Gedanken- und Erfahrungsaustausch bieten.

**Zeit:** Dienstag, 5. Juni 2012, Programm 10.30 Uhr—17.30 Uhr
Ausklang/get-together 17.30 Uhr—19.00 Uhr

**Ort:** Fachhochschule des Bundes für öffentliche Verwaltung
Willy-Brandt-Str. 1, 50321 Brühl

**Moderator:** Dipl.-Ing. Dietrich Läpke, Vorstand AFCEA Bonn e.V, Aufgabenbereich BOS

**Vorläufiges Programm:**

| | |
|---|---|
| Leistungsfähige mobile GIS – Anwendungen | Michael Mundt<br>Esri Deutschland GmbH |
| Mobile Computing zur Lagebewältigung bei der Feuerwehr – heute und morgen | Mag. Franz Petter<br>Berufsfeuerwehr Hamburg |
| Mobile Computing zur Aufgabenerfüllung bei der Polizei | Guido Karl, Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen |
| Sicherheitsrisiken beim mobilen Arbeiten | Dr. Gerhard Schabhüser<br>Bundesamt für die Sicherheit in der Informationstechnik, AbtLtr Krypto-Technologie |
| Sichere Kommunikation mit dem Smartphone | Dr. Hans-Christoph Quelle<br>Secusmart GmbH |
| Sicherheitsaspekte im Bereich Mobility/ Situational Awareness | Dr. Dipl.-Ing. Dan Temmer, Rainer Halanek<br>Projects and Programs FREQUENTIS AG |

Das aktuelle Programm finden Sie stets unter : www.afcea.de/Veranstaltungen/Termine

# Das Angebot von AFCEA für Behörden und Organisationen mit Sicherheitsaufgaben (BOS )

Dietrich Läpke, Vorstand AFCEA Bonn e.V.

*Dietrich Läpke*

Überweisung der Besoldung aller Hamburger Polizeibeamter zum 1. Dezember ins Ausland statt auf die Privatkonten, massive Ausfallerscheinungen bei der IT der sächsischen Polizei und die Einstellung des Flugbetriebes an deutschen Flughäfen wegen Manipulationen am Sicherheitssystem – das sind nur einige wenige Szenarien aus der strategischen Krisenmanagementübung LÜKEX 2011.

Fast 3.000 Angehörige von Behörden des Bundes und der Länder, Betreiber kritischer Infrastrukturen sowie Verantwortliche aus Firmen und Verbänden übten am 30.11. und 1.12. 2011, was passiert, was nicht mehr funktioniert und was man tun muss, wenn "Spytool" die elektronischen Lebensadern des Landes angreift.

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zuständige Bundesbehörden für Vorbereitung und Durchführung der Übung konnten u.a. der Bundes- und Landespolizei an einigen Beispielen demonstrieren, vor welchen Herausforderungen sie stehen, wenn die Informations- und Kommunikationstechnik als Basisinfrastruktur und zur Gefahrenabwehr und Strafverfolgung nicht mehr wie gewohnt zur Verfügung steht. LÜKEX zeigte auch beispielhaft die heute schon allumfassende Abhängigkeit der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) von ständig verfügbarer und vor allem sicherer IT.

Als unabhängige und neutrale Plattform und auch als Impulsgeber für den Gedankenaustausch zwischen Forschung, Industrie und den Anwendern moderner I- und K-Technik möchte AFCEA sein Angebot auch gegenüber den zivilen BOS weiter öffnen. Eine besondere Chance dabei liegt in den Möglichkeiten des Wissenstransfers. Dafür bürgen die namhaften AFCEA-Mitgliedsfirmen, das breite fachliche Spektrum der Vorstandsmitglieder und die enge Zusammenarbeit mit BITKOM und ZVEI.

Besonders die jährliche Fachausstellung als "kleine CEBIT" bietet einen Überblick über die aktuelle technologische Entwicklung aber auch für Forschungs- und Entwicklungsansätze. In den letzten Jahren fokussieren sich die Aussteller neben den traditionellen militärischen Aspekten verstärkt auch auf die zivilen Anwendungen.

Nunmehr zum vierten Mal organisiert AFCEA am 5. Juni 2012 an der Fachhochschule des Bundes in Brühl seine BOS-Fachveranstaltung mit dem Thema "Mobile Computing – Anwendungsmöglichkeiten und Sicherheitsaspekte". Das Programm finden Sie auf Seite 22 dieser Broschüre. In diesem Jahr ist das BSI wieder Mitveranstalter. Im letzten Jahr konnten wir fast 150 Gäste zu interessanten Vorträgen und Diskussionsbeiträgen zur Thematik "Computerspionage und Computersabotage – akute Bedrohung für Wirtschaft und Behörden" begrüßen.

Beim Europäischen Polizeikongress des Behörden Spiegel im Februar 2012 in Berlin nutzte AFCEA erstmals die Gelegenheit, sich dem zahlreichen Publikum mit einem Informationsstand vorzustellen.

Insgesamt ist es AFCEA Bonn e.V. ein Anliegen, in einem integrativen Ansatz und in vielfältiger Form auch den BOS ein Forum zur Vernetzung mit Wirtschaft, Wissenschaft und anderen Sicherheitsbehörden zu bieten.

AFCEA Bonn e.V.
*Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung*

→ *700 Mitglieder*
→ *70 Mitgliedsfirmen*

# Neue Rahmenbedingungen für die Programmgestaltung

## Reimar Scherz, Stv. Vorsitzender AFCEA Bonn e.V., Leiter Programmbeirat

*Brigadegeneral a.D. Reimar Scherz*

AFCEA Bonn e.V. wird bald 30 Jahre alt – drei Jahrzehnte am Standort Bonn mit all seinen Veränderungen in der Politik, aber auch in der Bundeswehr und in den Behörden und Organisationen mit Sicherheitsaufgaben. Für die Stadt Bonn war sicherlich der Umzug der Bundesregierung nach Berlin die größte Zäsur. Neue Organisationen aus den Vereinten Nationen und Konzerne der Informations- und Telekommunikationsbranche haben diese Lücke zum größten Teil jedoch geschlossen. Ein neues Kongresszentrum in Anlehnung an den alten Plenarsaal des Deutschen Bundestages sollte ein Zeichen dieses Wandels werden.

AFCEA Bonn e.V. hat sich in dieser Zeit ebenfalls verändert. Von den Anfängen mit ein paar Fachveranstaltungen und einer jährlichen Fachausstellung wurde im Laufe der Zeit ein gemeinnütziger Verein, der ein umfangreiches Jahresprogramm anbietet. Der Erfolg der letzten Jahre zog neue persönliche Mitglieder und viele neue Firmen an. AFCEA Bonn e.V. wurde so zum größten europäischen Chapter von AFCEA International, einer weltweiten Organisation mit mehr als 33.000 Mitgliedern in den USA, in Asien und in Europa.

Trotz der vergangenen ständigen Anpassungen an die immer wieder neuen Rahmenbedingungen steht AFCEA Bonn e.V. jetzt vor einer neuen Lage. Die im letzten Jahr beschlossene Neuausrichtung der Bundeswehr ist so umfangreich und betrifft auch die Rheinregion in solch einem Umfang, dass AFCEA Bonn e.V. die Planung und Vorgehensweise stärker als in den früheren Jahren daran anpassen muss.

Bisher war das Bundesministerium der Verteidigung auf der Bonner Hardthöhe trotz des Berlinumzugs relativ unverändert geblieben. In der Abteilung Modernisierung waren der IT-Direktor und die Anteile der Informations- und Kommunikationstechnik konstante Ansprechpartner. Das Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) in Koblenz wurde mit seiner zuverlässigen Unterstützung für fast alle Veranstaltungen und ganz besonders für die jährliche “Koblenzer Fachtagung IT” ein herausragender Partner für AFCEA Bonn.

AFCEA Bonn e.V. muss sich in der Zukunft auf die neue Abteilung “Ausrüstung, Nutzung u. Informationstechnik” im BMVg einstellen, in der der IT-Direktor jetzt als Unterabtei-

*Der Präsident IT-AmtBw, Wolfgang Stolp, und sein Stellvertreter, BrigGen Klaus Veit, besuchen die Fachausstellung 2011*

lungsleiter wirkt, und muss die Verbindung zu dem neuem "Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr" (BAAINBw) aufbauen, in dem das BWB und das IT-AmtBw zusammengefasst werden. Trotz dieser einschneidenden Änderungen bleiben die Ansprechpartner von AFCEA Bonn e.V. aber weitestgehend erhalten. Einschneidender ist jedoch die Ausgliederung der Inspekteure und ihrer Stäbe aus dem BMVg und ihre räumliche Verlegung an andere Standorte in Deutschland. Wichtige und interessierte Teilnehmer von Heer, Luftwaffe und Marine werden künftig bei Veranstaltungen und vor allem bei der jährlichen Fachausstellung fehlen.

*AFCEA-Veranstaltungen bereiten Freude*

Auch die Veränderungen in der NATO sind nicht ohne Auswirkungen auf die Programmplanung. Bisher gab es 15 Agenturen in den Bereichen Informationstechnik, Rüstung und Logistik, die nun zu drei Agenturen verschmelzen. Der Fortfall der NATO C3 Agency (NC3A) und der NATO Communication and Information Systems Services Agency (NCSA) sind dafür nur zwei Beispiele. Die neue NATO Communications & Information Agency fasst bisherige Aufgaben zusammen, reduziert aber auch die Anzahl der kompetenten Ansprechpartner.

Das Jahresprogramm 2012 von AFCEA Bonn e.V. ist bereits ein erster vorsichtiger Schritt in eine neue Richtung. Nach wie vor wird es noch die Fachveranstaltungen, die Informationsveranstaltungen für die Young AFCEANs, die Mittagsforen, die BOS-Tagung und vor allem die Fachausstellung geben. Es werden aber bereits zwei neue Veranstaltungen in das Programm genommen, die nicht am Standort Bonn stattfinden werden. Ein Parlamentarischer Abend in Berlin soll die Abgeordneten und die Teile des BMVg ansprechen, die in der Bundeshauptstadt wirken. Eine gemeinsame Veranstaltung mit BITKOM, dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., und dem Einsatzführungskommando der Bundeswehr soll viele neue Teilnehmer am Standort Potsdam erreichen.

Wie in der Vergangenheit legen wir weiterhin großen Wert auf gemeinsame Veranstaltungen mit Partnern. Die "BOS-Tagung" an der Fachhochschule des Bundes in Brühl ist dafür ein gutes Beispiel. Ein weiteres Beispiel ist die "Koblenzer Fachtagung IT", die seit dem Jahr 2005 in bewährter Zusammenarbeit mit dem Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr vorbereitet und durchgeführt wird. Auch wenn das IT-AmtBw in der neuen Struktur mit dem BWB zusammengefasst wird, so wird es weiter diese Veranstaltung am Standort Koblenz geben. Auch die Zusammenarbeit mit dem Fraunhoferinstitut FKIE in Wachtberg wird weiterhin große Priorität haben. Diese Partnerveranstaltungen werden in Zukunft aber in größerem Umfang außerhalb des bisherigen Wirkungsbereichs von AFCEA Bonn e.V. durchgeführt. Nur so können das Heer am Standort Strausberg, die Luftwaffe in Berlin und die Marine in Rostock erreicht werden.

AFCEA Bonn e.V. wird bei diesen externen Veranstaltungen die Zusammenarbeit mit dem Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI) und mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) suchen und diese ausbauen. Auch Auftritte bei ausgesuchten Veranstaltungen wie z.B. der jährlichen Berliner Sicherheitskonferenz des Behörden Spiegel und der CeBIT in Hannover sind Möglichkeiten, neue Teilnehmer anzusprechen. In diesen beiden Fällen bietet sich auch eine Partnerschaft mit der AFCEA Europe an. Diese zentrale Geschäftsstelle von AFCEA International in Brüssel nimmt seit Kurzem mit weiteren europäischen Chaptern auch an ausgesuchten, wichtigen Veranstaltungen in Deutschland teil – eine gute Chance für AFCEA Bonn e.V., sich als größtes Chapter in Europa einem breiten Fachpublikum vorzustellen.

Veränderungen der Rahmenbedingungen sind Herausforderungen für einen gemeinnützigen Verein, der sich fast ausschließlich auf ehrenamtliche Mitarbeiter stützt. Sie sind aber auch Chancen, Neues zu wagen und lange Geplantes endlich zu realisieren. Die Programmgestaltung für 2012 berücksichtigt beide Aspekte: bisher Bewährtes wird mit neuen Ansätzen verbunden. AFCEA Bonn e.V. – ein Chapter, das sich bewegt und das seinen besonderen Platz im großen Verbund von AFCEA International behaupten wird!

rs*IntCent*®

# ++ Bundeswehr setzt auf rs*IntCent*® Auswertesoftware ++

## rola liefert System SIEKA für das KdoStratAufkl und zur Einsatzunterstützung

Marineeinheiten, Spezialkräfte und das Einsatzführungskommando konnten bereits in den vergangenen Jahren mit der IT-Lösung aus Oberhausen unterstützt werden. Inzwischen nutzt auch das Kommando Strategische Aufklärung die Software für Informations-Auswertung zum Schutz deutscher Einsatzkräfte in Afghanistan. Die Auswertesoftware **rs*IntCent***® wurde innerhalb eines Projektes zur strukturierten Informationserschließung in der Kommunikationsaufklärung (SIEKA) eingeführt.

**Lagebild:** Eine Lagefeststellung, die alle verfügbaren relevanten Informationen berücksichtigt und zueinander in Beziehung setzt, ist die Grundlage für die Beurteilung der Lage und für die Entscheidungsfindung. Nur wenn möglichst alle Informationen und Erfassungen ausgewertet, aufbereitet und für die Berichterstattung genutzt werden, kann das KdoStratAufkl den geforderten Beitrag zur Erstellung eines umfassenden Lagebilds leisten.

**Dynamische Auswertung:** Für Einsätze in Kriegs- und Krisengebieten ist es von vitaler Bedeutung, dass alle verfügbaren Informationen vorliegen, um die Lage der operierenden Einheiten einzuschätzen und absichern zu können. Einzelerkenntnisse müssen verarbeitet und in einen Zusammenhang gestellt werden, um die Analyse von Netzwerken – z.B. terrorverdächtiger Personen – durchführen zu können. Dies gilt im Vorfeld eines Einsatzes, um eine möglichst verlässlich Planungsgrundlage zu erhalten. Aber auch während des Einsatzes müssen weiter aktuelle Erkenntnisse gesammelt und effizient analysiert werden. Das heißt der Prozess der Informationsgewinnung und -auswertung muss dynamisch gestaltet werden können.

**rs*IntCent***®**:** Durch das **rs*IntCent***® System von rola werden Einzelerkenntnisse aus unterschiedlichsten Quellen – Humint, Sigint, MilNw – in einer Datenbank gesammelt. Durch zahlreiche Auswerte- und Analysemechanismen entsteht aus Einzelinformationen ein Informationsraum, der Beziehungen, etwa zwischen Personen, zwischen Personen und Orten oder Personen und Ereignissen (IED-Anschläge, Treffen) usw. sichtbar macht und in Diagrammen und Schaubildern verständlich darstellt – ein wesentlicher Beitrag zum Lagebild!

**Mobilität:** Mit der Verwendung mobiler Einsatzkomponenten (Mobile Computing) können diese Informationen im Reachbackverfahren zwischen den beteiligten Dienststellen ausgetauscht und repliziert werden. Abstimmungsprozesse werden spürbar beschleunigt. Zudem wird ein wesentlicher Beitrag zur Force Protection geleistet.

**Sicherheit:** rola Security Solutions konnte die IT-Lösung jeweils fristgerecht innerhalb kürzester Zeit einsatzbereit im vollen geforderten Funktionsumfang und budgetgerecht zur Verfügung stellen – inklusive der Erstellung projektbezogener Konzepte (z.B. IT-Sicherheitskonzept) und unter Beachtung aller datenschutzrechtlichen Vorgaben.

**Weitere Informationen unter www.rola.com.**

rola SECURITY SOLUTIONS

ZVEI:
Die Elektroindustrie

# Fachverband Sicherheit

## Sicherheit verbessern und Wertschöpfung in Deutschland sichern.

Vernetzte Welten sicher gestalten, die Wertschöpfungsanteile der deutschen Industrie erhalten und ausbauen und die nachhaltige Finanzierung sicherzustellen – das sind die strategischen sicherheits- und verteidigungspolitischen Aufgaben der Zukunft.

Sicherheit ist Standortfaktor und – im Falle Deutschlands – Standortvorteil. Die deutsche Elektrotechnik- und Elektronikindustrie ist mit ihren innovativen Lösungskonzepten und ausgereiften Produkten der leistungsfähige Partner für die Bewältigung der anstehenden Aufgaben. Wie keine andere Branche liefert die Elektrotechnik- und Elektronikindustrie Produkte und Lösungen, die das künftige Zusammenleben der Menschen wesentlich beeinflussen werden. Als Schlüsselindustrie – unsere Branche trägt mit ihren Innovationen überproportional zum Wirtschaftswachstum bei – entscheidet sie zudem maßgeblich über die Zukunftsfähigkeit Deutschlands. Diesen Aufgaben stellen wir uns heute und in der Zukunft. Im Fachverband Sicherheit bündelt der ZVEI mit einem breiten Fokus das Thema Sicherheit mit den Leitmärkten Safety, Security und Defence und bringt die Sicherheitsthemen in der Gremienarbeit nach vorn.

Der ZVEI übernimmt in einer zunehmend vernetzten Welt Verantwortung, hilft, Zukunft zu sichern und gestaltet diese aktiv mit.

### Leitmarkt Safety

**Sicherheit in Gebäuden und Anlagen**

### Leitmarkt Security

**Innere/ Öffentliche Sicherheit**

### Leitmarkt Defence

**Äußere Sicherheit/ Landes-verteidigung**

# Vernetzte Welten sicher gestalten – Sicherheit in einer vernetzten Welt

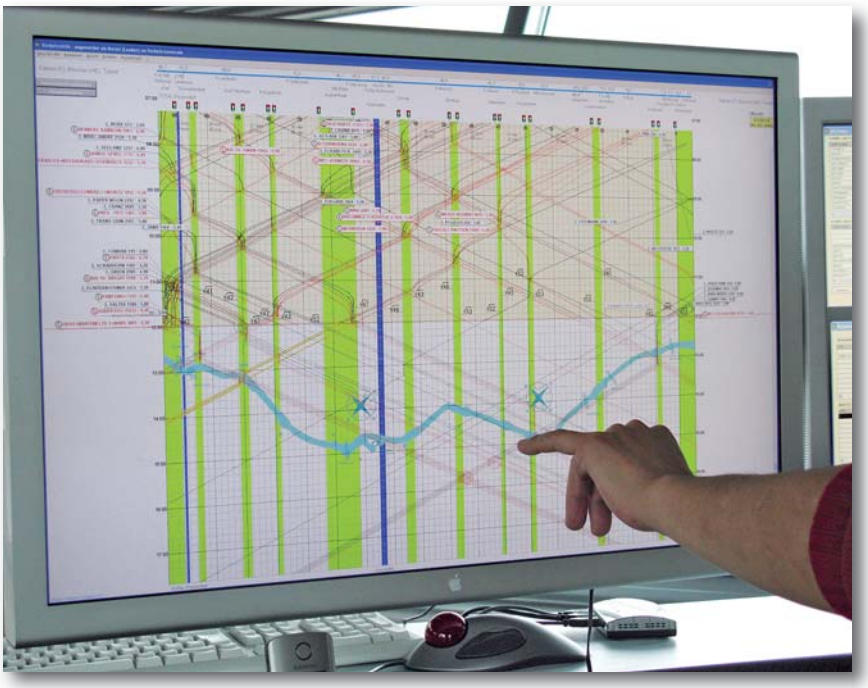
Dr. Klaus Mittelbach, Vorsitzender der Geschäftsführung des ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

*Dr. Klaus Mittelbach*

Vernetzte Welten sicher gestalten, die Wertschöpfungsanteile der deutschen Industrie erhalten und ausbauen und eine nachhaltige Finanzierung sicherstellen – das sind die strategischen industrie-, sicherheits- und verteidigungspolitischen Aufgaben der Zukunft. Unsere Branche, die Elektroindustrie, weiß um die schwierigen Aufgaben sowohl der internationalen Staatengemeinschaft wie der nationalen Politik und bietet sich als starker Partner an. Die deutsche Elektroindustrie verfügt mehr denn je über technologische Lösungen für gesellschaftlich drängende Fragestellungen, die aus der Globalisierung, der demografischen Entwicklung oder dem Klimawandel erwachsen. Der ZVEI bündelt dieses Wissen in seinen Kompetenzzentren und bringt es umfassend auf Konferenzen, Messen und im politischen Dialog ein.

Die Welt wächst weiter zusammen mit vielfältigen Verflechtungen und steht dabei vor enormen Herausforderungen. Die umfassende Vernetzung umfasst alle Lebensbereiche, sowohl in der militärischen, als auch in der zivilen Welt. Was vor Jahrzehnten bereits postuliert und angestrebt wurde, ist in den letzten Jahren durch neue leistungsfähige Technologien möglich und wirklich geworden. Umfassende Vernetzung betrifft nicht nur den jeweiligen Betrieb oder Organisation, sondern verlängert sich bis zu den Lieferanten und Kunden/Abnehmer.

Die konzeptionellen Vorstellungen der umfassenden militärischen Vernetzung im Sinne von Network Centric Operations hat die Bundeswehr mit dem Konzept der Vernetzten Operationsführung (NetOpFü) umgesetzt. Sie realisiert es durch den Zulauf neuer Systeme, die bei den Auslandseinsätzen auch den Zugang in die zivile Welt von Regierungen und Nichtregierungsorganisationen, von örtlicher Industrie und Dienstleistern ermöglichen.



*Weg-Zeit-Diagramm*

*Quelle: Wasser-und Schifffahrtsdirektion Nord, Kiel*

Doch neben den unschätzbaren Vorteilen und Synergien einer umfassenden Vernetzung stehen auch Risiken und Gefahren. Wir machen uns gerade auf den Weg in die 4. Industrielle Revolution: Künftig können Fabriken, Unternehmen und ganze Wertschöpfungsnetzwerke im Internet der Dinge und der Dienste in nahezu Echtzeit gesteuert werden. Die vertikale Vernetzung eingebetteter Systeme mit betriebswirtschaftlichen Prozessen bietet neben ganz neuen Geschäftsmodellen erhebliche Optimierungspotenziale in Produktion, Logistik und Vermarktung. Aber wie kann industrielle Wertschöpfung unter

diesen Bedingungen sicher organisiert werden? Wie kann Wohlstand unter sicheren Rahmenbedingungen erzielt, gerechter verteilt und trotz neuer Risiken und Gefahren dauerhaft gesichert werden? All diese Herausforderungen stehen in Beziehung zueinander, sind gewissermaßen “vernetzt”, wobei durch die vervielfachten Wechselwirkungen es nochmals schwieriger ist, Lösungen für sie zu finden.

Mit den Terroranschlägen von New York, Madrid und London hat sich die europäische und deutsche Sicherheitslage spürbar verändert. Es ist deutlich geworden, dass die strikte Trennung von äußerer und innerer Sicherheit nach Ende des Ost-West-Konflikts obsolet geworden ist. Sicherheit ist ein Schlüsselfaktor für die Gesellschaft in einer globalisierten Welt geworden. Nur mit einer Strategie der vernetzten Sicherheit kann der Schutz der Gesellschaft in einer zunehmend vernetzten Welt gewährleistet werden. Dies beinhaltet die Akzeptanz von Sicherheitstechnik in der Öffentlichkeit und der Politik. Nicht umsonst spielen die gesellschaftlichen Aspekte der zivilen Sicherheit eine zentrale Rolle im neuen Sicherheitsforschungsprogramm der Bundesregierung. Nur wer Technologien sicher handhaben und zum Effizienzgewinn einsetzen kann, kann Vertrauen gewinnen und Märkte schaffen. Die wachsende Wertschätzung der Elektroindustrie in der Politik ist ein Ausdruck dieses Vertrauens.

Sicherheit ist Standortfaktor und – im Falle Deutschlands – Standortvorteil. Die deutsche Elektrotechnik- und Elektronikindustrie ist mit ihren innovativen Lösungskonzepten und ausgereiften Produkten der leistungsfähige Partner für die Bewältigung der anstehenden Aufgaben. Wie keine andere Branche liefert die Elektrotechnik- und Elektronikindustrie Produkte und Lösungen, die das künftige Zusammenleben der Menschen wesentlich beeinflussen werden. Als Schlüsselindustrie – unsere Branche trägt mit ihren Innovationen überproportional zum Wirtschaftswachstum bei – entscheidet sie zudem maßgeblich über die Zukunftsfähigkeit Deutschlands. Diesen Aufgaben stellen wir uns heute und in der Zukunft. Der ZVEI übernimmt in einer zunehmend vernetzten Welt Verantwortung, hilft, Zukunft zu sichern, und gestaltet diese aktiv mit.

# Der Fachverband Sicherheit im ZVEI – Kompetenzen in drei Leitmärkten

Gert van Iperen, Vorsitzender des Vorstands des ZVEI-Fachverbands Sicherheit und Peter Krapp, Geschäftsführer des ZVEI-Fachverbands Sicherheit

*Gert van Iperen, Vorsitzender des Bereichsvorstands der Bosch Sicherheitssysteme GmbH*

*Peter Krapp*

Sicherheitsmärkte und Sicherheitstechnologien sind in stetigem Wandel, ebenso die Aufgaben und Anforderungen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Politik, die Unternehmen und nicht zuletzt die Verbände versuchen, diesen Wandel zu gestalten und daraus resultierende Chancen zu ergreifen. Der ZVEI hat der beschleunigten Entwicklung frühzeitig Rechnung getragen und alle Aspekte der Sicherheit durch die Zusammenführung der ehemaligen Fachverbände Sicherheitssysteme (Sicherheit in Gebäuden und Anlagen) und Wehrtechnik unter dem Dach des neuen Fachverbandes Sicherheit Rechnung getragen, um in der Gremienarbeit umfassende Synergien zwischen unterschiedlichen Bereichen zu heben. Im Fachverband Sicherheit mit den Leitmärkten Safety, Security und Defence werden aktuelle Herausforderungen der Inneren/Öffentlichen Sicherheit aufgegriffen, wobei der Fokus des ZVEI dort vor allem auf den Bereichen des Bevölkerungs- und Katastrophenschutzes sowie Krisenmanagement, dem Schutz kritischer Infrastrukturen und öffentliche Räume, der Überwachung und Kontrolle von Grenzen sowie der maritimen Sicherheit liegt.

Dem Begriff “Leitmarkt” liegt unsere Überzeugung zugrunde, gemeinsam mit der Produktkompetenz der einen und der Systemkompetenz der anderen Unternehmen mehr erreichen zu können, als wenn jeder für sich allein marschiert. Besondere Aufmerksamkeit werden wir künftig dem Querschnittsthema Thema Cyber-Sicherheit widmen; sie wird entweder die Achillesferse oder das Sprungbrett zu neuen Märkten sein.

Dass wir mit der Überwindung der bisherigen Grenzen – auch zwischen Verbänden! – und der gemeinsamen Themenbearbeitung in Leitmärkten den richtigen Weg eingeschlagen haben, zeigen uns die Bewegungen der Amtsseite und der Politik: Unsere bisher punktuellen Kooperationen mit der Polizei münden in naher Zukunft in ein gemeinsames, verbändeübergreifendes Symposium mit der Polizei zu Forschungsfragen, die sich zum Thema Sicherheitsforschung damit komplett neu aufstellt. Unser Vorschlag, die Anforderungen der Industrie an künftige Kooperationen und die dazu notwendigen Rahmenbedingungen beim Thema Logistik im Dialog mit der Bundeswehr zu diskutieren und den Gedankenaustausch zu intensivieren, ist beim zuständigen Staatssekretär Beemelmans auf ein sehr positives Echo getroffen. Und schließlich wird auch das Bundeswirtschaftsministerium mit dem “Masterplan Zivile Sicherheitswirtschaft” die Konzeption des “Zukunftsmarktes zivile Sicherheit” fortschreiben, um das Thema Sicherheit als Wirtschaftsfaktor in Deutschland auszubauen. Nur gemeinsam können wir beim Thema Sicherheit etwas bewegen.


*Der neue ZVEI-Fachverband Sicherheit*

*Quelle: ZVEI*

# Der Leitmarkt Security im ZVEI-Fachverband Sicherheit

## Peter Obermark, CEO und Vorsitzender der Geschäftsführung Thales Deutschland

*Peter Obermark, Vorstand des ZVEI-Fachverbands Sicherheit*

Sicherheit in einer vernetzen Welt zu gestalten, zählt zu den zentralen Herausforderungen, denen sich Politik, Industrie und Wissenschaft im 21. Jahrhundert stellen müssen. Die Auswirkungen der voranschreitenden technischen und sozialen Vernetzung, aber auch die übergreifende Bedeutung der aktuellen Wirtschafts- und Finanzkrise erhalten wachsende Bedeutung für die weitere Gestaltung der sicherheitspolitischen Rahmenbedingungen, wie dieses in der Vergangenheit bereits für das Ende des Kalten Krieges oder die Anschläge vom 11. September 2001 gegolten hat.

Hieraus ergeben sich verschiedene Trends auf Staaten und deren Sicherheitsorgane, auf die aber auch Industrie und Wirtschaft reagieren müssen. Die Konfliktbilder der vergangenen Jahre haben uns bereits gelehrt, dass sich die dogmatische Trennung zwischen Fragen der “inneren” und “äußeren” Sicherheit in der Praxis überholt hat. Die Einsätze westlicher Streitkräfte auf den Balkan, in Afghanistan und anderen Krisengebieten beinhalten in weiten Teilen Aufgaben mit polizeilichem Charakter. Die Abwehr von Piraten vor dem Horn von Afrika bewegt sich seit Jahren im Spannungsfeld der quasi-polizeilichen Aufgabe der Kriminalitätsbekämpfung, die jedoch aufgrund der Ausrüstungs- und Personallage weitgehend von der Marine wahrgenommen wird.

Die Praxis verlangt von den Sicherheitsbehörden also ressortübergreifend zu arbeiten und zu denken. Die Folgen der Wirtschafts- und Finanzkrise werden diesen Trend zur gemeinschaftlichen Aufgabenwahrnehmung verstärken, nachdem es in praktisch allen westlichen Staaten in den kommenden Jahren zu einem erheblichen Absinken der Verteidigungsetats kommen wird, was – wie im Falle der Bundeswehr – ebenfalls Reduzierungen des Umfangs der Streitkräfte nach sich zieht. In manchen Staaten Europas kommt es zudem zu einem gänzlichen oder zeitweisen Verzicht der Streitkräfte auf bestimmte Fähigkeitskategorien. Um vor diesem Hintergrund die eher gestiegenen sicherheitspolitischen Herausforderungen zu bestehen – laut UNHCR befanden sich im Jahr 2011 weltweit 43,7 Millionen Menschen auf der Flucht, die höchste Zahl seit 15 Jahren – sind Effizienzsteigerungen durch eine verstärkte Zusammenarbeit der verschiedenen staatlichen Ressorts, aber auch durch Einbeziehung der Wirtschaft, unabdingbar.

Außerdem werden neue Sicherheitsparadigmen nach neuen Antworten verlangen. Die Umbrüche des letzen Jahres in vielen arabischen Staaten waren nicht zuletzt getragen von den Möglichkeiten einer freien Kommunikation in sozialen Netzwerken auf der Basis einer kaum kontrollierbaren Internetstruktur. Gleichzeitig erkennen wir in der rasant steigenden technischen Vernetzung aber auch Risiken, da mit der zunehmenden Durchsetzung unserer Lebensbereiche mit IT, die zudem oftmals internetbasiert ist, auch eine neue Art der Angreifbarkeit einher geht. Mit der Diskussion um die Stuxnet-Malware wurde erstmals auch in einer breiten Öffentlichkeit eine mögliche Betroffenheit der Industrie durch Cyberangriffe thematisiert. In dem Maße, in dem in den kommenden Jahren auch Kritische Infrastrukturen in unserer Gesellschaft zunehmend von funktionierender IT und dem Internet abhängen, wird dieses Thema weiter an Relevanz gewinnen. Wir stehen hier erst am Anfang der Entwicklung eines neuen Handlungsraums, der gleichfalls nach neuen Antworten in sicherheitstechnischer Hinsicht verlangt. In diesem Bereich die künftigen Lösungen im Gleichgewicht zwischen bürgerlicher Freiheit und staatlicher Sicherheitsvorsorge zu erarbeiten, wird eine Aufgabe sein, bei der sich auch die Industrie durch neue Ansätze engagieren muss. Daneben bleiben die bekannten Herausforderungen der kommenden Jahre wie Migration, Urbanisierung, Rohstoff- und Nahrungsmittelknappheit sowie das Management und die Bewältigung von Naturkatastrophen und Großschadenlagen ständige Schwerpunkte unserer sicherheitspolitischen Überlegungen.

Um diese komplexen Themen in einer systematischen und für die Wirtschaft greifbaren Weise aufzubereiten, wird die Bearbeitung im Leitmarkt Security des Fachverbandes Sicherheit im ZVEI in den Fachkreisen

- Maritime Sicherheit,
- Überwachung und Kontrolle von Grenzen,
- Bevölkerungs-, Katastrophenschutz und Krisenmanagement,
- Überwachung und Kontrolle von Grenzen

wahrgenommen. Fragen der Cybersecurity finden im Fachverband Sicherheit eine querschnittliche Betrachtung, wobei auch aktiv andere Bereiche des ZVEI wie die Industrieautomation und Energietechnik einbezogen werden.

Die Arbeit im Leitmarkt Security ist dabei vom Gedanken getragen, durch moderne technische Lösungen zur Effizienzsteigerung und zur Ermöglichung der Nutzung von Synergien bei der behördlichen Aufgabenerfüllung beizutragen, aber auch Sicherheitslösungen für den privaten Sektor zu betrachten. Beispiele sind etwa der Austausch mit dem Maritimen Sicherheitszentrum in Cuxhaven, in dem verschiedene Bundesressorts und Länderpolizeien ihre Arbeit koordinieren. Weiterhin arbeiten verschiedene Mitgliedsfirmen des Fachverbandes Sicherheit in einem Projekt zur Abwehr von Piraten vor dem Horn von Afrika, welches wir in enger Abstimmung mit dem Bundesministerium für Wirtschaft und Technologie betreiben. Beim Thema Grenzüberwachung liegt der aktuelle Schwerpunkt im Leitmarkt Security auf dem Dialog mit Frontex, deren Rolle bei der Absicherung der EU-Außengrenzen durch die Neufassung der Frontex-Verordnung abermals gestärkt wurde. Nach einem kürzlichen Gespräch hierzu im Bundesministerium des Innnern, entwickeln wir diesen Bereich auch in Zusammenarbeit mit der Capacity Building Division von Frontex weiter. Cybersecurity nimmt eine zentrale Rolle im Leitmarkt Security ein, auch wegen der prominenten Stellung des Themas innerhalb des ZVEI. Neben der Beteiligung am Aufbau eines Kommunikationsnetzwerks zur Cyber-Sicherheit unter dem Dach des BDI und in Kooperation mit dem BSI engagiert sich der Fachverband Sicherheit mit einem eigenen Forum zur IT-Sicherheit auf der CeBIT unter dem Oberbegriff “Cybersecurity: Achillesferse oder Sprungbrett zu neuen Märkten?”. Hersteller und Anwender von IT-Systemen diskutieren dabei Themen und Trends, Märkte und Meinungen zum Thema Cybersecurity.

Im Leitmarkt Security stehen die Vernetzung und der übergreifende Charakter künftiger sicherheitspolitischer Fragestellungen sowohl als Rahmenbedingung als auch als Chance für langfristig tragfähige Lösungen im Fokus. Die Firmen des Leitmarktes stehen an der Spitze bei der Erarbeitung von Lösungen für die Herausforderungen unserer Zeit.

# Vom Einsatz her denken – auch im Leitmarkt Defence des ZVEI-Fachverbandes Sicherheit

Dipl.-Math. Gerhard Schempp, Vorsitzender der Geschäftsführung der ESG Elektroniksystem- und Logistik-GmbH

*Dipl.-Math. Gerhard Schempp, Vorstand ZVEI-Fachverband Sicherheit und Sprecher Leitmark Defence*

Der Leitmarkt Defence als eine der drei Säulen des Fachverbandes Sicherheit im ZVEI umfasst die Fähigkeiten der für die Bundeswehr tätigen Unternehmen mit den Kernkompetenzen für Entwicklung und Nutzung ihrer Elektronik- und ITK-Systeme im Verbund Führung, Aufklärung und Wirkung, in Ausbildung und Simulation und Logistik. Mit dem einzigartigen Know-how der Mitgliedsfirmen ist der Leitmarkt Defence der Wissensträger zur Steigerung der Fähigkeit zur Vernetzten Operationsführung (NetOpFü) und bietet die wichtigste Innovationsquelle zur zeitnahen Deckung von erkanntem Bedarf aus Einsatz und Grundbetrieb.

## Neuorientierung Bundeswehr und wehrtechnische Industrie

Die Bundeswehr befindet sich in einem massiven Veränderungsprozess. Die Ausrichtung der Streitkräfte auf Einsätze im multinationalen Verbund mit häufig wechselnden Einsatzkontingenten und Einsatzregionen führte zwangsläufig zur Optimierung der Bundeswehrstrukturen und der Prozesse zur Aufgabenbewältigung. Beschaffungs- und Nutzungsprozesse müssen unter Berücksichtigung geringerer Budgets den aktuellen Anforderungen angepasst werden. Der Bedarf der Ausstattung der Streitkräfte mit ITK-Lösungen orientiert sich bereits an den Einsatzerfordernissen. Die Reduzierung des personellen Umfanges der Streitkräfte macht es erforderlich, die Aufgabenteilung zwischen Bundeswehr und Industrie auf eine neue Basis zu stellen und Kooperationsmöglichkeiten verstärkt zu nutzen. Wesentliche Forderungen und Randbedingungen der Neuorientierung sind:

- Steigerung der Fähigkeit zur vernetzten Operationsführung mit Einbindung aller Sensoren und Effektoren bei umfassender Interoperabilität in streitkräftegemeinsamen und multinationalen Szenarien,
- schnelle Verfügbarkeit kostengerechter, einsatzreifer Lösungen mit geringem Ausbildungsaufwand, hoher Nutzerakzeptanz und uneingeschränkter Anbindung an den Grundbetrieb,
- Fokussierung und Optimierung der Logistikleistungen auf die Erfordernisse des Einsatzspektrums der Bundeswehr im Einsatzland und der Versorgungskette,
- intensive Nutzung von Technologiefortschritt und Optimierungsmöglichkeiten bei der Realisierung von ITK-Lösungen unter Verwendung verfügbarer Komponenten.

Für die Unternehmen des Leitmarktes Defence im Fachverband Sicherheit des ZVEI resultiert daraus die Notwendigkeit zu Veränderungen. Der Leitmarkt Defence hat mit seinen Unternehmen die Herausforderung angenommen und aktiv umgesetzt. Deutlich wird dieses z.B. durch:

- den Zusammenschluss der Fachverbände Wehrtechnik und Sicherheitssysteme im Sinne “Vernetzte Sicherheit” zum Fachverband Sicherheit mit den Leitmärkten Defence, Security und Safety mit mehr als 90 Unternehmen der ITK-Branche,
- der Neuausrichtung der Gremienarbeit im Leitmarkt Defence auf die Erfordernisse der Einsatzorientierung durch Umstrukturierung der Gremien und der Einrichtung des übergreifenden Fachkreises “Einsatzorientierung ITK/NetOpFü”.

## Erwartungen und Kompetenz

Der Leitmarkt Defence betrachtet sich als der flexible und innovative Partner der Bundeswehr. Der Mehrwert des Leitmarktes Defence und seiner Mitgliedsfirmen entsteht durch die kompetente Unterstützung der Ziele der Bundeswehr, im Wesentlichen über den querschnittlichen Einsatz von Schlüsseltechnologien in der Entwicklung und Nutzung von Systemen des Führungs-Aufklärungs-Wirkungsverbundes (C4ISR). Die Gremienarbeit des Leitmarktes ist darauf fokussiert. Als Know-how-Träger repräsentiert der Leitmarkt das

entscheidende Fähigkeitsprofil für schnell bereitstellbare und kosteneffiziente Lösungen zur Schließung von Ausrüstungs- und Prozesslücken. Diese Fähigkeit haben Unternehmen des Leitmarktes Defence in mehr als 100 sogenannten NetOpFü-Projekten vertragsgetreu nachgewiesen. Prägnante Beispiele sind multinationale Interoperabilitätsprogramme (wie MIP, ASCA), Führungsinformationssystem Streitkräfte, Führungsinformationssystem Heer, Mobiles Führungssystem Luftwaffe, Lösungen für die Streitkräftegemeinsame Taktische Feuerunterstützung STF, Multi-Sensor-Auswertesystem HERON-1 oder die Integration MILDS CH-53 GS aus dem Bereich "embedded ITK".

Die Unternehmen des Leitmarktes Defence im Fachverband Sicherheit sind den Weg der Transformation zusammen mit der Bundeswehr bisher erfolgreich gegangen. Nun geht es darum, die Technologiepotenziale zu erschließen, gemeinsam noch schneller, effizienter und effektiver zu nutzen, um den Grundbetrieb in der Heimatbasis sowie die Sicherheit und den Erfolg im Einsatzland weiter zu stärken. Entscheidend für den gemeinsamen Erfolg wird sein, dass die Industrie frühzeitig über konzeptionelle Überlegungen informiert und zu praktikablen Konditionen in "Integrierte Projektteams" zur Definition von Anforderungen und Lösungen partnerschaftlich eingebunden werden kann.

Vor dem Hintergrund knapper Haushaltsmittel und der Überschneidung von Innerer und Äußerer Sicherheit ist es nur folgerichtig, bereits erprobte und im Bereich der Streitkräfte erfolgreich genutzte ITK-Lösungen oder Technologien z.B. auch zum Schutz kritischer Infrastrukturen zukünftig verstärkt einzusetzen. Der Leitmarkt Defence stärkt mit den Erfahrungen seiner Mitgliedsunternehmen den Fachverband Sicherheit und schafft die Basis zum Heben der Synergiepotenziale.

*UAV Bodenkontrollstation* Quelle: Reiser Systemtechnik GmbH

## Fazit

Die nationale Verteidigungs- und Sicherheitsindustrie ist im Umbruch. Konsolidierungen und Internationalisierung verändern bestehende Wertschöpfungsketten nachhaltig. Die mittelständisch geprägten Firmen des Leitmarktes Defence im Fachverband Sicherheit des ZVEI halten mit Elektronik, ITK und Logistik das Know-how über die wichtigste Innovationsquelle für die Produkte und die Prozesse der Streitkräfte und aller Sicherheitsorganisationen bereit. Gemeinsam mit unserem Hauptkunden Bundeswehr und der Politik werden wir diese singulären und essenziellen Kenntnisse aufrechterhalten, stärken und ausbauen.

*Unmanned Mission Avionics Test Helicopter UMAT-®* Quelle: ESG GmbH

# Bundeswehr: Mitten im Einsatz und mitten in der Reform

Stéphane Beemelmans, Staatssekretär im Bundesministerium der Verteidigung

*Staatssekretär Stéphane Beemelmans*

Derzeit sind rund 7.000 deutsche Soldatinnen und Soldaten u.a. in Afghanistan, am Horn von Afrika oder auf dem Balkan im Einsatz. Sie tun dies oftmals unter erheblicher Gefahr für die eigene Gesundheit und das eigene Leben.

Trotz des vorbildlichen Einsatzes unserer Soldatinnen und Soldaten sowie unserer zivilen Mitarbeiterinnen und Mitarbeiter kann die Bundeswehr aber insgesamt noch leistungsfähiger werden. Eine zu geringe Anzahl verfügbarer Kräfte für den Einsatz, eine zu geringe Durchhaltefähigkeit, schwerfällige Entscheidungsprozesse und langjährige Unterfinanzierung sollen als Stichworte an dieser Stelle genügen.

Wir haben das Ziel, über Streitkräfte zu verfügen, die dem Stellenwert und der Verantwortung unseres Landes entsprechen und bei denen Auftrag und Mittel zusammenpassen. Im Ergebnis soll eine Bundeswehr mit einsatzbereiten und einsatzfähigen Streitkräften stehen, die effizientere Verfahren und Strukturen hat und in der Lage ist, die Aufträge zu erfüllen, die unser Land ihr gibt.

## Sicherheitspolitische Rahmenbedingungen

Nach der Beendigung des Kalten Krieges ist unsere territoriale Integrität militärisch nicht mehr bedroht. Damit ist das strategische Sicherheitsumfeld allerdings zunehmend komplexer und dynamischer geworden. Regionale Konflikte – obwohl ggf. geografisch weit entfernt – haben angesichts der politischen, wirtschaftlichen und technologischen Entwicklungen der vergangenen 20 Jahre einen nicht unerheblichen Einfluss auf unsere Sicherheit. Internationaler Terrorismus, die Verbreitung bzw. der Einsatz von Massenvernichtungswaffen und ihrer Trägermittel, Piraterie sowie neue mögliche zusätzliche Bedrohungen wie zum Beispiel Cyberangriffe sind die neuen sicherheitspolitischen Herausforderungen, vor denen wir stehen.

In den im Mai 2011 vom Bundesminister der Verteidigung erlassenen Verteidigungspolitischen Richtlinien sind aufgrund dieser sicherheitspolitischen Rahmenbedingungen für die Bundeswehr folgende ineinandergreifende Aufgaben definiert worden:

- Landesverteidigung als Bündnisverteidigung im Rahmen der Nordatlantischen Allianz,
- internationale Konfliktverhütung und Krisenbewältigung einschließlich des Kampfes gegen den internationalen Terrorismus,
- Beteiligung an militärischen Aufgaben im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik der EU,
- Beiträge zum Heimatschutz,
- Rettung und Evakuierung sowie Geiselbefreiung im Ausland,
- Partnerschaft und Kooperation als Teil einer multinationalen Integration und globalen Sicherheitszusammenarbeit,
- humanitäre Hilfe im Ausland.

## Welche Mittel benötigt die Bundeswehr zur Auftragserfüllung?

Die mögliche Vielfalt und Bandbreite potenzieller Konflikte führen dazu, dass die Bundeswehr eine breite Palette unterschiedlicher Fähigkeiten vorhalten muss, um im gesamten Aufgaben- und Fähigkeitsspektrum wirken zu können. Dieses Spektrum reicht von rein stabilisierenden Einsätzen – wie zum Beispiel auf dem Balkan –, über Einsätze in bewaffneten Konflikten – wie in Afghanistan – bis hin zu Kampfeinsätzen höchster Intensität. Hierzu werden hochprofessionelle Streitkräfte benötigt, die bestmöglich ausgestattet und ausgebildet sind. Als nationale Zielvorgabe ist festgelegt, dass zeitgleich rund 10.000 Soldatinnen und Soldaten durchhaltefähig in Einsätze entsendet werden können.

Dabei gilt es zu berücksichtigen, dass sich aufgrund der komplexen und dynamischen sicherheitspolitischen Lage Bedrohungsszenarien schnell ändern können. Gleiches gilt für die Lage in Einsätzen. Hier sind kurze Reaktionszeiten für die Bereitstellung jeweils angemessen ausgebildeter Soldaten und adäquaten Materials erforderlich. Deutsche Streitkräfte werden – mit der möglichen Ausnahme einer Evakuierungsoperation – nie für sich allein, sondern stets eingebunden in multinationale Koalitionen eingesetzt wer-

den, so dass der Interoperabilität mit Bündnispartnern eine besondere Bedeutung zukommt.

## Wie werden die Ziele der Neuausrichtung erreicht?

Die Schere zwischen militärisch Erforderlichem, technologisch Machbarem und finanziell Leistbarem stellt sowohl die Bundeswehr als auch die wehrtechnische Industrie vor große Herausforderungen.

Die in den Verteidigungspolitischen Richtlinien genannten Aufgaben der Bundeswehr werden dazu mit entsprechenden Fähigkeiten hinterlegt. Angesichts reduzierter Umfänge muss dabei nach dem Grundsatz “Breite vor Tiefe” vorgegangen werden. Die Bundeswehr wird im Ergebnis mit einer abgestuften Durchhaltefähigkeit im gesamten Aufgaben- und Fähigkeitsspektrum wirken können.

Um die Truppe schneller und effizienter mit dem benötigten Material auszustatten, wird im Rahmen der Neuausrichtung zudem die gesamte Beschaffungsorganisation gestrafft sowie der Rüstungs- und Nutzungsprozess optimiert. Dabei gilt, dass die Ausrüstung vor allem zeitgerecht, technisch hochwertig und einsatzreif in den festgelegten Parametern sowie im vereinbarten finanziellen Rahmen vorliegen soll.

Besondere Anforderungen gelten hier für die Informationstechnik, deren Funktionsfähigkeit als “Nervensystem” der Bundeswehr Grundvoraussetzung für ihre Handlungsfähigkeit ist. Um der hohen Innovationsgeschwindigkeit der IT und den Veränderungen im Einsatz und im Inland folgen zu können, ist unter anderem eine Konzentration auf überschaubare, schnell umsetzbare IT-Projekte erforderlich.

Im Rahmen der Neuausrichtung der Bundeswehr haben wir – unter Beteiligung der Industrie – eine neue IT-Strategie erarbeitet und in Kraft gesetzt. In dieser ist festgelegt, wie die Ziele der Bundeswehr – auch während des Übergangs in neue Strukturen – bestmöglich durch IT unterstützt werden können.

Insgesamt kann sich die Industrie darauf einstellen, dass langwierige Produktentwicklungen mit anschließenden Bestellungen von großen Stückzahlen durchweg nicht mehr möglich sein werden. Die Ausrüstung muss vielmehr möglichst marktverfügbar sein. Im Vordergrund werden dabei modulare Systeme stehen, die zu einem hohen Prozentteil unterschiedliche Einsatzszenarien abdecken und im Einzelfall einer lediglich geringfügigen Anpassentwicklung bedürfen. Das bedeutet, dass die wehrtechnische Industrie in Deutschland mit Blick auf das priorisierte Fähigkeitsprofil der Bundeswehr und den internationalen Markt auf eigenes Risiko Produkte entwickeln muss. Das bedeutet zugleich auch, dass große Stückzahlen letztlich nur unter Einbeziehung anderer als dem heimischen Markt erzielbar sein werden.

*Mobiler Gefechtsstand der Luftwaffe als Teil des MobFüSys-Lw*

*Quelle: ESG GmbH*

Die Neuausrichtung bietet jedoch auch für die Industrie zusätzliche Chancen. Durch die Konzentration der Bundeswehr auf ihre Kernaufgaben werden sich für die Industrie weitere Kooperationsmöglichkeiten ergeben. Ein möglicher weiterer Ausbau von Kooperationen ist beispielsweise in den Bereichen Logistik, Instandhaltung, IT und Ausbildung denkbar.

## Ausblick

Der organisatorische Rahmen der neuen Bundeswehr ist gesteckt. Jetzt geht es an die Umsetzung. Dabei gilt es zu berücksichtigen, dass die Einsatzfähigkeit der Bundeswehr gewährleistet bleibt. Angesichts der laufenden Einsätze und der gleichzeitig stattfindenden Neuausrichtung nutzen manche dabei das Bild von einer Reparatur bei laufendem Motor. Dieses Bild wird der Situation aber nur teilweise gerecht. Es handelt sich eher um eine Reparatur bei laufendem Motor in voller Fahrt.

Die Neuausrichtung wird daher nur gelingen, wenn sie als gemeinsame Aufgabe von Bundeswehr, Gesellschaft und wehrtechnischer Industrie verstanden wird. Wir setzen daher weiter auf eine enge Kooperation mit der Industrie. Nur dann wird es eine zukunftsfähige Bundeswehr geben.

Jetzt ist die Zeit, diese gemeinsame Chance zu nutzen!

# Die Konzeption des neuen Ausrüstungs- und Nutzungsprozesses

Ministerialdirektor Detlef Selhausen, Abteilungsleiter Ausrüstung, Informationstechnik und Nutzung, Bundesministerium der Verteidigung

*Ministerialdirektor Detlef Selhausen*

Die Beweggründe und Herausforderungen der Neuausrichtung der Bundeswehr sind hinlänglich bekannt und diskutiert. Ihre Notwendigkeit ist unbestritten. Auch der Rüstungsbereich ist von großen Veränderungen betroffen, deren Kern die Konzeption eines neuen Ausrüstungs- und Nutzungsprozesses bildet. Die Umsetzung führt zu einer Novellierung des CPM (Customer Product Management) und zu einer neuen Aufbauorganisation des Rüstungsbereiches, in der zivile und militärische Mitarbeiter und Mitarbeiterinnen in einer gemeinsamen Organisation eng miteinander zusammen arbeiten werden.

Für die Erarbeitung der Konzeption sind im Rahmen eines Projektauftrages "Rüstung, Nutzung, IT" folgende Ziele vereinbart worden:

1. Erarbeitung eines neuen Rüstungs- und Nutzungsprozesses mit klaren Verantwortlichkeiten, eindeutigen Entscheidungskompetenzen und reduzierten Schnittstellen.
2. Schaffen einer Aufbauorganisation des Rüstungsbereichs, in der die Beschaffung und die "Materialverantwortung für die Einsatzreife" in einem zentralen Ausrüstungs- und Nutzungsamt zusammengeführt werden.
3. Leisten eines Beitrages zum erforderlichen Personalabbau im zivilen und militärischen Ämterbereich.

## Die neue Ausrüstungs- und Nutzungsorganisation

Auf ministerieller Ebene wird eine neue Abteilung "Ausrüstung, Informationstechnik und Nutzung" (AIN) im Bundesministerium der Verteidigung (BMVg) aufgestellt. Deren Aufgabenspektrum leitet sich aus dem ministeriellen Kernauftrag ab, die nationalen und internationalen Rüstungsaktivitäten zu planen, zu steuern und zu kontrollieren. Aus der Fusion des Bundesamtes für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) und des Bundesamtes für Wehrtechnik und Beschaffung (BWB) sowie der Integration des in der Nutzung eingesetzten Personals aus den Streitkräften wird das künftige "Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr" (BAAINBw) als zentrales Ausrüstungs- und Nutzungsamt entstehen. Die damit einhergehende Bündelung der in der Bundeswehr vorhandenen Kompetenzen aus den Bereichen des Ausrüstungs- und des Nutzungsmanagements bis hin zur Verwertung schafft Synergien und reduziert den Abstimmungsaufwand. Die neue Struktur basiert auf dem Systemgedanken von streitkräftegemeinsamen Entwicklungen und querschnittlichen Technologiebetrachtungen. Sie vereinfacht Rückkopplungen aus der Nutzung von Wehrmaterial, insbesondere aus den Einsätzen. Diese Erkenntnisse können in Neubeschaffung aber auch in die Weiterentwicklung und Anpassung eingeführter Produkte effektiv eingebracht werden. Um insbesondere diesen Anspruch erfüllen zu können, obliegt dem BAAINBw die "Materialverantwortung für die Einsatzreife" für sämtliche Produkte. Die "Betriebs- und Versorgungsverantwortung für den Erhalt der Einsatzfähigkeit und Einsatzbereitschaft" verbleibt bei den militärischen Organisationsbereichen.

Unterstützt wird das neue Bundesamt durch sechs wehrtechnische und zwei wehrwissenschaftliche Dienststellen, dem Zentrum für Informationstechnik der Bundeswehr sowie dem Marinearsenal. Letzteres wird auch zukünftig Wartungs- und Instandsetzungsleistungen für die Deutsche Marine sicherstellen. Eine Verbindungsstelle in Reston/USA vertritt die wehrtechnischen und rüstungswirtschaftlichen Belange gegenüber Stellen des amerikanischen und kanadischen Amts- und Industriebereichs.

## Der neue Ausrüstungs- und Nutzungsprozess

Ausgangsbasis für die Konzeption des neuen Ausrüstungs- und Nutzungsprozesses ist die aktuelle Fassung des CPM, der sich grundsätzlich bewährt hat. Die Konzeption sieht künftig nur noch die drei Phasen vor, nämlich

- die Analysephase,
- die Realisierungsphase und
- die Nutzungsphase.

Die bisherigen Regelungen zur Deckung des Einsatzbedingten Sofortbedarfs entfallen. An ihre Stelle treten die Bestimmungen zur sogenannten “Sofortinitiative”. Diese sind integraler Bestandteil des novellierten CPM. An die Nutzungsphase wird sich die Verwertung des Materials anschließen.

Wesentliches Strukturmerkmal des neuen Prozesses ist die Einrichtung von Integrierten Projektteams (IPT). In diesen werden während des gesamten Prozesses verantwortliche Vertreter der Bereiche Rüstung, Streitkräfte und – soweit möglich – der Industrie phasenbezogen fachübergreifend zusammenarbeiten. Damit werden ein größtmöglicher Erkenntnisgewinn, eine ununterbrochene Bereitstellung von Know-how und eine möglichst durchgängige und schnittstellenarme Zusammenarbeit aller am Ausrüstungs- und Nutzungsprozess Beteiligten gefördert.

In der Analysephase wird der Rüstungsprozess mit der Billigung des Dokuments “Fähigkeitslücke und Funktionale Forderung” durch den Generalinspekteur der Bundeswehr initiiert. Der Abteilungsleiter Ausrüstung, Informationstechnik und Nutzung beauftragt daraufhin das BAAINBW mit der Erarbeitung von mehreren Lösungsvorschlägen in der sogenannten Planungskategorie “Rüstung”. Diese werden jeweils hinsichtlich Realisierung und Nutzung bzw. Life Cycle Costs mit einem Preisschild versehen. Dabei wird es unter Berücksichtigung marktverfügbarer Lösungen regelmäßig einen Lösungsvorschlag geben, der die Funktionale Forderung zu 100% abdeckt. Ergänzt wird dieser durch Lösungsvarianten mit abgestufter Abdeckung der Forderungen. Die Vorschläge werden insbesondere hinsichtlich des Zeitbedarfs für die Realisierung und hinsichtlich der Kosten variieren. Auf Basis der Lösungsalternativen trifft der Generalinspekteur der Bundeswehr eine Auswahlentscheidung (AWE). Die Auswahlentscheidung anhand substantiierter, bepreister und jeweils mit einem Realisierungszeitraum versehener Lösungsalternativen ist Teil eines Systems von “Checks and Balances”, das die Einbindung aller beteiligten Stellen vor der endgültigen Auswahl der materiellen Lösung sicherstellt.

Die Auswahlentscheidung des Generalinspekteurs der Bundeswehr und der endverhandelte Entwurf des Industrievertrages sind Ausgangspunkt für eine Zielvereinbarung zwischen dem Abteilungsleiter AIN und dem Präsidenten des BAAINBw zur Realisierung der ausgewählten Lösung. Sie hat einen weitgehend abschließenden Charakter und legt einvernehmlich Zeit- und Kostenrahmen sowie – soweit möglich – Vorgaben für das Life Cycle Cost Management (LCCM) am Beginn der Realisierungsphase fest.

Ziel der Realisierungsphase ist es, auf Basis der getroffenen Zielvereinbarung dem Nutzer geeignete Produkte und Dienstleistungen zeitgerecht und einsatzreif zur Verfügung zu stellen. Sie umfasst alle Maßnahmen, die zur Umsetzung der Zielvereinbarung im Rahmen von Projekt- und Risikomanagement sowie Projektcontrolling notwendig sind. Um eine möglichst störungsfreie, zügige und eigenverantwortliche Realisierung des Projekts zu ermöglichen, sind während der Realisierung grundsätzlich keine externen Eingriffe in das Projekt vorgesehen. Am Ende der Realisierungsphase wird – wie bisher – mit der “Genehmigung zur Nutzung” (GeNu) die Einsatzreife des Produktes sowie die Übernahmebereitschaft des Nutzers bescheinigt und das Produkt für die Nutzung freigegeben.

In der Nutzungsphase werden alle Maßnahmen, die dem Erhalt und dem Wiederherstellen der Einsatzreife der eingeführten Produkte und Dienstleistungen dienen, unterbrechungsfrei durch das BAAINBw weiter geplant und gesteuert. Erkenntnisse aus den Einsätzen können dabei auf kurzem Weg durch den Planungsprozess in den laufenden Rüstungsprozess und umgekehrt Erkenntnisse aus dem Rüstungsprozess in den Planungs- und Haushaltsprozess einfließen. Erstmals wird eine über alle Prozessphasen durchgehende Materialverantwortung für den Erhalt und das Wiederherstellen der Einsatzreife von der Realisierung bis zur Verwertung an einer einzigen verantwortlichen Stelle verankert.

Insgesamt stellt der neue Ausrüstungs- und Nutzungsprozess – gemeinsam mit der neuen Ausrüstungs- und Nutzungsorganisation – eine deutliche Optimierung des aktuellen Prozesses dar. Die neue Konzeption ist der Startpunkt für die bereits begonnene Überarbeitung des CPM und die Umsetzung der organisatorischen Maßnahmen, die im Rahmen der Neuausrichtung der Bundeswehr im Rüstungsbereich erfolgen müssen. Das gemeinsame Ziel ist die in vereinbartem Kosten- und Zeitrahmen vorgesehene Bereitstellung der Produkte und Dienstleistungen für die im Einsatz befindlichen Streitkräfte. Ich bin sicher, dass wir dafür mit der Umsetzung der Konzeption des neuen Ausrüstungs- und Nutzungsprozesses den richtigen Weg beschreiten.

# Die IT-Strategie des BMVg

Ministerialdirigent Dr. Dietmar Theis, Unterabteilungsleiter AIN IV (Informationstechnik, IT-Direktor), Bundesministerium der Verteidigung

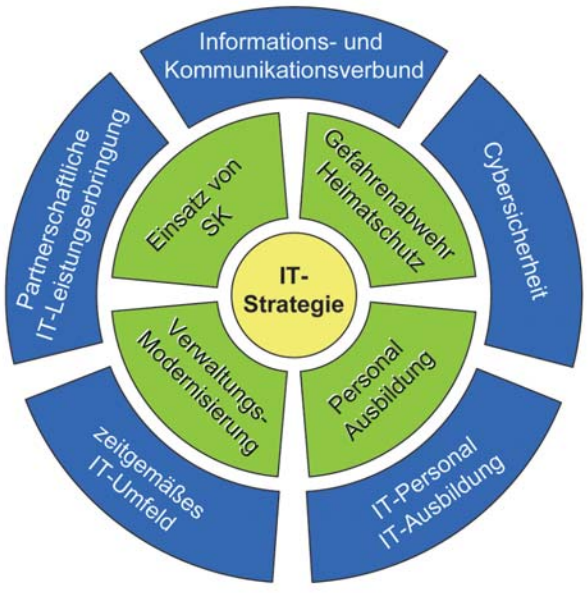
*Ministerialdirigent Dr. Dietmar Theis*

Im Rahmen der Neuausrichtung der Bundeswehr hat das Bundesministerium der Verteidigung (BMVg) auch seine IT-Strategie grundlegend überarbeitet. In dieser IT-Strategie werden für den gesamten Geschäftsbereich des BMVg künftig der Rahmen für die Ausgestaltung der IT in der Bundeswehr festgelegt und – ergänzend zur neu zu erarbeitenden Konzeption der Bundeswehr – Vorgaben für alle Folgedokumente gesetzt. Neben allen Aspekten der Konzeption, der Realisierung und des Betriebs eines durchgängigen Informations- und Kommunikationsverbundes umfasst die IT-Strategie auch Festlegungen zu den Bereichen Cybersicherheit, IT-Personal, IT-Ausbildung sowie die Gestaltung eines zeitgemäßen IT-Umfeldes für alle Bundeswehrangehörigen.

In vielen Bereichen greift das BMVg in seiner IT-Strategie auf bewährte Ansätze zurück. So bleibt es z.B. bei der konsequenten Orientierung an zivilen Standards, der Verwendung kommerziell verfügbarer Produkte und der strikten Begrenzung von Projekten auf einen überschaubaren Zeitbedarf von zwei bis drei Jahren, um Risiken zu begrenzen und aktuelle Innovationen berücksichtigen zu können. Neu sind die stärkere Berücksichtigung multinationaler Anforderungen und Lösungen, die klare Hinwendung zu serviceorientierten Architekturen (SOA) und das umfassende Verständnis des IT-Systems der Bundeswehr (IT-SysBw) als Gesamtsystem. SOA bedeutet insbesondere, dass die Bundeswehr bei ihrer IT zukünftig mehr auf flexibel konfigurierbare Module setzt, anstatt auf große, komplexe und monolithische Software-Lösungen. Dies ermöglicht der Bundeswehr, ihre IT flexibler an sich ändernde Anforderungen anzupassen und in multinational geprägte Einsatzumgebungen mit kurzem Vorlauf besser zu integrieren.

Um die Architektur des IT-SysBw zu steuern, sind im zukünftigen Bundesamt für Ausrüstung, Informationstechnik

## Handlungsfelder der IT-Strategie BMVg




- Verbesserung der Befähigung der Bundeswehr zur Vernetzten Operationsführung
- Rationalisierung des Betriebes mit Hilfe der IT
- Personalabbau ohne an Schlagkraft zu verlieren
- Ganzheitlicher Ansatz
- IT-System Bundeswehr ist EIN System

und Nutzung der Bundeswehr (BAAINBw) die Rollen des IT-Systemarchitekten und des Service Designers vorgesehen.
Der IT-Systemarchitekt hat die Aufgabe, die technische und die serviceorientierte Systemarchitektur des IT-SysBw zu erarbeiten und weiterzuentwickeln. Um Interoperabilität zwischen den nationalen und zu den Systemen unserer Partner zu gewährleisten, sind IT-Projekte nach seinen Vorgaben in das IT-SysBw einzubinden. Er muss die gesamte Komplexität der IT-Landschaft der Bundeswehr überblicken und in all ihren Interdependenzen im Griff haben.
Daneben hat der Service Designer die Aufgabe, alle neuen IT-Services in das Service-Design des IT-SysBw zu integrieren. Bisherige IT-Services, die auch zukünftig erforderlich sind, sind zu überführen oder, falls dies nicht möglich ist, zu ersetzen.
Auch in der überarbeiteten IT-Strategie des BMVg kommt der Rolle des IT-Direktors eine besondere Bedeutung zu. Im Einklang mit einer Festlegung der Bundesregierung von 2007 hat er die zentrale Rahmenkompetenz für die IT des gesamten Ressorts und vertritt deren Belange entscheidungsbefugt nach außen. Auch gewährleistet er weiterhin die IT-Sicherheit des Ressorts sowie die Übereinstimmung des IT-Einsatzes in der Bundeswehr mit den politischen, strategischen und operativen Zielen des Ressorts und den IT-Festlegungen der Bundesregierung.
Zur Umsetzung der IT-Strategie ist der bereits bei der Aufstellung des Bundesamtes für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) im Jahre 2001 verfolgte Ansatz, die Verantwortung für den gesamten Lebensweg eines Produktes von der Wiege bis zur Bahre zu bündeln, besonders geeignet. Er liegt daher auch der Gestaltung des neuen Ausüstungs- und Nutzungsprozesses der Bundeswehr sowie der künftigen Zusammenführung des IT-AmtBw mit dem Bundesamt für Wehrtechnik und Beschaffung (BWB) zugrunde. Durch die Verschmelzung der Aufgabenbereiche Rüstung und Informationstechnik wird zugleich die enge Verknüpfung von Sensorsystemen und Waffensystemen mit dem IT-System der Bundeswehr, wie sie für eine vernetzte Operationsführung erforderlich ist, organisatorisch besser unterstützt.

# Zukunftsmarkt Zivile Sicherheit – Industriepolitische Konzeption des Bundesministeriums für Wirtschaft und Technologie

MdB Hans-Joachim Otto, Parlamentarischer Staatssekretär beim Bundesminister für Wirtschaft und Technologie

*Parlamentarischer Staatssekretär Hans-Joachim Otto*

Deutschland gehört zu den weltweit sichersten Staaten. Offene Gesellschaften mit einer hohen internationalen Vernetzung und einer hoch entwickelten Infrastruktur sind heute jedoch in zunehmendem Maße Bedrohungen, wie z.B. durch Terrorismus und organisierte Kriminalität, aber auch durch Naturkatastrophen oder technische Großunfälle, ausgesetzt.

Sicherheit ist heute mehr denn je auch ein Wirtschaftsfaktor. So weisen die Märkte für Sicherheitstechnologien und -dienstleistungen nicht nur weltweit die stärksten Wachstumsraten auf. Standorte mit einer zuverlässigen Versorgung mit Energie und Telekommunikationsdiensten sowie mit einer sicheren Verkehrsinfrastruktur haben auch im internationalen Wettbewerb um Investitionen deutliche Vorteile.

Die hohe Bedeutung, die die Bundesregierung der zivilen Sicherheitswirtschaft beimisst, zeigt sich daran, dass das Bundesministerium für Wirtschaft und Technologie bereits im Jahr 2010 mit seiner industriepolitischen Konzeption zum "Zukunftsmarkt zivile Sicherheit" einen wichtigen Beitrag geleistet hat, um den Standort Deutschland und die internationale Wettbewerbsfähigkeit deutscher Unternehmen weiter zu stärken. Die wesentlichen Elemente dieser industriepolitischen Konzeption sollen im folgenden kurz skizziert werden.

## Auslandsaktivitäten unterstützen, Exporte stärken

Die für deutsche Unternehmen interessanten Auslandsmärkte im Bereich Sicherheit sind von einem starken Wettbewerb geprägt. Dabei nehmen öffentliche Entscheidungsträger auf den internationalen Märkten eine besondere Rolle ein – sei es als Kunden oder Betreiber kritischer Infrastrukturen, teilweise aber auch als Eigentümer von Firmen, mit denen deutsche Unternehmen im direkten Wettbewerb stehen. Die Präsenz und Vernetzung in den Auslandsmärkten sowie die politische Flankierung sind vor dem Hintergrund dieser speziellen Kundenstruktur und der Beschaffungskultur sowohl für Systemhäuser als auch für kleine und mittlere Unternehmen von großer Bedeutung.

Die neu geschaffene Exportinitiative "Sicherheitstechnologien und -dienstleistungen" des Bundesministeriums für Wirtschaft und Technologie hat daher zum Ziel, die Außenhandelsaktivitäten deutscher Unternehmen der Sicherheitsbranche zu fördern. Dabei wird das gesamte Instrumentarium der Außenwirtschaftsförderung der Bundesregierung unter Berücksichtigung der spezifischen Anforderungen der Sicherheitsbranche genutzt. Insbesondere mittelständische Firmen sollen dadurch die Möglichkeit bekommen, sich auf Drittmärkten zu etablieren. Schwerpunktländer/-regionen werden in diesem Jahr neben den bisherigen Zielmärkten Brasilien, Indien und die Arabische Halbinsel zusätzlich Russland, Vietnam und Mexiko sein.

Bundeswirtschaftsminister Rösler hat bei seinen großen Auslandsreisen oft Themen der zivilen Sicherheitswirtschaft im Gepäck. Ich selbst bin sowohl in 2011 und 2012 mit großen Industriedelegationen in Katar und den Vereinigten Arabischen Emiraten gewesen. Mein Staatssekretärskollege Burgbacher hat in Indien gemeinsam mit zahlreichen Großunternehmen, aber speziell auch vielen Mittelständlern mehrere Workshops durchgeführt. Die Erfolge dieser Reisen für die deutsche Wirtschaft können sich durchaus sehen lassen. Es sind strategische Partnerschaften entstanden, die wir in diesem Jahr noch weiter intensivieren wollen.

## Normung, Standardisierung und Zertifizierung

Normung und Standardisierung sorgen auch in der Sicher-

heitstechnik für Transparenz und Vergleichbarkeit, für hohe Qualität und Sicherheit bei Produkten und Dienstleistungen. Als Wettbewerbsfaktoren leisten Normen und Spezifikationen einen wesentlichen Beitrag zur Entwicklung eines Marktes und zur Positionierung der deutschen Sicherheitswirtschaft. Zur Stärkung der Wettbewerbsposition und der Innovationskraft wurde daher im Rahmen des industriepolitischen Konzeption eine "Koordinierungsstelle Sicherheitswirtschaft" beim DIN eingerichtet. Ihr Ziel ist u.a., den nationalen Meinungsbildungsprozess voranzubringen und die rechtzeitige und koordinierte Einbringung nationaler Interessen auf europäischer und internationaler Ebene im Bereich der Normung zu fördern. Mit der frühzeitigen Koordinierung deutscher Interessen werden auf europäischer Ebene wichtige Themenfelder begleitet: Der Fachbeirat für Sicherheitswirtschaft und die Normenausschüsse des DIN haben sich an der Ausarbeitung des "Security-Mandats" (M487) der Europäischen Kommission an die Europäischen Normungsorganisationen beteiligt. Zudem haben sie Beiträge zur angekündigten Mitteilung der Europäischen Kommission zur Industriepolitik für den Sicherheitsmarkt erarbeitet. Das DIN war auch maßgeblich an der Initiierung der Cyber Security Coordination Group der Europäischen Normungsorganisationen beteiligt.

## Forschung und Entwicklung

Sicherheitsforschung ist ein wesentliches Element der Hightech-Strategie der Bundesregierung. Mit dem gerade verabschiedeten 2. Rahmenprogramm "Forschung für die zivile Sicherheit (2012-2017)" bietet die Bundesregierung Forschungsinstituten, Unternehmen sowie privaten und öffentlichen Nachfragern die Möglichkeit, sich auf neue Technologiefelder auszurichten.

Sicherheitsforschung kann einen zentralen Beitrag zur Sicherheit der Wirtschaft leisten und zu neuen Produkten und Dienstleistungen führen, mit denen sich deutsche Unternehmen auf dem internationalen Markt positionieren können. Die Bundesregierung legt daher beim nationalen ebenso wie beim europäischen Sicherheitsforschungsprogramm großen Wert auf eine ausgeprägte Umsetzungsorientierung, d.h. Überführung der Forschungsergebnisse in konkrete Innovationen, eine intensive Einbindung der Endnutzer, eine hohe Beteiligung der mittelständischen Wirtschaft sowie eine enge Verknüpfung von Forschungs-, Innovations- und Industriepolitik.

## Aktivitäten in Brüssel

Im Rahmen der "Leitinitiative Europa 2020: Industriepolitik im Zeitalter der Globalisierung" beabsichtigt die Europäische Kommission noch im ersten Halbjahr diesen Jahres die Veröffentlichung einer industriepolitischen Mitteilung zur europäischen Sicherheitsindustrie. Damit trägt sie sowohl der großen Bedeutung des Themas Sicherheit angesichts der heutigen sicherheitspolitischen Herausforderungen wie auch dem Stellenwert der Sicherheitsindustrie als wichtiger und gleichzeitig wachstumsstarker Branche Rechnung. Das Bundesministerium für Wirtschaft und Technologie setzt sich – neben der europäischen Sicherheitsforschung und Normung/Standardisierung – auch auf diesem Gebiet für die Einbringung deutscher Interessen ein.

## Ausblick

Mit der industriepolitischen Konzeption zum "Zukunftsmarkt zivile Sicherheit" hat das Bundesministerium für Wirtschaft und Technologie im November 2010 neue Akzente gesetzt. Angesichts der Bedeutung der Sicherheitsbranche mit ihren enormen Wachstumspotenzialen beabsichtigen wir in den kommenden zwölf Monaten eine Fortschreibung und Vertiefung dieser industriepolitischen Konzeption. Wir werden dabei die großen Industrieverbände, wie den ZVEI, in unsere Arbeit einbinden.

# Status quo der Umsetzung der EU-Richtlinie für "Vergaben in den Bereichen Verteidigung und Sicherheit" in nationales Recht *)

Niels Lau, Leiter der Abteilung Wettbewerb, Öffentliche Aufträge und Verbraucher und Anja Mundt, Referentin in der Abteilung Wettbewerb, Öffentliche Aufträge und Verbraucher, Bundesverband der Deutschen Industrie e.V., Berlin

*Niels Lau*

*Anja Mundt*

Die EU-Richtlinie für Vergaben in den Bereichen Verteidigung und Sicherheit (RL 2009/81/EG vom 13.07.2009) gilt einerseits für militärische Vergaben wie Beschaffungen von Waffen, Munition und Verteidigungsmaterial sowie diesbezügliche Bau- und Dienstleistungen, andererseits prinzipiell auch für nicht-militärische Sicherheitsbeschaffungen, beispielsweise in den Bereichen Innere Sicherheit und Terrorismusabwehr. Sie wurde geschaffen, um die bisher häufig noch abgeschottenen Märkte für Sicherheits- und Verteidigungsbeschaffungen konsequent für eine europaweit zugängliche und transparente Auftragsvergabe zu öffnen.

Die deutsche Industrie hätte es begrüßt, wenn es bereits begleitend zur Erstellung der Richtlinie 2009/81/EG gelungen wäre, gleiche Rahmenbedingungen in Europa ("level playing field") herzustellen. Umso wichtiger ist es nun, die Intention der europäischen Richtliniengeber, einen echten europäischen Markt für Verteidigungs- und Sicherheitsgüter und gleiche Wettbewerbsbedingungen zu schaffen, zu unterstützen.

Die Richtlinie hätte bis 21.08.2011 in nationales Recht umgesetzt werden müssen. Eine vollständige Umsetzung ist jedoch bis heute nicht erfolgt.

Bislang ist nur das "Gesetz zur Änderung des Vergaberechts für die Bereiche Verteidigung und Sicherheit" vom 07.12.2011 (BGBl I 2011 Nr. 64 vom 13.12.2011) am 14.12.2011 in Kraft getreten. Mit diesem ersten Schritt werden das Gesetz gegen Wettbewerbsbeschränkungen (GWB), die Vergabeverordnung (VgV) und die Sektorenverordnung (SektVO) geändert. Die Änderungen im 4. Teil des GWB betreffen u.a. den Anwendungsbereich, die Ermächtigung für eine neu zu schaffende Verteidigungsvergabeverordnung (VSVgV) sowie den Rechtsschutz bei derartigen Aufträgen. Die Änderungen in der VgV und in der SektVO schließen im Wesentlichen die Anwendbarkeit dieser beiden Verordnungen für verteidigungs- und sicherheitsrelevante Aufträge i.S.d. § 99 Abs. 7 GWB aus.

In einem nächsten Schritt müssen daher die weiteren materiellen Vorschriften der Richtlinie 2009/81/EG in deutsches Recht umgesetzt werden. Dazu gehören der Anwendungsbereich, die Grundsätze, die Schwellenwerte, die Schätzung der Auftragswerte, die Versorgungs- und die Informationssicherheit sowie die Nachunternehmerregelung. Das Bundeswirtschaftsministerium (BMWi) hat dafür – unterstützt durch das Bundesverteidigungsministerium (BMVg) und das Bundesinnenministerium (BMI) – eine separate Verordnung vorlegt. Die bereits für Herbst 2011 angekündigte Vorlage wurde immer wieder verschoben. Die Vergabe von Liefer- und Dienstleistungsaufträgen, die unter die Richtlinie 2009/81/EG fallen, soll nach den Vorstellungen des BMWi in dieser neuen Rechtsverordnung und nicht wie bisher in der VOL/A geregelt werden. Diese neue Rechtsverordnung soll

weiterhin in einem ersten Abschnitt allgemeine und grundsätzliche Regelungen aus der Richtlinie enthalten, die für alle Vergaben, d. h. auch Bauaufträge, Gültigkeit erlangen.

Der BDI hatte sich bereits frühzeitig für eine fristgemäße Umsetzung unter Berücksichtigung der Argumente der wehr- und sicherheitstechnischen Industrie eingesetzt. Insbesondere hat sich die deutsche sicherheits- und wehrtechnische Industrie dafür ausgesprochen, die Vergabeverfahrensregelungen aus der Richtlinie entsprechend der bisherigen Terminologie in den Vergabe- und Vertragsordnungen (VOB, VOL, VOF) zu implementieren. Eine separate "Verteidigungsvergabeverordnung" würde demgegenüber zu einer Zersplitterung der Vergaberegelungen beitragen und damit die praktische Handhabbarkeit dieses wichtigen Segments der öffentlichen Auftragsvergabe für Auftraggeber und Auftragnehmer erschweren.

Mit einer Umsetzung auf dem Verordnungswege droht darüber hinaus ein schwerwiegendes praktisches Problem. Denn mit der Schaffung einer neuen "Verteidigungsvergabeverordnung" würde dem auch aus offizieller Sicht der Bundesregierung "bewährten" System des Vergaberechts der Bereich der sicherheits- und verteidigungsrelevanten Beschaffung entzogen. Die bisherige sinnvolle Befassung der zuständigen Gremien DVA und DVAL, die mit Vertretern der auftraggeber- und auftragnehmerseitigen Praxis besetzt sind, entfiele. Dem Sachverstand der Praxis würde vielmehr die vermeintliche Weisheit des Verordnungsgebers vorgezogen; diejenigen, "die es angeht", sind auf das einmalige Anhörungsrecht bei der Verordnungsgebung beschränkt. Dies geht zulasten der Vergabeverfahren.

Neben anderen betroffenen Wirtschaftsverbänden hat auch das Bundesbauministerium (BMVBS) die Position des BDI unterstützt. Im Baubereich konnte gemeinsam ein Teilerfolg erzielt werden. Während alle Grundsätze sowie die Verfahrensregelungen für Liefer- und Dienstleistungen in einer "Verteidigungsvergabeverordnung" geregelt werden sollen, soll für Bauleistungen sodann hinsichtlich der Verfahrensregelungen auf einen neuen 3. Abschnitt der VOB/A "Vergabebestimmungen im Anwendungsbereich der Richtlinie 2009/81/EG – VOB/A-VS" verwiesen werden. Der neue 3. Abschnitt der VOB/A ist zwar bereits als Sonderbeilage Nr. 182a zum Bundesanzeiger Nr. 182 vom 02.12.2011 veröffentlicht worden. Er ist jedoch erst anwendbar, wenn die künftige Verteidigungsvergabeverordnung (VSVgV) darauf Bezug nimmt. Diese lässt jedoch auf sich warten.

Da das BMWi für Liefer- und Dienstleistungen keinen eigenen 3. Abschnitt in der VOL/A vorsehen, sondern die Verfahrenregelungen der Richtlinie in der Verteidigungsvergabeverordnung regeln will, müsste letztere zumindest die entsprechenden Regelungen aus dem 2. Abschnitt der VOL/A enthalten sowie auf die Anwendbarkeit der Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) verweisen. Die Folge wäre eine unschöne Doppelung der Vorschriften, die aber bei einer Verordnungslösung zwingend erforderlich ist. Dieser unnötige Bürokratieaufbau hätte vermieden werden können, wenn der Vorschlag des BDI zur Umsetzung der Verfahrenregelungen innerhalb der VOL/A erfolgt wäre.

Ungeachtet der derzeitigen Situation werden erste Vergaben nach der neuen Richtlinie bereits vorbereitet. Hilfe bietet dabei derzeit nur ein Blick in die Richtlinie selbst, die mangels fristgemäßer Umsetzung in Deutschland nun unmittelbar gilt. BMWi und BMVBS hatten mit Ablauf der Umsetzungsfrist – jeweils für ihre Bereiche – sog. Interimsregelungen erlassen, um die Anwendung der Richtlinie bis zur vollständigen Umsetzung zu erleichtern. Diese Regelungen wurden nunmehr verlängert.

Auch die EU-Kommission ist mittlerweile ungeduldig. Sie hat am 26.01.2012 eine Aufforderung an Deutschland in Form einer mit Gründen versehenen Stellungnahme geschickt und damit ein Vertragsverletzungsverfahren eingeleitet. Antwortet Deutschland nicht binnen zweier Monate zufriedenstellend, kann die EU-Kommission den Gerichtshof anrufen und die Verhängung von Strafgeldern beantragen. Dies hätte, wie das Beispiel DVA zeigt, vermieden werden können, wenn die bislang zuständigen Gremien DVA und DVAL in Gänze mit der Umsetzung der Verfahrensregelungen befasst worden wären.

*) Stand 27.01.2012

# Bevölkerungsschutz – Aktuelle Herausforderungen

Klaus-Dieter Fritsche, Staatssekretär im Bundesministerium des Innern

*Staatssekretär Klaus-Dieter Fritsche*

Im letzten Jahrzehnt haben Bund und Länder in Deutschland ein integriertes Notfallvorsorgesystem etabliert. Bund, Länder und Kommunen arbeiten im Verbund mit den Feuerwehren und den großen Hilfsorganisationen eng zusammen. Je nach Ereignisfall kann das System schnell und flexibel von unten bis oben aufwachsen.

Die Erstverantwortung liegt dezentral bei den Kommunen und Behörden vor Ort. Sie können im Regelfall am besten unmittelbar, schnell und effektiv reagieren. Sie kennen die Örtlichkeiten, können die Lage und die erforderlichen Maßnahmen am besten einschätzen und die nötigen Kräfte mobilisieren. Bei Bedarf stehen die Länder zur Unterstützung im Krisenmanagement und der Koordinierung bereit. Auf ihre Anforderung hin kann bei großflächigen Schadenslagen der Bund weitere Koordinierungsaufgaben übernehmen. Die notwendigen Strukturen hierfür sind eingerichtet. Diese Option ist eine der wesentlichen Neuerungen aus dem Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes (ZSKG) von 2009.

Dieses Gesetz war letzter Meilenstein und Abschluss einer Entwicklung, die nach den Terroranschlägen 2001 und den Sommerhochwassern 2002 begann. Als Antwort auf diese Ereignisse vereinbarten Bund und Länder eine “Neue Strategie für einen modernen Bevölkerungsschutz”. Kernziele dieser politischen Rahmenkonzeption waren eine bessere Verzahnung, Abstimmung und partnerschaftliche Zusammenarbeit aller Akteure über föderale Grenzen hinweg und eine stärkere Verantwortung des Bundes zur Unterstützung der Länder bei der Bewältigung von Großschadenslagen.

In der Folge wurden das Gemeinsame Melde- und Lagezentrum von Bund und Ländern, die Datenbank deNIS für das Informations- und Ressourcenmanagement und das satellitengestützte Warnsystem des Bundes aufgebaut. Die Akademie für Krisenmanagement wurde neu ausgerichtet. Organisatorischen Niederschlag fand die “Neue Strategie” im 2004 errichteten Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. 2009 wurde mit Erlass des ZSKG der rechtliche Rahmen fixiert für eine Unterstützung der Länder durch den Bund bei der Vorbereitung auf und der Bewältigung von Großschadenslagen.

Damit sind die Forderungen aus der “Neue Strategie” von 2002 im Wesentlichen umgesetzt. Die großen Entscheidungen im Bevölkerungsschutz sind gefallen. Mit unserem integrierten Notfallvorsorgesystem sind wir für die Bewältigung von Großschadenslagen heute gut aufgestellt. Aber auch Gutes kann noch besser werden.

Zu den verbleibenden gemeinsamen Aufgaben von Bund und Ländern gehört der Aufbau eines zeitgemäßen Warn- und Alarmierungssystems mit Weckeffekt. Das aktuelle (Bundes-)System SatWaS ermöglicht den Lagezentren von Bund und Ländern binnen Sekunden Gefahrendurchsagen durch 140 angeschlossene Medienbetreiber. Dies erfolgt überwiegend über Radio und Fernsehen, vereinzelt auch übers Internet und Paging. Dieses System wird als gemeinsames Projekt von Bund und Ländern zu einem modularen Warnsystem ausgebaut.

Mit dem künftigen System soll ein im Bevölkerungsschutz Verantwortlicher (Bund, Länder, Katastrophenschutzbehörden, Leitstellen) unmittelbar und ohne Medienbruch alle in seinem Verantwortungsbereich vorhandenen Alarmierungs- und Warnsysteme auslösen können. Diverse zusätzliche Warnmittel können angeschlossen werden – darunter Sirenen, Rauchwarnmelder oder Mobiltelefone. Neu und wichtig ist der dadurch ermöglichte “Weckeffekt”. Neu ist auch die stärkere regionale Differenzierung: Flankierend zur Einrüstung von Leitstellen wird es auch möglich, Warnungen regional begrenzt herauszugeben.

Anders als noch vor zehn Jahren – damals waren Radio und Fernsehen die zentralen Medien, um den Großteil der Bevölkerung zu erreichen – gibt es heute kein einheitliches Medium mehr, mit dem wir alle erreichen können. Nicht jeder hört mehr Radio, aber auch nicht jeder besitzt ein Mo-

biltelefon. Das modulare Warnsystem ist der richtige Weg, um die unterschiedlichsten Bevölkerungsgruppen mit ihren jeweils eigenen Medien zu erreichen.

Einen vergleichbaren Weg gilt es, für die Risikokommunikation mit der Bevölkerung zu finden. Trotz intensiver Berichterstattung der Medien über Katastrophen in aller Welt ist Risikobewusstsein in Deutschland wenig ausgeprägt. Wir leben – Gott sei Dank – in einem katastrophenarmen Land. Dennoch oder gerade deshalb ist es wichtig, die relevanten Risiken zu kennen. Sonst wird man im Ereignisfall vom Geschehen überrascht und überfordert.

“Der Zufall begünstigt den, der vorbereitet ist”, sagte einmal Louis Pasteur. Das beschreibt kurz und prägnant die Aufgabe des Bevölkerungsschutzes: Vorsorge zu treffen für Ereignisse, von denen wir nicht wissen, ob und wann sie passieren und wie sie konkret aussehen.

Diese Aufgabe erleichtern soll eine bundesweite Risikoanalyse. Hiermit erfüllen wir einen weiteren gesetzlichen Auftrag aus dem ZSKG. Verschiedene Risiken werden mit diesem Instrument strukturiert nach Eintrittswahrscheinlichkeiten und Schadensausmaß analysiert und vergleichbar gemacht. Methoden und Strukturen haben wir zunächst entwickelt. Jetzt wird das Projekt in der Sache vorangetrieben und soll in diesem Jahr erste Ergebnisse zu ausgewählten Szenarien wie z.B. Hochwasser erbringen.

Ein weiterer zentraler gesetzlicher Auftrag aus dem ZSKG ist die Förderung des Ehrenamtes als Grundlage des Bevölkerungsschutzes. Unser System verdankt seine Stärke und Schlagkraft den vielen freiwilligen Helfern in Feuerwehren, Hilfsorganisationen und Regieeinheiten. Sie garantieren durch ihre Präsenz in der Fläche für schnelle und effektive Hilfe vor Ort. Diese Struktur zu erhalten, ist angesichts einer Vielzahl geänderter Rahmenbedingungen von der Wehrstrukturreform über den demographischen Wandel bis hin zur Fülle konkurrierender Freizeitangebote heute die zentrale Herausforderung für unseren nationalen Bevölkerungsschutz.

Hierzu müssen laufende Maßnahmen konsequent umgesetzt und weiterentwickelt werden, so etwa im Bereich des THW das Mentorinnenprojekt zur Förderung von Frauen, das Projekt “Interkulturelle Öffnung” zur Kontaktaufnahme mit Migranten, die Zusammenarbeit mit Schulen, die Zertifizierung von Ausbildungsabschlüssen und die in 2011 gestartete und bis 2014 laufende Kampagne “Raus aus dem Alltag – Rein ins THW”.

Wichtig ist auch die Wertschätzung und Anerkennung bürgerlichen Engagements. Hierzu hat das Bundesministerium des Innern vor drei Jahren den Wettbewerb um den Förderpreis “Helfende Hand” ins Leben gerufen. Mit der Preisverleihung werden herausragende Projekte für das Ehrenamt im Bevölkerungsschutz öffentlich gewürdigt. Gleichzeitig bilden die auf der Homepage der Helfenden Hand vorgestellten Projekte einen Ideenpool für andere, die nach Lösungen und bewährten Praxisbeispielen für ihre Arbeit vor Ort suchen.

Um neue Projekte und strategische Maßnahmen zu entwickeln, hat das Bundesministerium des Innern in Abstimmung mit den Ländern und den Hilfsorganisationen Ende letzten Jahres ein umfassendes Forschungsprojekt zur nachhaltigen Sicherstellung der ehrenamtlichen Strukturen im Bevölkerungsschutz initiiert. Einen Schwerpunkt dieses Vorhabens bildet die Auswertung von Praxisbeispielen im Zusammenhang mit Motivation und Lebenssituation. Daraus soll ein Baukasten mit bewährten Vorgehensweisen (best practice) entstehen. Zugleich wollen wir einen Überblick über noch unbearbeitete Felder gewinnen. Aus diesen Ergebnissen werden anschließend neue Projekte und strategische Maßnahmen sowie Ansätze zur Optimierung des Systems durch Selbstschutz, Technik und neue Organisationsstrukturen entwickelt werden. Ende 2013 soll das Gesamtprojekt abgeschlossen sein.

Wichtig ist, dass die ehrenamtlichen Strukturen der heutigen Lebenswirklichkeit gerecht werden. Wenn es dafür neuer Formate wie befristeter oder projektbezogener Engagements bedarf, einer stärkeren Unterstützung durch hauptamtliche Kräfte oder einer organisierten Einbindung spontaner Helfer in akuten Großschadenslagen, müssen wir hierfür Wege schaffen. Ziel muss es sein, unseren Bevölkerungsschutz langfristig zu sichern und zukunftsfähig zu machen – und zwar auf Grundlage unserer bewährten ehrenamtlichen Strukturen.

# Sicherheitsforschung in der Europäischen Union

Dr. Christian Ehler, Mitglied des Europäischen Parlaments (CDU/EVP)

*Dr. Christian Ehler*

Elektronische Datenverarbeitung ist die technologische Voraussetzung, durch die sich die Wirtschaft in Europa und der Welt in den letzten 50 Jahren radikal verändert hat. In ihrer jungen Geschichte ist die EDV aufgrund der rasanten Entwicklungen jetzt in eine neue bedeutsame Phase getreten: Mobile Geräte wie Smartphones und Tabletcomputer sind neben Computern mit Zugang zur Cloud für Millionen von Bürgern und Unternehmen als die neuen Universalrechner hervorgegangen. Angaben des Branchenverbands BITKOM zufolge werden 2012 in Deutschland erstmals mehr internetfähige Smartphones als einfache Handys verkauft. Erst kürzlich hat das Europäische Parlament einer Richtlinie zugestimmt, die die Mitgliedsstaaten auffordert, ab 2013 mehr Frequenzen für drahtlose Breitbandnetze zur Verfügung zu stellen, um mit der wachsenden Nachfrage nach drahtloser Datenübertragung Schritt zu halten und Europa im globalen Wettbewerb wieder eine Spitzenposition bei der mobilen Kommunikation zu ermöglichen.

Innerhalb des 7. EU-Forschungsrahmenprogramms bildet die Informations- und Kommunikationstechnologie eines von zehn Gebieten des Spezifischen Programms “Zusammenarbeit”, in dem “Mobile Computing” im elektronischen Sektor und darüber hinaus adressiert wird. Dabei baut es auf Europas Stärken in der Entwicklung entsprechender Systeme und erweitert sie in Richtung der nächsten IT-Architekturrevolution.

*Europäisches Parlament* *Quelle: Europäisches Parlament*

Die vielleicht komplexeste Herausforderung mobiler Informationsübertragung ist das Thema Sicherheit. Deshalb zieht sich das Thema ICT Security wie ein roter Faden durch alle Missionen des Sicherheitsforschungsprogramms der EU. Seit 2007 steht dafür erstmals ein Budget von rund 1,4 Milliarden Euro zur Verfügung. Ziel ist es, ein sicheres und widerstandfähiges Europa zugunsten der Bürger und der kritischen Infrastrukturen zu schaffen sowie gleichzeitig KMU und die internationale Wettbewerbsfähigkeit zu stärken. Mit den jährlichen Ausschreibungen unterstützt die EU die direkte Zusammenarbeit zwischen Anbietern und öffentlichen wie privaten Endnutzern von Sicherheitslösungen.

Mit dem Folgeprogramm Horizon 2020 soll Sicherheitsforschung ab 2014 in einem breiteren Kontext unter der gesellschaftlichen Herausforderung “integrative, innovative und sichere Gesellschaften” angesiedelt sein. Die Europäische Kommission schlägt für diesen Titel ein Gesamtbudget von 4,3 Milliarden Euro vor. Als Generalberichterstatter der größten Fraktion im Parlament werde ich mich dafür einsetzen, dass Sicherheitsforschung auch in Zukunft das Gewicht erhält, das es verdient: ein eigenständiger Bereich mit eigenem Budget.

Die Sicherheitsforschung in Horizon 2020 wird auch neue inhaltliche Schwerpunkte setzen: Neben Cyber-Kriminalität und -Terrorismus soll die externe Dimension der gemeinsamen Sicherheits- und Verteidigungspolitik der EU eine wesentliche Rolle spielen. Dem Aufbau der zivil-militärischen Fähigkeiten Europas sollte eine eigene “Mission” gewidmet werden. Hier wird das Thema Interoperabilität von Kommunikation aus meiner Sicht eine herausragende Rolle spielen und erstmals auch durch das Instrument der vorkommerziellen Auftragsvergabe genutzt werden. Die erste Ausschreibung im neuen Programm soll im Sommer 2014 veröffentlicht werden. Zuvor erwarten wir im Juli 2012 den letzten FP7 Security Call mit einem Budget von rund 300 Millionen Euro. Auch hier wird IKT im Dienste der Integration und Interoperabilität von Sicherheitssystemen adressiert.

Die Aktivitäten der EU in Forschung, Entwicklung und Innovation werden dabei von der industriellen Agenda der europäischen Schlüsselakteure auf der Systemanbieter- wie auch der Dienstleistungs- und Anwenderseite inspiriert. Dies verdeutlicht auch die für den Frühsommer angekündigte industriepolitische Mitteilung für eine "Security Industrial Policy". Die Kommission wird erste Überlegungen aufzeigen, wie die derzeitige Fragmentierung des Sicherheitsmarktes überwunden und ein einheitlicher europäischer Sicherheitsmarkt geschaffen werden kann. Hauptaspekte sind Zertifizierung und Standardisierung sowie die Nutzung von Synergien zwischen zivilen und militärischen Technologien. Des Weiteren soll die Brücke von der Forschung zum Markt optimiert werden, indem die EU ihre Förderprogramme in eine Linie bringt – siehe Horizon 2020 Vorschläge – und vorkommerzielle Beschaffungsinstrumente einführt.

Arbeitsplätze und Sicherheit sind die beiden zentralen politischen Themen der europäischen Bürger. Hebel für beide

*EU-Flagge* *Quelle: Europäisches Parlament*

Themen sind in erster Linie Investitionen in Forschung und Innovation. Als einer der Berichterstatter des europäischen Parlaments zu Horizon 2020 werde ich mich für ein eigenständiges Sicherheitsforschungsprogramm und einen substanziellen Aufwuchs der Mittel einsetzen.

# Forschungs- und Technologiebedarf der Polizei

Klaus Neidhardt, Präsident der Deutschen Hochschule der Polizei, Münster-Hiltrup

*Klaus Neidhardt*

Die ständige Konferenz der Innenminister und -senatoren (Innenministerkonferenz – IMK) hat in ihrem "Programm Innere Sicherheit – Fortschreibung 2008/2009" die Leitlinien für die polizeiliche Sicherheitsforschung u.a. mit folgenden Grundsätzen festgelegt:

- Veränderte Rahmenbedingungen erfordern ein hohes Maß an Innovation und eine gezielte Erschließung von Forschungs- und Entwicklungspotenzial.
- Die Spezialität und Komplexität der Anforderungen verlangen die Kooperation mit allen Trägern der Forschung und der Wirtschaft.
- Die Deutsche Hochschule der Polizei (DHPol) und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sind Koordinierungsstellen für Fragen der Sicherheitsforschung. Außerdem vertreten sie die Interessen der Sicherheitsbehörden im jeweiligen Aufgabenbereich. Künftig sind sie als zentrale Anlaufstellen ("one-step-agency") zu entwickeln.

Für die DHPol hat Sicherheitsforschung dabei auch wichtige prognostische Aufgaben:

- Vor welche Risiken/Bedrohungen werden wir uns gestellt sehen?
- Welche Mittel bzw. Technologien können Straftätern künftig zur Verfügung stehen?
- Welche neuen Konzepte, Instrumentarien und Technologien können von der Polizei zur Prävention, Gefahrenabwehr und Strafverfolgung eingesetzt werden?

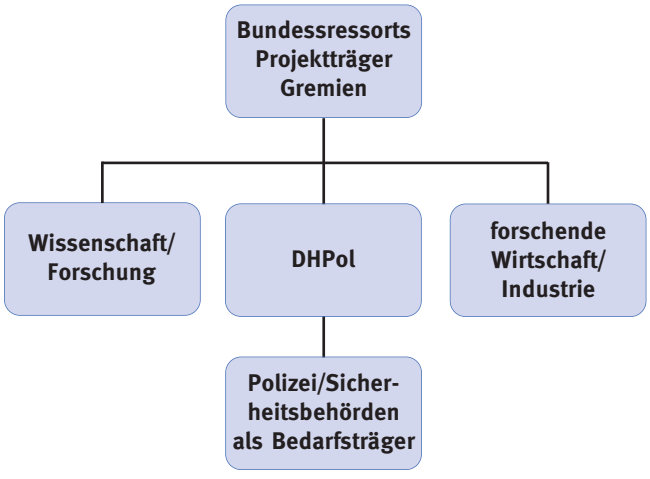
Ziele polizeilicher Sicherheitsforschung sind vor allem:

- Ursachen von Kriminalität, Gewalt und Extremismus erforschen,
- Bedrohungspotenziale untersuchen, Sicherheitslücken eruieren,
- Wirkung von gesellschaftlicher und polizeilicher Prävention ermitteln,
- Strategien zur Gewährleistung von Sicherheit fortentwickeln,
- das polizeiliche Einsatzmanagement optimieren,
- Koordination und Kooperation sicherheitsrelevanter Akteure verbessern,
- Technologietransfer zur Polizei sicherstellen,
- Spezielle Technologien für polizeiliche Zwecke (weiter-)entwickeln.

Grundprinzip dabei ist stets, die Balance von Freiheit und Sicherheit zu erhalten und zu gewährleisten, dass die Bürger ihre grundgesetzlich verbürgten Rechte in Anspruch nehmen können.

Neuen Risiken, Bedrohungen, Tatphänomenen und Tattechnologien muss mit neuen gesellschaftlichen, politischen, rechtlichen und technischen Konzepten und Instrumenten begegnet werden. Hierfür Möglichkeiten und Grenzen aufzuzeigen, sollte auch eine wichtige Aufgabenstellung der Sicherheitsforschung sein.

Die DHPol versteht ihre Rolle – als zentrale Anlaufstelle – im Sinne der nachstehenden Graphik von Wirtschaft und Wissenschaft zur Schaffung von Kontakten zur Polizei und umgekehrt.



Dazu wurden in einem ersten Schritt Kontaktgespräche mit der Fraunhofergesellschaft, mit dem BDI und mit hochrangigen Vertretern der Polizei organisiert.

Eine wichtige Funktion wird das Forschungssymposium der DHPol am 19. und 20. Juni 2012 in Münster erfüllen, in dem wichtige Themenfelder von Forschung und Entwicklung aus der Sicht der Polizeien des Bundes und der Länder im Mittelpunkt stehen sollen:

- Gesellschaftliche Dimensionen / Sicherheit und Kommunen,
- Kriminalitätsbekämpfung / Prävention,
- IuK- / Cyber-Kriminalität / IT-Forensik,
- Führungsmittel / Aufklärung / Sensorik / Simulation / Analyse
- Einsatzmittel / Wirkung und Schutz.

Die Etablierung forschungsorientierter sektoraler Themenplattformen zur Vernetzung von Polizei, Wissenschaft und Industrie/gewerblicher Wirtschaft wird sicherlich dazu beitragen, dass gemeinsame, erfolgversprechende Verbundforschungsanträge gestellt werden können.

*Deutsche Hochschule der Polizei, Münster-Hiltrup*

*Quelle: DHPol*

# Fachkreis “Einsatzorientierung ITK / vernetzte Operationsführung”

Oberst a.D. Friedrich W. Benz, Leitmarkt Defence im ZVEI–Fachverband Sicherheit

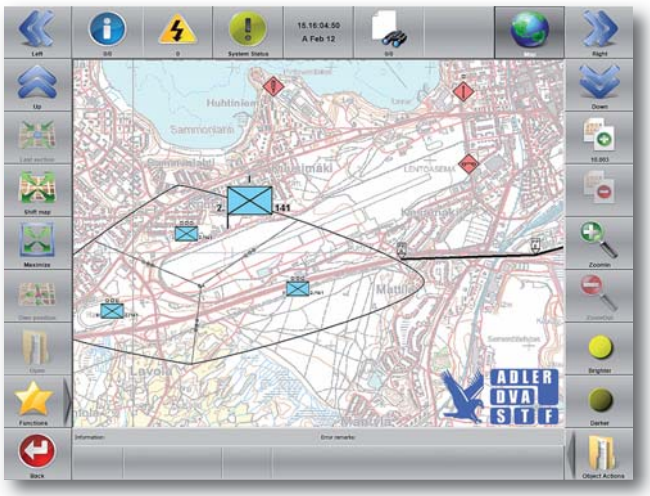
*Oberst a.D. Friedrich W. Benz*

Die Neuausrichtung der Bundeswehr ist geprägt durch die Orientierung an den aktuellen und möglichen künftigen streitkräftegemeinsamen und multinationalen Einsätzen in einem breiten Einsatzspektrum – von friedenserhaltenden Maßnahmen bis zu einem kriegerischen Konflikt. “Vom Einsatz her denken” ist die zwangsläufig daraus resultierende Maxime für die Beschaffung der ITK-Ausrüstung der Bundeswehr zur Ermöglichung einer vernetzten Operationsführung innerhalb der Bundeswehr, im Bündnis oder in einem sehr breiten Spektrum von möglichen Koalitionen unter VN-Mandat.

## Fachkreis “Einsatzorientierung ITK/NetOpFü”

Um den Aspekt der Einsatzorientierung künftig stärker in der Gremienarbeit zu berücksichtigen, hat der Vorstand des ZVEI-Fachverbandes Sicherheit im Dezember 2011 entschieden, bisherige Gremien umzustrukturieren und einen Fachkreis “Einsatzorientierung ITK-Systeme/Vernetzte Operationsführung” einzurichten. Dieser geht hervor aus der ehemaligen Fachabteilung ITK-Systeme, in der bisher zugleich auch Belange der FüInfoSys/FüWES und Gefechtsstände mit bearbeitet wurden. Darin sollen künftig, unter Einbeziehung bestehender Gremien des Leitmarktes Defence, die einzelnen Teilbereiche der Führungsunterstützung/ITK (InfoÜbermittlung; InfoVerarbeitung; Gefechtsstände; IT-Sicherheit; IT-Architekturen) in einem übergreifenden, gesamtheitlichen Ansatz, insbesondere unter dem Fokus der konkreten Einsatzerfordernisse betrachtet und pragmatische einsatzorientierte Lösungen verfolgt werden.

Der Fachkreis “Einsatzorientierung ITK/vernetzte Operationsführung” versteht sich als Expertengremium des Leitmarktes Defence hinsichtlich des Einsatzes moderner Technologien und Systemlösungen der ITK/Führungsunterstützung zur Umsetzung der Vernetzten Operationsführung. Er fungiert dabei für den Gesamtbereich der Führungs- und Einsatzunterstützung als zentrales Bindeglied zwischen den Know-how-Trägern/Kompetenzzentren der wehrtechnischen ITK-Industrie und der Bundeswehr auf Bedarfsträger- und Bedarfsdeckerseite. Mit diesem neuen Gremium als Informationsplattform sollen in aktiver Wechselwirkung zwischen Streitkräften und Industrie erkannte Defizite, festgestellte Fähigkeitslücken und der operationelle Bedarf für die Einsätze verdeutlicht, neue Verfahren und Technologien für die Vernetzte Operationsführung diskutiert und Einsatzmöglichkeiten und Chancen innovativer und pragmatischer Systemlösungen zur Abdeckung des einsatzorientierten Bedarfs aufgezeigt werden, um schnellere Beschaffungsabläufe im Rahmen des neuen Ausrüstungs- und Nutzungskonzeptes der Bundeswehr zu ermöglichen und um neue Lösungen möglichst schnell in die Anwendung überführen zu können. Der Fachkreis Einsatzorientierung ITK/NetOpFü im Leitmarkt Defence im ZVEI-Fachverband Sicherheit steuert zudem die Arbeit der unmittelbar nachgeordneten Arbeitskreise IT-Architekturen, AK IT-Sicherheit, AK Kommunikation und des AK FüInfoSys/FüWES/Gefechtsstände, indem er diese mit Detailuntersuchungen im jeweiligen Themenbereich, der Erstellen von Positionspapieren, etc., beauftragt.




*Screenshot des FüWES der Artillerie ADLER* Quelle: ESG GmbH

Die nachgeordneten Arbeitskreise des Fachkreises “Einsatzorientierung ITK/NetOpFü”, in denen ähnlich wie im Fachkreis “Product Support & Logistik” spezifische Themen oder Untersuchungen bearbeitet werden, sind

- der Arbeitskreis “IT-Architekturen”
- der Arbeitskreis “IT-Sicherheit”
- der neue Arbeitskreis “FüInfoSys/FüWES/Gefechtsstände” und
- der Arbeitskreis Kommunikation.

## Arbeitskreis “IT-Architekturen”

Die Architekturmethode, bei der Analyse, Planung und Realisierung einer hoch komplexen Kommunikations- und Führungsinformationsinfrastruktur ermöglicht, bzw. erleichtert wird, wurde in den letzten Jahren auch in der Bundeswehr in einzelnen Projekten eingesetzt. Da einheitliche Regelungen und Vorgaben zur Architekturentwicklung sowie auftraggeberseitige Konventionsrichtlinien fehlten und die dabei entwickelten Architekturen mit verschiedenen Modellierungswerkzeugen unter Verwendung unterschiedlicher Rahmenwerke und durch unterschiedliche Auftragnehmer realisiert wurden, gab es in der Folge eine Vielzahl von Architekturen, die nicht zusammenpassten, sondern nur die Lösung für das jeweilige Projekt darstellten. Aufgrund der unterschiedlichen Detaillierungsgrade und der unterschiedlichen Tools waren auch eine Vergleichbarkeit und Wiederverwendbarkeit – wenn überhaupt – nur durch immensen zusätzlichen Aufwand möglich.

Um in einen industrieseitig abgestimmten Dialog zum Thema Architekturen mit der Amtsseite einzutreten, wurde vom ZVEI – zusammen mit BITKOM – der Arbeitskreis “IT-Architekturen” gebildet, der sich als das industrieseitige Spiegelgremium zur ämterseitigen Arbeitsgruppe “Architekturen” versteht, mit dem ein intensiver Informations- und Know-how-Austausch zwischen der Industrie und den Streitkräften sowie den beteiligten Behörden der NATO und der EU ermöglicht werden soll.

Die Aktivitäten im gemeinsamen Arbeitskreis haben das Ziel, eine einheitliche Wissensbasis für die IT-Architekturentwicklung zu schaffen. Hierzu sollen zum einen die diesbezüglichen Vorgaben und Randbedingungen der Bundeswehr, der NATO und – soweit vorhanden – auch der EU reflektiert und zum anderen die industrieseitigen Notwendigkeiten und Randbedingungen der wehrtechnischen Industrie aufgezeigt werden. Dazu wurden Vorschläge zur gemeinsamen Erarbeitung von IT-Architekturen erarbeitet und in Form eines in der Industrie abgestimmten und im Dialog mit der Amtseite entwickelten “Leitfaden IT-Architekturen” festgehalten, der im Februar 2010 an die Amtsseite übergeben wurde. Der Leitfaden soll als gemeinsame Grundlage für die Ausschreibung und Entwicklung von IT-Architekturen genutzt werden und zu einem gemeinsamen Verständnis beitragen. Um der stetigen Entwicklung und Erfahrungen aus neuen Projekten Rechnung zu tragen, soll der Leitfaden als lebendes Dokument verstanden und iteraktiv fortgeschrieben werden.

*Führungs- und Einsatzsysteme* Quelle: ESG GmbH

## Arbeitskreis “IT-Sicherheit”

Als Konsequenz aus der hohen Bedrohung der IT-Infrastruktur ist ein umfassendes Sicherheits- und Risikomanagement der Bundeswehr erforderlich.

Dies bedeutet auch, dass sich die Bundeswehr im Bereich der I&K-Systeme nicht nur mit der Beschaffung von Sicherheitskomponenten zufrieden gibt, sondern sich stärker den Methoden und Standards im Bereich des Sicherheits- und Risikomanagements widmet, um den Prozessen der NetOpFü, dem Betrieb und der Fortentwicklung des IT-SysBw und der IT-Anteile in den Waffensystemen gerecht zu werden.

Der Arbeitskreis “IT-Sicherheit” versteht sich als kompetentes und beratendes Expertengremium des Leitmarktes Defence im ZVEI hinsichtlich des Einsatzes moderner Technologien und Systemlösungen im Bereich der IT-Sicherheit, fungiert dabei als ein zentrales Bindeglied zwischen den Know-how-Trägern und Kompetenzzentren der wehrtechnischen IT-Industrie und der Bundeswehr, der NATO/EU sowie ausgewählten Behörden des Bundes. Wesentliche Zielsetzung ist es, in aktiver Wechselwirkung zwischen Industrie und Streitkräften, Einsatzmöglichkeiten und Chancen innovativer und pragmatischer Systemlösungen im Bereich IT-Sicherheit aufzuzeigen und in die Anwendung zu überführen.

*PUMA mit Multifunktionaler Schutzausstattung (MUSS)*

*Quelle: CASSIDIAN*

## Arbeitskreis "FüInfoSys/FüWES/Gefechtsstände"

Eine wesentliche Rolle bei der Realisierung der Vernetzten Operationsführung spielen interoperable und nutzerfreundliche FüInfoSys und FüWES sowie leistungsfähige und flexible Gefechtsstände unterschiedlicher Ebenen als Knoten im Netz.
Der Arbeitskreis FüInfoSys/FüWES/Gefechtsstände verfolgt und befasst sich umfassend mit den Belangen der Führungsinformationssysteme und FüWES, Interoperabilitätsprogrammen sowie den Gefechtsständen für Bundeswehr und auch für BOS. Der Arbeitskreis sieht sich dabei als zentrales Bindeglied zwischen den Know-how-Trägern und Kompetenzzentren der wehrtechnischen Industrie und der Bundeswehr sowie den Behörden des Bundes und der Länder.
Die Erhaltung und der Ausbau der FüInfoSys und FüWES in der Bundeswehr als nationale Kernfähigkeit ist eines der wesentlichen Ziele des Arbeitskreises. Ein besonderer Fokus liegt auf dem Themengebiet Interoperabilität im Bündnis und bei unterschiedlichsten Koalitionen im Einsatz. Dabei genießen Forderungen aus dem Einsatz, insbesondere hinsichtlich des Afghanistan Mission Networks und die Nutzung von SOA besondere Aufmerksamkeit.

## Arbeitskreis "Kommunikation"

Die wesentliche Voraussetzung für die Vernetzte Operationsführung ist eine leistungsfähige Kommunikation, aus dem Heimatland bis zum Konvoi und dem einzelnen Trupp.
Der Arbeitskreis Kommunikation verfolgt und befasst sich umfassend mit den Belangen der taktischen und strategischen Kommunikation. Er versteht sich als kompetentes und beratendes Expertengremium des Fachverbandes Wehrtechnik hinsichtlich des Einsatzes moderner Technologien und Systemlösungen im Bereich der taktischen und strategischen Kommunikation und sieht sich dabei als zentrales Bindeglied zwischen den Know-how-Trägern und Kompetenzzentren der wehrtechnischen Kommunikationsindustrie und der Bundeswehr sowie den Behörden des Bundes und der Länder.
Die Erhaltung und der Ausbau der taktischen und strategischen Kommunikation als nationale Kernfähigkeit ist eines der wesentlichen Ziele des Arbeitskreises. Weiter wird der Fokus auf die Interoperabilität zwischen den Teilstreitkräften und zwischen Streitkräften verschiedener Nationen sowie die Netzwerkfähigkeit im Sinne der vernetzen Operationsführung (NetOpFü) gelegt.

# Fachkreis "Aufklärung/EloKa"

## Dipl.-Ing. Jürgen Steiner, Vice President Product Sales Development, CASSIDIAN

*Dipl.-Ing. Jürgen Steiner, Leiter des Fachkreises Aufklärung/EloKa des Leitmarkts Defence im ZVEI-Fachverband Sicherheit*

Mit der Konzeption der Bundeswehr von 2004 hat sich die Bundeswehr der Verbesserung der Einsatzwirksamkeit durch die Befähigung der Streitkräfte zur vernetzten Operationsführung verschrieben. Eine zentrale Rolle spielt dabei das umfassende, ebengerechte Lagebild, für das eine Vielzahl von Informationen aus unterschiedlichsten Quellen ermittelt, zusammengeführt und adäquat bewertet werden müssen. Dabei sind eine große Menge von Informationen schnell zu verarbeiten und sicher, ggf. auch über weite Strecken, zu verteilen. Information ist zum neuen operativen Faktor geworden, den es zu nutzen und zu kontrollieren gilt. Die neue Herausforderung besteht darin, durch effiziente Aufklärung und Informationsverarbeitung Informationsüberlegenheit zu gewinnen, diese durch schnelle und fundierte Entscheidungen in Führungsüberlegenheit umzusetzen, um daraus Wirkungsüberlegenheit zu erzielen. Dies gilt nicht nur für das Lagebild der Streitkräfte auf den unterschiedlichen Ebenen, sondern auch für das gesamtstaatliche Lagebild zur Krisenfrüherkennung und dem daraus abzuleitenden Krisenmanagement der Bundesregierung. Informationen bleiben überall die Grundlage jeder Entscheidung. Diese Informationen werden durch unterschiedliche Organisationen geliefert, die sich bei der Informationsgewinnung unterschiedlichster Sensoren, technischer Aufklärungsmittel und Systeme zur Informationsverarbeitung bedienen.

Ein großer Anteil der Firmen, die Sensoren zur Aufklärung, Aufklärungssysteme und Systeme zur Informationsverarbeitung entwickeln und unterstützen und in den letzten Jahren der Bundeswehr geliefert haben, sind Mitglied des Fachkreises Aufklärung/EloKa im Leitmarkt Defence des ZVEI-Fachverbandes Sicherheit und leiten mit ihrem industriellen Potenzial wesentliche Beiträge zur technischen Unterstützung für die weltweite Aufklärung, die weiträumige Aufklärung und die Aufklärung im Einsatzgebiet.

Der Fachkreis Aufklärung/EloKa versteht sich als kompetentes, beratendes und auch in eigener Initiative tätiges Expertengremium des ZVEI-Fachverbandes Sicherheit – Leitmarkt Defence für Einsatz und Anwendung moderner Technologie in Aufklärungs- und EloKa-Systemen. Der Fachkreis fungiert dabei als Bindeglied zwischen den Know-how-Trägern und Kompetenzzentren der Industrie und der Bundeswehr, weiteren Behörden und Einrichtungen des Bundes, der Länder, der Europäischen Union sowie sonstigen Bedarfsträgern (z.B. NATO) sowohl auf System- als auch auf Ausrüstungsebene. Wesentliche Zielsetzung der Arbeiten ist es, in aktiver Wechselwirkung zwischen Industrie und Bedarfsträgern die Kommunikation zu fördern, Einsatzmöglichkeiten und Chancen innovativer Systemlösungen aufzuzeigen, zu bewerten und in die Anwendung zu überführen.

Ziele und Aufgaben des Fachkreises:

- Informationsaustausch zwischen Mitgliedsunternehmen und Amtsvertretern über erkannte Defizite, festgestellte Fähigkeitslücken und Angebote an neuen Verfahren und Technologien
- Synergiegewinnung aus den Potenzialen der deutschen wehrtechnischen Industrie und Stärkung der Wettbewerbsposition der Mitgliedsunternehmen bei allen Fachthemen


*AWACS bei Wartung* Quelle: EADS

*Bodenüberwachungsradar GO12* Quelle: Thales Deutschland GmbH

- Erarbeitung von übergeordneten Systemlösungen im vorwettbewerblichen Bereich, soweit dies im Interesse der Mitgliedsunternehmen liegt
- Einflussnahme auf F&T-Anstrengungen im Bereich Sicherheit und Verteidigung
- Inhaltliche und zielgruppenspezifische Abstimmung mit den Gremien des ZVEI und anderer Verbände

Damit die Firmen der wehrtechnischen Industrie frühzeitig ihre F&E-Aktivitäten in die richtige Richtung vorwärts treiben können, ist es unerlässlich, den Bedarf der Streitkräfte frühzeitig zu erkennen, um Entwicklungen rechtzeitig anzuschieben. Da es zurzeit noch keine regelmäßige und systematische Information der Industrie über den Bedarf der Streitkräfte in den unterschiedlichen Fähigkeitskategorien gibt, informieren sich die Firmen punktuell bei unterschiedlichsten Ansprechpartnern und Dienststellen auf unterschiedlichen Ebenen. Der Fachkreis Aufklärung/EloKa des ZVEI-Fachverbandes Sicherheit bündelt diese Aktivitäten in seiner Gremienarbeit. Auf der Grundlage aktueller Fragestellungen besucht er die für ihn relevanten Dienststellen und führt einen Informationsaustausch mit den dortigen Funktionsträgern und gegebenenfalls auch mit den zu den Treffen eingeladenen Konzeptionären der ministeriellen und/oder Ämterebene durch. Dabei richtet sich der Fokus sowohl auf die für Aufklärung/EloKa zuständigen Bereiche in der Streitkräftebasis, wie auch in den Teilstreitkräften.
Eine Analyse des entsprechenden Bedarfs und ein Informationsaustausch zum gegenseitigen Nutzen wurden in der zurückliegenden Zeit bei folgenden Dienststellen durchgeführt:

- Wehrtechnische Dienststelle 81 (WTD 81), Greding
- Wehrtechnische Dienststelle 71 (WTD 71), Eckernförde
- Kommando Strategische Aufklärung (KSA), Gelsdorf
- Ausbildungszentrum Heeresaufklärungstruppe, Munster
- Zentrum Elektronischer Kampf Fliegende Waffensysteme, Lagerlechfeld

Im Gespräch werden dabei mit den Amtsvertretern und Dienststellen Informationen über den aktuellen Bedarf aus den Einsätzen, Planungen, neue Technologien und darauf aufbauende Lösungen ausgetauscht. Dabei spielen aber auch Fragen der Kundenzufriedenheit und die Alltagstauglichkeit von bereits eingeführten Produkten eine große Rolle. Darüber hinaus unterstützen die Treffen auch die bessere Identifizierung von Ansprechpartnern auf der Amts- und Industrieseite für die einzelnen Firmen im Rahmen ihres Interessenspektrums und fördern den Ausbau eines Netzwerkes zur schnelleren und zielgerichteten Kommunikation zwischen Bundeswehr und Industrie.

Auch im weiteren Verlauf der Neuausrichtung der Bundeswehr bieten die im Fachkreis Aufklärung/EloKa mitarbeitenden Firmen den Ausbau des Dialogs an, um gemeinsam übergeordnete Systemlösungen im vorwettbewerblichen Bereich zu diskutieren und zu erarbeiten. Großen Wert legen die Firmen dabei auf die frühzeitige Information über neue konzeptionelle Überlegungen, gebilligte Konzepte und zeitliche Planungen durch die Bundeswehr, weil nur dann die Firmen sich mit ihren eigenen F&E-Aktivitäten frühzeitig und gezielt auf diese Themen/Herausforderungen einstellen können.

Die Neuausrichtung der Bundeswehr führt unter anderem auch zur personellen Reduzierung in nahezu allen Bereichen. Bereits jetzt gibt es Industrieunterstützung in unterschiedlichsten Abstufungen von Kooperationen bis hin zum vollständigen Outsourcing, von der Verpflegungsbereitstellung bis zum Betriebsstofftransport im Einsatzland. Mit SAATEG Zwischenlösung – Heron 1 gibt es auch im Bereich Aufklärung einen Dienstleistungsvertrag für den Betrieb des unbemannten Aufklärungssystems Heron 1 in Afghanistan. Aus Sicht des Fachkreises Aufklärung/EloKa gibt es im eigenen Interessensspektrum weiteres Potenzial für Kooperationen der Bundeswehr mit der Industrie oder partiell zur Übernahme von Aufgaben durch die Industrie, die zur personellen Entlastung führen und zusätzliche Kräfte für den Einsatz freisetzen könnten. Diese Chancen sollten genutzt werden. Der Fachkreis Aufklärung/EloKa steht für den Dialog bereit.

# Fachkreis "Simulationssysteme"

Tom Schüller, Key Account Director Air bei Thales Defense & Security Systems

*Tom Schüller, Leiter des Fachkreises Simulationssysteme des Leitmark Defence im ZVEI-Fachverband Sicherheit*

Der Fachkreis (FK) Simulationssysteme ist das zentrale Bindeglied der wehrtechnischen Industrie zur Amtsseite hinsichtlich der Nutzung moderner Simulationstechnologien bei Ausbildung und Einsatz sowie zur Unterstützung von Entwicklungs- und Beschaffungsvorhaben.

## Ziele und Aufgaben

Als zentrales Bindeglied zwischen den Fachfirmen der wehrtechnischen Industrie und der Amtsseite setzt sich der Fachkreis Simulationssysteme u.a. für die Interessen der deutschen Simulationsindustrie ein.

Die Ziele des FK Simulationsssysteme sind:

- Informationsabgleich im Rahmen der kartellrechtlichen Zulässigkeit in Bezug auf die nationale und internationale Marktsituation zur Identifizierung von Trends und zur Entwicklung eines zielgerichteten Bedarfs,
- Führen des Dialogs mit dem öffentlichen Auftraggeber zur konzeptionellen Weiterentwicklung von Simulationsanwendungen,
- Führen des Dialogs mit dem öffentlichen Auftraggeber zur Definition von Standards im Rahmen nationaler und internationaler Zusammenarbeit im Vorfeld geplanter Projekte,
- Anlaufstelle und Dialogplattform für Themen "Simulation" zur Erarbeitung von Problemlösungen im Rahmen des aktuellen und zukünftigen Aufgabenspektrums der Simulation in der Bundeswehr.

## Inhaltliche Schwerpunkte und Themen

Die teilnehmenden Unternehmen des FK Simulationssysteme repräsentieren den überwiegenden Teil der in Deutschland verfügbaren wehrtechnischen Kernkompetenz im Bereich Simulationstechnologie.

Diese Simulationstechnologie findet vielfältige Anwendung in

- Ausbildung und Training für die drei Teilstreitkräfte der Bundeswehr und für die Streitkräftebasis bei
- virtuellen Simulatoren und Live-Training,
- konstruktiver Simulation für Analyse, Planung und Entscheidungsunterstützung,
- Bereitstellung von Simulations- und Testumgebung für CD&E/M&S.

Die inhaltlichen Schwerpunkte sind deshalb stark an dem Erhalt und Ausbau dieser Kompetenz ausgerichtet. Von hohem Interesse der Mitglieder sind hier Informationen über

- Themen Simulation und Standards,
- zukünftige Anforderungen der Bundeswehr an Ausbildung,
- aktuelle Trends und neue Technologien (national und international) im Themenfeld Modellbildung und Simulation,
- Möglichkeiten zur Verifizierung und Validierung bereits vorhandener Simulationsmodule und deren Algorithmen.

Die sich verändernden Aufgaben im Sicherheitskontext, die gestiegene Dynamik im Zusammenhang von Bundeswehreinsätzen, die Bedrohung des Cyber-Space und weiterer grundlegend neuer Anforderungen und nicht zuletzt die Transformation der Bundeswehr – nicht nur der Streitkräfte – führen zu einer völlig neuen Bedeutung von Simulation. Simulation ist auf dem Weg integraler Bestandteil unterschiedlicher Prozesse und Vorgehen zu werden.

Als ein wesentliches Element im CD&E Prozess, aber auch bei der Evaluation von Beschaffungsvorhaben oder der Überprüfung von Einsatzgrundsätzen bietet die Simulation fundamentalen Mehrwert. Der Einsatz bei Entscheidungsunterstützung und Vorbereitung von Bundeswehrmissionen kann Sicherheit erhöhen und Kosten reduzieren.

*Schiesssimulator SAGITTARIUS* Quelle: Thales Deutschland GmbH

*Cockpitzelle Tiger* *Quelle: Reiser Systemtechnik GmbH*

In den letzten Jahren sind eindrucksvolle Fähigkeiten in den o.g. Bereichen unter Nutzung von Elementen der SuTBw nachgewiesen. Durch die Verwendung gängiger Standards ist eine Lösung erstellt worden, die jederzeit – auch durch Dritte – adaptier- und erweiterbar ist, um auch zukünftig mannigfaltigen Herausforderungen begegnen zu können. Sensor-Effektor-Untersuchungen im Kontext der sogenannten Network Enabled Capabilities (NEC) für Konzeptüberprüfungen sowie für die Analyse, Planung und Entscheidungsunterstützung wurden vielfach erfolgreich durchgeführt.

## Abdeckung von Fähigkeiten für NetOpFü durch die mitarbeitenden Firmen

Simulation ist ein wesentliches Element für die Konzeption, die Entwicklung und den Test von vernetzten Einsatzsystemen. Gestützt durch operationelle Erfahrung der Mitgliedsfirmen tragen diese mit ihren Fähigkeiten und langjährigen Erfahrungen zu technischen Lösungen der Vernetzung und Infrastruktur bei. Diese sind u.a.:

- Infrastruktur für Simulations- und Testumgebung,
- Lösungen zur Kopplung von Systemen und Simulatoren,
- Bereitstellung von Scenariogeneratoren zur Durchführung von Experimenten,
- Entwicklung von Software und Hardware zur Unterstützung und Auswertung.

Die Interaktion zwischen den unterschiedlichen (militär-) fachlichen Experten und den sogenannten Operational Advisers bereits in der Konzeptentwicklungsphase von Projekten hat sich als Vorgehensmodell bewährt. Diese Methode ist ebenfalls integraler Bestandteil der Data Farming Experimente im Rahmen unterschiedliche CD&E Aktivitäten im Kontext von NetOpFü-Fähigkeiten, um eine reibungslose und optimale Implementierung des operativen Bedarfs in die Simulation zu gewährleisten.

## Nutzen und Ergebnisse der Zusammenarbeit mit der Amtsseite

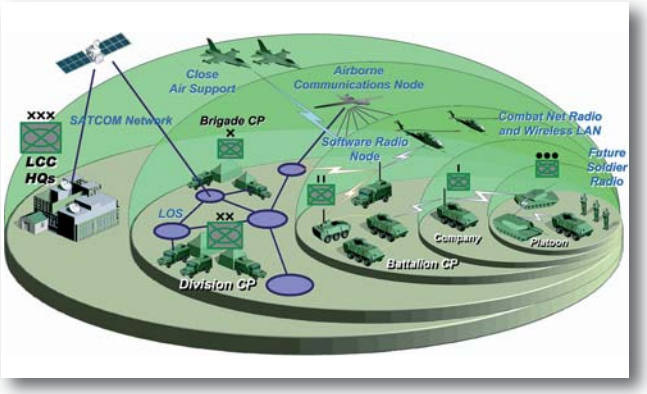
Die Mitglieder

- erhalten breit gefächerte Informationen aus dem Leitmark Defence des Fachverbands Sicherheit und des FK Simulationssysteme,
- haben die Möglichkeit, ihre Wissensbasis durch den Erfahrungsaustausch untereinander sowie zwischen Industrie und Bundeswehr/Behörden auszubauen,
- können ihre Anliegen gegenüber dem Kunden durch den Verband mit Nachdruck einbringen, d.h. sie profitieren von der Möglichkeit, offene Punkte sowie gemeinsame Unternehmensinteressen und -ziele mit relevanten Vertretern der Bundeswehr/Behörden zu erörtern und dabei die Sichtweise des Kunden kennenzulernen,
- profitieren von den unterschiedlichen Arbeitsgremien/Veranstaltungen mit Beteiligung der Bundeswehr.

Dies fördert

- die Positionierung der Mitgliedsfirmen im Wettbewerb sowie
- das frühzeitige Erkennen von Chancen und Risiken für die Mitgliedsunternehmen und schnelle Reaktion über den Fachverband mit Zugang zu Entscheidungsträgern.

Der FK Simulationssysteme ist die zentrale Plattform, welche sowohl auf konzeptioneller als auch auf technischer Ebene den Informations- und Gedankenaustausch zwischen der beteiligten wehrtechnischen Industrie und der Amtsseite ermöglicht. Insbesondere die Tatsache, dass dies im offenen Austausch mit verschiedenen Industrievertretern und außerhalb dedizierter Projekte erfolgt, bietet für alle Beteiligten einen echten Mehrwert.




*Taktisches Internet* *Quelle: THALES*

# Fachkreis “Product Support & Logistik”

## Dipl.-Kfm. Lothar Berndt, Leiter Geschäftsbereich Logistik und Mitglied der Geschäftsleitung der ESG Elektroniksystem- und Logistik GmbH

*Dipl.-Kfm. Lothar Berndt, Leiter des Fachkreises Product Support & Logistik des Leitmarkts Defence im ZVEI-Fachverband Sicherheit*

Der Fachkreis Product Support & Logistik ist das Lenkungsgremium der Arbeitskreise Prozesse/Technologien PS&L und Dokumentation/ Ausbildung PS&L für alle fachlichen Fragen im wehrtechnischen Product Support und der Logistik über den Life Cycle militärischer Vorhaben im Leitmarkt Defence des ZVEI-Fachverbands Sicherheit. Er bildet die verbandsseitige Informationsdrehscheibe für den Lenkungskreis, die zugeordneten Arbeitskreise und den industriell und militärisch besetzten Arbeitskreis (Bundeswehr) Logistik (AK LOG). Innerhalb seines Aufgabengebietes erarbeitet der Fachkreis strategische Vorschläge für die Verbandsarbeit und wirkt bei der Gestaltung von Rahmenbedingungen und Standards mit. Hierbei bildet die Konzeption des neuen Ausrüstungs- und Nutzungsprozesses den zukünftigen Orientierungsrahmen.

Folgende Aufgaben hat sich der Fachkreis gestellt:

- Definition seiner strategischen und inhaltlichen Weiterentwicklung und der der zugehörigen Arbeitskreise
- Querschnittliche und fachliche Koordination der Arbeitskreise und deren Aufgabenverteilung
- Verbandsseitige Kommunikation mit Kunden und Kundenorganisationen
- Erarbeitung und Darstellung zukunftsorientierter Themen in Zusammenarbeit mit dem Kunden
- Erarbeitung von speziellen logistischen Lösungen in Unterarbeitsgruppen
- Wahrnehmung der Berichtspflicht gegenüber dem Lenkungskreis
- Überwachung der Trennung von Verbands- und Unternehmensinteressen

Schwerpunktthemen für die Zukunft sind die pragmatische Ausgestaltung der Konzeption des neuen Ausrüstungs- und Nutzungsprozesses und die Erstellung von Beiträgen zu neuen Kooperationen zwischen Bundeswehr und Industrie in der Logistik und dem damit verbundenen Dialog mit der Amtsseite. Dabei bringt sich der Fachkreis in den oben erwähnten AK LOG ein, dessen industrieseitige Koordination durch den Fachkreis wahrgenommen wird. Als Reaktion auf das vom Fachkreis Product Support initiierte Positionspapier “Künftige Kooperationen der Industrie/gewerblichen Wirtschaft im Bereich der Logistik mit der Bundeswehr” hat Staatssekretär Beemelmans die Vertreter im AK LOG zum gemeinsamen, proaktiven Vorgehen aufgefordert.

### Arbeitskreis “Technologien und Prozesse (PS&L)”

Der Arbeitskreis “Technologien und Prozesse (PS&L)” im Fachkreis “Product Support & Logistik” (FK PS&L) stellt die verbandsseitige Informationsdrehscheibe und das Zuarbeitsgremium zum Fachkreis für neue Technologien im logistischen Umfeld, für alle logistischen Fragen im Zusammenhang mit Materialerhaltung, Materialbewirtschaftung, IT-Konzepten und IT-Projekten mit logistischer Relevanz für Bundeswehr und Industrie dar.
Der Schwerpunkt der Arbeit im AK “Technologien und Prozesse” liegt in der firmenübergreifenden Diskussion von erkennbaren Trends in der Logistik sowie deren Analyse und

*Integrated Starter Generator G36* Quelle: L-3 Magnet-Motor GmbH

*Schutz von Logistikketten* Quelle: ESG GmbH

Bewertung. Ein Informationsaustausch zwischen Industrievertretern über teilstreitkraftspezifische (Heer, Luftwaffe, Marine) logistische Themen hinaus sichert dem Arbeitskreis eine ständige Aktualität.

Inhaltliche Schwerpunkte und Themen:

- Neue Technologien im logistischen Umfeld
- Proaktives Obsoleszenz-Management
- Positionspapier "Künftige Kooperationen der Industrie/gewerblichen Wirtschaft im Bereich der Logistik mit der Bundeswehr"
- Positionspapier "Industrieunterstützung der Truppe im Einsatz"
- Technologische Möglichkeiten für den Instandsetzer der Zukunft (z.B. Telemaintenance)
- Supply-Chain-Management-Prozesse der Bundeswehr (Analysen zu Hardware und Software)
- Vorschläge zur Ausgestaltung des Ausrüstungs- und Nutzungskonzeptes
- Full Service Support – industrieller Austausch

Alle im Arbeitskreis vertretenen Mitgliedsfirmen des ZVEI erhalten über den Arbeitskreis denselben Informationsstand und den gleichen Zugang zur Amtsseite. Gemeinsame Handlungsfelder werden vorwettbewerblich mit dem öffentlichen Auftraggeber neutral diskutiert und bewertet. Hierdurch werden sowohl unmittelbare Beiträge zur Fähigkeitssteigerung der Bundeswehr im Bereich eines querschnittlichen Logistikansatzes als auch zur Problembeseitigung innerhalb logistischer Arbeitsfelder der Industrie ermöglicht. Die erarbeiteten Konzepte dienen weiterhin als Dialoggrundlage zur Diskussion der zukünftigen Zusammenarbeit zwischen Bundeswehr und Industrie.

## Arbeitskreis "Technische Dokumentation und Ausbildung"

Die im ZVEI-Arbeitskreis "Technische Dokumentation und Ausbildung" (AK TDA) vertretenen Firmen haben es sich zum Ziel gesetzt, die nationalen Belange der "Beschreibenden Technischen Dokumentation" nach ASD-S1000D-Standard durch breite Beteiligung von am Prozess beteiligten Dienststellen der Bundeswehr, der Verbände (BDLI, ZVEI) und der herstellenden Industrie intensiv zu begleiten und Empfehlungen für künftige Versionen und das mittelfristige Vorgehen zu beschließen. Mitglieder dieses Arbeitskreises wirken in diversen nationalen und internationalen Gremien mit und vertreten dort die Interessen der nationalen Industrie.

Darüber hinaus verfolgen die Mitglieder im Arbeitskreis Fragestellungen im breiten Anwendungsbereich der interaktiven elektronisch-technischen Dokumentation (IETD). Insbesondere geht es um Problemlösungen und Vorschläge, mit denen die Materialerhaltung der Waffensysteme unter Nutzung der digital verfügbaren Daten der Dokumentation künftig aktueller, moderner und kostengünstiger als bisher gestaltet werden kann. Zudem soll zur Bewusstseinsbildung hinsichtlich der Einsatzmöglichkeiten und -chancen innovativer IETD- und CUA-Lösungen beigetragen werden.

Zu den Aufgaben des Arbeitskreises gehört auch die enge Zusammenarbeit mit anderen Verbänden, wie z.B. dem Bundesverband der Deutschen Luft- und Raumfahrtindustrie (BDLI), um ein industriell abgestimmtes Vorgehen zu erreichen und um Doppelarbeiten zu vermeiden.

Inhaltliche Schwerpunkte und Themen:

- Technische Dokumentation nach ASD-Standards (S 1000D, S 2000M, Nationale Durchführungsbestimmungen)
- Konzeption der Übernahme von Elementen aus der IETD in SASPF
- Computerunterstützte Ausbildung (CUA), Fernausbildung und E-Learning unter Berücksichtigung bereits erstellter Informationen aus dem Anteil Technischer Dokumentation

Der Arbeitskreis ist Teil des Fachkreises "Product Support & Logistik" des Leitmarktes Defence im ZVEI-Fachverband Sicherheit und ist im definierten Aufgabenbereich das zentrale Bindeglied zwischen wehrtechnischer Industrie und Logistik-Dienstleistern, das den Know-how- und Technologie-Transfer mit der Bundeswehr sowie Behörden des Bundes und der Länder unterstützt.

# Zivil- und Katastrophenschutz – Warnung der Bevölkerung mittels Rauchwarnmeldern

Heinrich Herbster, Geschäftsbereichsleiter Marktentwicklung,
Hekatron Vertriebs GmbH

*Heinrich Herbster, Leiter des Fachkreises Brandmeldesysteme des Leitmarks Safety im ZVEI-Fachverband Sicherheit*

In der Euphorie über das Ende der äußeren Bedrohung wurde in den 90er Jahren beim Drang nach Kostensenkung übersehen, dass zur Warnung der Bevölkerung vor heraufziehenden akuten Bedrohungen durch Umwelt- oder Naturereignisse, wie durch Großbrände in Industrieanlagen freigesetzten Giftwolken, durch Überschwemmungen usw. ohne die vorher allgegenwärtigen Sirenen ein effektives und kostengünstiges Warnsystem fehlt. Die Sirenensysteme künftig flächendeckend wieder aufzubauen, wäre allerdings viel zu teuer.

Selbst wo die Sirenen noch in Betrieb sind, mehren sich die Zweifel, ob sie künftig noch ausreichen, besonders zur Nachtzeit die Bevölkerung im Gefahrenfalle zu wecken. Immer besser gedämmte Türen, Fenster und Wände verhindern nicht nur den Wärmeverlust von innen nach außen, sondern auch die Schallübertragung von außen nach innen. Wenngleich der Hörsinn als einziger Sinn im Schlaf nie völlig abgeschaltet wird, bedarf es meist erheblicher Lautstärke, einen Menschen aus dem Tiefschlaf zu wecken. Desweiteren verfügen in der Regel diese Sirenennetze über keine redundanten Energieversorgungssysteme und sind somit bei Ausfall des elektrischen Versorgungsnetzes nicht funktionsfähig.

Rauchwarnmelder schaffen das typischerweise, weil sie konstruiert sind, um bei Detektion von Brandrauch die Personen im Installationsraum jederzeit sicher zu warnen, zur Nachtzeit also zu wecken, notfalls aus dem Tiefschlaf. Dazu legt die einschlägige europäische Produktnorm (EN 14604) eine Mindestlautstärke des Warnsignals von 85dB fest, zu messen in drei Metern Abstand vom Melder. Für hörgeschädigte Personen gibt es inzwischen serienmäßig hergestellte, spezielle Zusatzgeräte wie Rüttelkissen oder optische Signalgeräte, die zur Tag- und Nachtzeit für eine rasche Wahrnehmung sorgen. Diese Geräte werden mittels einer speziellen Funkschnittstelle, die in den Rauchwarnmelder eingebaut wird, an diesen angebunden und bei Rauchdetektion ebenfalls aktiviert.

Diese besonderen Eigenschaften von Rauchwarnmeldern lassen sich technisch auch nutzen, um im Katastrophenfall die Bevölkerung jederzeit mit einem Aufmerksamkeitssignal zu versorgen, vor allem aber nachts zu wecken. Damit würde eine große Lücke im Warnsystem in Deutschland geschlossen. Warnsignale können über SATWAS und künftig MOWAS zentral und/oder regional erzeugt und abgesetzt werden. Doch nützt die Meldungsübertragung per SMS oder E-Mail wenig, wenn diese Geräte abgeschaltet, gerade stromlos, z.B. in Handtaschen außerhalb des Schlafzimmers liegen und nicht gehört werden (können). Ein Rauchwarnmelder ist, sofern er in einer Wohnung installiert ist, stets präsent und bei regelmäßiger Wartung auch funktionsbereit. An der Zimmerdecke montiert, kann er nicht unter Kleidung oder Zeitungen begraben, nicht in Handtaschen versenkt und vor allem nicht ausgeschaltet werden.

Inzwischen haben neun Bundesländer zur Verbesserung des Brandschutzes in Wohnhäusern und Wohnungen sogar eine Pflicht zum Einbau von Rauchwarnmeldern in ihre Bauordnungen eingefügt, sieben davon mit Nachrüstpflicht für Be-

*Katastrophenfall Erdbeben* Quelle: THW/Michael Walsdorf

standswohnungen; in Niedersachsen und Nordrhein-Westfalen haben die Regierungen entsprechende Gesetzgebungsinitiativen einschließlich Nachrüstpflicht für den Bestand eingeleitet oder angekündigt. Wo die Übergangsfrist für die Bestandsnachrüstung bereits abgelaufen ist, sind die Ausstattungsquoten auf deutlich über 80% aller Wohnungen und Einfamilienhäuser gestiegen. Diese absehbar in allen Bundesländern vorhandene Ausstattung stellt eine hervorragende Basis dar, darauf ein System zur Warnung der Bevölkerung im Katastrophenfall aufzusetzen.

Die Aktivierung eines Rauchwarnmelders beinhaltet ein Weck- oder Aufmerksamkeitssignal. Das gilt nicht nur zur Nachtzeit. Schichtarbeiter, die tagsüber schlafen müssen, werden ebenso zuverlässig geweckt wie wache Personen zur Aufmerksamkeit gezwungen, allein durch die nicht regelbare Lautstärke des Signals. Notwendig ist für die technische Nutzung von Rauchwarnmeldern für ein solches Weck- oder Aufmerksamkeitssignal der Einbau einer spezifischen Empfangseinrichtung für das per Funk aus SATWAS/MOWAS übertragene Alarmsignal. Die Empfangseinrichtung ist mit einem Chip ausgestattet, der die Signale empfängt, decodiert und ggf. dechiffriert und das Warnsignal auslöst.

Für die Funkübertragung des Warnsignals aus dem SATWAS/MOWAS-System oder von der alarmierenden Leitstelle an die Rauchwarnmelder kommen verschiedene Funksysteme in Betracht, wie z.B. DCF77, eMessage, BOS-Digitalfunk, GSM, GSM-Broadcasting, GSM mittels SMS-Massenversand sowie RDS-TCM. Alle Systeme haben ihre speziellen Vor- und Nachteile bei Nutzung in Rauchwarnmeldern zur flächendeckenden Warnung der Bevölkerung. Zusätzlich stellen sich bisweilen komplexe, teils gegenläufige technische Anforderungen an solche Melder bzw. das Funkempfangsmodul.

Das System sollte verschlüsselt und dadurch möglichst sabotagefrei arbeiten. Die batteriegestützte Stromversorgung des Funkempfangsmoduls sollte mindestens 5 Jahre Standzeit gewährleisten, um den Komfort moderner Melder, deren Batterie für die Detektionseinheit heute bei Qualitäts-

meldern 10 Jahre beträgt, nicht zu sehr zu mindern und zugleich die Betriebssicherheit zu erhöhen. Um dies zu erreichen, muss auf eine aktive Funkanbindung (Empfangen und Senden) verzichtet werden; in Betracht kommt einzig eine passive Anbindung, also ausschließlich eine Empfangsfunktion. Der Signalton muss sich von der Warnung im Brandfall deutlich unterscheiden. Die Signalisierung muss seitens der Leitstelle regional eingrenzbar sein, in Gebieten mit dichter Besiedlung möglichst kleinzellig.

Die hausgenaue Warnung wäre zwar ideal, würde aber die jeweils individuelle Eingabe von geographischen Koordinaten oder einer Gerätenummer in jedes Gerät und deren Hinterlegung im System erfordern, beides nicht zu leisten oder mit Fachpersonal unbezahlbar, mit Eigenaktivität der Bürger im Ergebnis ineffizient, weil viele Bürger technisch und im Mitwirkungswillen überfordert würden. Für ein effektives und effizientes Warnsystem muss sich folglich die lokale Eingrenzung des Warnbereichs aus dem System selbst ergeben, sie darf nicht auf einer Eingabe am Empfangsgerät basieren.

Infolgedessen erscheint derzeit der Massenversand von Warnsignalen im GSM-Netz als eine der besten Lösungen, weil die Zahl der Sendemasten gerade in Ballungsgebieten bereits außerordentlich hoch ist und damit die kleinteilige Funkzellausdehnung eine nötigenfalls enge Begrenzung des Warnbereichs erlaubt. Dafür kommen technisch sowohl eine Broadcasting-Funktion wie ein SMS-Massenversand in Betracht. Doch stehen dieser Nutzung in Deutschland derzeit noch verschiedene rechtliche Hürden entgegen. Beide Systeme sind im Ausland bereits im Einsatz, wenngleich nicht in Verbindung mit Rauchwarnmeldern, und haben sich bislang bewährt.

Die Industrie steht bereit, technisch ausgereifte Systeme zur Warnung der Bevölkerung mittels Weck- oder Aufmerksamkeitssignal zu jeder Tages- oder Nachtzeit in jede Wohnung zu liefern. Gefordert sind jetzt Politik und Regierungen in den Bundesländern, die notwendigen politisch-administrativen Entscheidungen zu treffen und die rechtlichen Voraussetzungen für ein solches dringend benötigtes Warnsystem zu schaffen.

# Auf dem Weg von den Kritischen Infrastrukturen zur Superkritischen Infrastruktur

Peter Krapp, Geschäftsführer des ZVEI-Fachverbands Sicherheit und
Justin Just, Referent Security/Defence des ZVEI-Fachverbands Sicherheit

*Peter Krapp*

*Justin Just*

Die Bundesregierung hat in den zurückliegenden Jahren viel unternommen, um dem Schutz Kritischer Infrastrukturen Systematik zu verleihen und um das Schutzniveau in Deutschland in Zusammenarbeit mit der Wirtschaft zu verbessern. Immer stärker rückt die Frage in den Vordergrund, ob bei diesen Ansätzen auch die rasant ansteigenden Interpendenzen einzelner Kritischer Infrastrukturen voneinander angemessen berücksichtigt werden und auf welche Weise der zunehmenden Vernetzung einzelner Infrastrukturen im Sinne der Sicherheit Rechnung getragen werden kann.

Die Bundesregierung definiert Kritische Infrastrukturen als Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1]

In technischer Hinsicht hat man die Energieversorgung, Informations- und Kommunikationstechnologie, Transport und Verkehr sowie die Wasserversorgung und Abwasserentsorgung als kritische Basisinfrastrukturen identifiziert. Daneben existieren die staatlichen und privaten Dienstleistungsinfrastrukturen wie das Gesundheitswesen, Ernährung, Notfall- und Rettungswesen, Katastrophenschutz, das Parlament und die Regierung, die öffentliche Verwaltung, Justizeinrichtungen, Finanz- und Versicherungswesen sowie Medien und Kulturgüter, deren Existenz und Verfügbarkeit für unser Zusammenleben unabdingbar sind. Hierbei liegt auf der Hand, dass die Dienstleistungsinfrastrukturen von der Funktionsfähigkeit der technischen Basisinfrastrukturen abhängen.

Von der Bundesregierung wurde zu Recht ein besonderer Schwerpunkt auf die Berücksichtigung der IT-Infrastruktur gelegt, da gerade der Ausfall bestimmter IT-Anwendungen leicht den Ausfall weiterer Kritischer Infrastrukturen nach sich ziehen kann. Ausgestaltung hat diese Schwerpunktsetzung im “Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)” und dessen Umsetzungsplan gefunden. Losgelöst hiervon wird in letzter Zeit zudem das Internet als eigene schützenswerte Infrastruktur diskutiert.

Allerdings ist vor diesem Hintergrund auch das Paradigma der Interpendenzen von Infrastrukturen untereinander, bei denen der Ausfall einer Infrastruktur den domino- und kaskadenartigen Ausfall weiterer Infrastrukturen nach sich ziehen kann, neu zu betrachten. Die voranschreitende Durchsetzung vieler Lebensbereiche mit IT ist ein volkswirtschaftlich richtiger und notwendiger Prozess. Die Diffusion von Standard IT trägt zur Erschließung von Effizienzreserven bei, ermöglicht interoperable und herstellerübergreifende kompatible Lösungen, steigert die Verfügbarkeit von Anlagen und Systemen und den Komfort im Alltag. Smart Grids ermöglichen eine effiziente Energienutzung; in der Kommunikation, im Verkehrswesen, der Logistik, aber auch in der industriellen Fertigung ist der Einsatz von IT-basierter Prozesssteuerung an der Tagesordnung. Hierbei kommt es zu einer Vernetzung von Infrastrukturen und Systemen miteinander, die früher unabhängig bzw. proprietär waren und nun enger zusammenrücken und Interdependenzen entwickeln. Stromversorgungsnetze als Beispiel sind grundsätzlich “n-1-sicher”, d.h. so konzipiert, dass sie den Ausfall eines beliebigen Betriebsmittels verkraften können. Die Durchdringung mit IT und internetbasierten Anwendungen gepaart mit einer Vernetzung mit anderen Infrastrukturen unter dem Vorzeichen der Effizienzsteigerung hingegen macht sie für Störungen aus angrenzenden Systemen emp-

findlicher, unabhängig davon, ob diese natürlichen oder anthropogenen Ursprungs sind.

Gleichzeitig mit den positiven Effekten der Vernetzung, nämlich der besseren Nutzung von Effizienzreserven bedingt durch eine verbesserte Steuerungs- und Kontrollierbarkeit, geht analog zum "Verletzlichkeitsparadoxon" also auch ein Risiko einher, nämlich die umso stärkere Auswirkung einer Störung, in einem Maße, in dem ein Land seine Versorgungsleistungen weniger störanfällig macht.[2] Durch die Vernetzung verschiedener Infrastrukturen miteinander sind unsere Systeme leistungsfähiger geworden und beispielsweise Energieengpässe leichter vermeidbar. Die Versorgungssicherheit wird erhöht. Gleichzeitig vernetzen wir jedoch verschiedene kritische Infrastrukturen miteinander, sodass "Superkritische Infrastrukturen" entstehen, in denen sich Störfälle gleichfalls potenziert auswirken. Ebenfalls potenziert stellt sich dann auch die Frage, welches System nach einer Störung in der Superkritischen Infrastruktur die Fähigkeit besitzt, aus sich selbst heraus wieder den Betrieb aufzunehmen, ohne hierzu Input von den ebenfalls funktionsgestörten Nachbarsystemen zu benötigen (sogenannte "Schwarzstartfähigkeit").

Einen Schritt weitergehend könnten Kritische Infrastrukturen künftig nicht als einzelne, durch Interpendenzen verbundene Bereiche betrachtet werden, sondern stattdessen eher als ein zusammenhängendes und übergreifendes "System der Systeme". Das wiederum verlangt gerade vom Schutzgedanken her eine veränderte und ganzheitlichere Herangehensweise. Anstelle der sektoral geprägten Wahrnehmung kritischer Infrastrukturen, wie beispielsweise Energieversorgung oder Informations- und Kommunikationstechnologie etc., wirft der Blick auf eine zusammenhänge Superkritische Infrastruktur andere Fragen auf. Dieses System der Systeme könnte beispielsweise organisatorisch in eine bestimmte Anzahl von Subsystemen gegliedert werden, die jeweils alle Sektoren der Kritischen Infrastrukturen beinhalten, unter Berücksichtigung von Resilienzerwägungen gestaltet sind, über Notlaufeigenschaften und Verfahren zum Lastabwurf in Gefahrensituationen verfügen und jeweils eine eigene Schwarzstartfähigkeit besitzen. Kann durch die technische Gestaltung der Übergänge zu den benachbarten Subsystemen die Ausbreitung einer potentiellen Störung verhindert werden, so können sich Subsysteme im Falle einer Störung gegenseitig bei einem Neustart unterstützen. Die Vorteile der Nutzung von Effizienzreserven durch Vernetzung könnten so innerhalb der Subsysteme weiterhin ausgeschöpft werden, während das durch verminderte Redundanzen entstandene Risiko ein Stück weit kompensiert würde.

Mit ihren Produkten und Strukturen ist die Elektroindustrie in allen Sektoren der kritischen Infrastrukturen fest verankert. Entsprechend hat das Thema Sicherheit in seinen jeweils verschiedenen Facetten einen festen Platz in den unterschiedlichen Arbeitsbereichen des ZVEI. Die Elektroindustrie ist mit ihren "enabling technologies" Gesprächspartner für die Politik sowie nationale und supranationale Institutionen der Sicherheit und der Öffentlichkeit. Der ZVEI ist mehr als die bloße Addition der Produkte und Systeme, indem er auf politischer Ebene Anstöße zur Bewältigung der zukünftigen Aufgaben beim Thema Sicherheit gibt und sich bei der Entwicklung neuer Risikoszenarien und Sicherheitsphilosophien aktiv einbringt.

[1] Bundesministerium des Innern (2009), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 3.
[2] Bundesministerium des Innern (2009), Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), S. 8.

# Der Fachkreis Maritime Sicherheit im ZVEI und sein Projekt für technische Lösungen zur Abwehr von Piraten vor dem Horn von Afrika

Stefan Jock, Head of Sales Security Radars, CASSIDIAN Sensors and Electronic Warfare

*Stefan Jock, Leiter des Fachkreises Maritime Sicherheit des Leitmarks Security im ZVEI-Fachverband Sicherheit*

Der Themenfokus des Fachkreises Maritime Sicherheit im ZVEI ist breit angelegt. So beschäftigt er sich unter anderem mit den Möglichkeiten zur Unterstützung der ressortübergreifenden staatlichen Zusammenarbeit. Ein Beispiel für dieses Engagement ist etwa der Austausch mit dem Maritimen Sicherheitszentrum – zuletzt durch einen Besuch unserer Industrievertreter vor Ort. Weitere Themen sind die maritime Grenzüberwachung, die Absicherung von Hafenanlagen und Offshore Windparks sowie der einheitliche maritime Informationsraum der EU. Einen besonderen Schwerpunkt unserer Arbeit bildet unser Projekt für technische Lösungen zur Abwehr von Piraten vor dem Horn von Afrika, auf das im Folgenden eingegangen werden soll.

In den Jahren zwischen 2008 und 2011 wurden vor dem Horn von Afrika jedes Jahr über 200 Schiffe durch Piraten angegriffen. Eine jeweils zweistellige Zahl dieser Angriffe endete in Entführungen. Nach Meldung des International Maritime Bureau kam es auch in diesem Jahr bis März bereits wieder zu 31 Angriffen und 6 Entführungen in diesem Seegebiet. Insgesamt befinden sich rund 200 Seeleute auf 14 Schiffen in Geiselhaft von Piraten. Nach einer Erhebung des Think Tanks Oceans Beyond Piracy verursachte die Piraterie allein im Jahr 2011 Kosten von ca. 5,1 Milliarden Euro, wovon etwa 20% Militäreinsätzen zur Pirateriebekämpfung geschuldet waren. 80% der Kosten lagen jedoch bei der privaten Schifffahrtindustrie. Lösegelder machten hierbei den geringsten Anteil aus. Stattdessen waren es Gegenmaßnahmen der Schifffahrt, wie beispielsweise das Aufrechterhalten einer hohen, einer Enterung erschwerenden Geschwindigkeit und der damit verbundene Treibstoffverbrauch, welcher hohe Kosten verursachte. Es handelt sich also um ein Problem mit volkswirtschaftlicher Tragweite. Hinzu kommt das enorme menschliche Leid, das durch die Piraterie versucht wird.

*Schiffscockpit* *Quelle: CASSIDIAN*

Deutschland ist von diesem Problem in besonderem Maße betroffen, da der deutsche Import und Export hauptsächlich über den Seeweg abgewickelt wird. Die deutsche Handelsflotte ist die drittgrößte weltweit. Allein 2010 wurden über 70 Schiffe deutscher Reedereien vor dem Horn von Afrika Opfer von Piratenangriffen.

Aus diesem Grund hat die deutsche Politik eine Reihe von diesbezüglichen Initiativen ins Leben gerufen. Neben dem Einsatz der Marine in der EU-Mission ATALANTA und dem Engagement des Bundesministeriums des Innern, müssen an dieser Stelle insbesondere die Aktivitäten des Koordinators der Bundesregierung für Maritime Wirtschaft und des niedersächsischen Innenministeriums erwähnt werden. Gleichwohl gestaltet sich der Fortschritt schwierig, zumal ein umfassender Schutz durch staatliche Kräfte laut Ministerien schon aus personellen Gründen nicht gewährleistet werden kann. Deswegen ist die Bundesregierung zurzeit bemüht, die Nutzung

privater Sicherheitsdienste durch die Reeder zu ermöglichen, um die Situation weiter zu verbessern.

Vor diesem Hintergrund haben sich im Sommer 2011 deutsche Unternehmen im Fachkreis Maritime Sicherheit zusammengeschlossen, um in einem gemeinsamen Projekt technische Lösungen zur Abwehr von Piraten zu erarbeiten. Hierbei knüpften sie insbesondere an ein Rundgespräch zur Piratenabwehr im Bundeswirtschaftsministerium im Mai 2011 an, welches aus Industriesicht einen Optimierungsbedarf im Hinblick auf die technologischen Antworten auf das Piraterieproblem offenbarte. In der Folge geführte Gespräche machten deutlich, dass ein Erfolg versprechender Ansatz nur möglich ist, wenn er neben technischen Aspekten insbesondere die Bedürfnisse von Reedern, Logistikdienstleistern und Versicherern berücksichtigt und von diesen mit getragen wird.

Um diesem Anspruch gerecht zu werden, befindet sich bei den Unternehmen des Fachkreises Maritime Sicherheit ein dreistufiges Konzept in der Ausarbeitung. Hierbei sind diverse Rahmenbedingungen zu berücksichtigen.

Zum einen sind zur Pirateriebekämpfung Kräfte unter Führung der NATO, der USA, der EU sowie verschiedene Einzelnationen vor Ort, die durch das Maritime Security Centre Horn of Africa (MSCHOA) und das regelmäßig tagende Gremium SHADE (Shared Awareness and De-Confliction) koordiniert werden. Zum anderen handelt es sich bei der fraglichen Region um ein enorm großes Seegebiet, welches allein im Bereich des Golfes von Aden jährlich von ca. 25.000 Schiffen passiert wird.

Alle Missionen zusammengenommen, operieren zwar bis zu 40 staatliche Einheiten im Seegebiet, was jedoch auf Grund der geographischen Dimension für eine effektive und effiziente Überwachung verhältnismäßig wenig ist. Daher ist der Faktor Zeit in diesem Szenario besonders kritisch, da staatliche Kräfte einen Piratenangriff unterbinden müssen, bevor ein Schiff geentert wird und Geiseln genommen werden.

*Containerschiff* *Quelle: Wasser- und Schifffahrtsdirektion Nord, Kiel*

Die zu beantwortende Frage ist also, wie Piratenangriffe von vornherein verhindert werden können bzw. das Zeitfenster zwischen dem Beginn eines Angriffs und einer Geiselnahme so vergrößert werden kann, dass staatliche Kräfte rechtzeitig zu Hilfe kommen können. Um hierzu einen Beitrag zu leisten, konzentriert sich das Konzept des Fachkreises Maritime Sicherheit auf drei Ansatzpunkte:

Erstens, die Unterstützung der technischen Fähigkeiten privater Sicherheitsdienste. War die Bundesregierung bezüglich der Nutzung bewaffneter privater Sicherheitsdienste zur Abwehr von Piraten eher zurückhaltend gewesen und Sicherheitsdienste von den Reedern lediglich als “zweitbeste Lösung” angesehen worden, so hat sich hier die Ausgangslage geändert. Aktuell arbeitet die Bundesregierung an einer Zertifizierung für maritime Sicherheitsdienste durch die Bundespolizei, auf der Grundlage einer Änderung der Gewerbeordnung. In einer Umfrage der Unternehmensberatung PWC bekannte sich fast ein Drittel der deutschen Reedereien zur Inanspruchnahme bewaffneter privater Sicherheitsdienste. In der Praxis dürfte die Zahl sogar noch höher liegen. Um die Qualität der Arbeit dieser Sicherheitsdienste sicherzustellen, ist es unabdingbar in einer Zertifizierung auch technische Fähigkeiten privater Sicherheitsdienste zu berücksichtigen, wie kommunikative Interoperabilität mit hoheitlichen Kräften, Fähigkeiten zur Überwachung des Umfeldes des Schiffes sowie gesicherte und dokumentierte Handhabung von Waffen und Gerät.

Zweitens, beschäftigen wir uns mit der Überwachung des Umfeldes eines zivilen Schiffes und den Möglichkeiten einer automatisierten Früherkennung von Gefahren. Heutige Handelsschiffe haben nur kleine Besatzungen. Die personellen Kapazitäten für zusätzliche Überwachungsaufgaben sind nicht vorhanden und zusätzliche Ausbildung zur Handhabung komplizierter Überwachungstechnik ist kaum möglich. Moderne Überwachungssysteme arbeiten jedoch selbständig, erkennen untypische Annährungen bereits auf große Entfernung und warnen die Besatzung automatisiert. Auf diese Weise wird die Reaktionszeit, die zum Einnehmen eines günstigen Kurses bleibt, vergrößert. Ebenfalls steht damit deutlich mehr Zeit für einen Hilferuf und nötigenfalls für einen geordneten Gang in einen Schutzraum zur Verfügung. Die Systeme sollen mobil und temporär einrüstbar sein, um so die Kosten gering zu halten.

Mit beschränktem Aufwand kann so eine erhebliche Verbesserung der Sicherung des Schiffes erfolgen. Eine Ergänzung der in den Best Management Practices der International Maritime Organization (IMO) empfohlenen Schutzmaßnahmen für Schiffe, die sich aktuell auf dem Niveau von Stacheldraht und Dummies bewegen, ist in dieser Hinsicht zu prüfen.

Drittens, sollte langfristig daran gearbeitet werden, die Grundlagen für die Erstellung eines umfassenden Lagebildes in diesem Gebiet mit wenigen Sensoren zu verbessern. Durch die weiträumige Überwachung des Seegebietes sowie von erkannten Piraten und deren Mutterschiffen wäre es möglich, die zivile Schifffahrt um Gefahrenstellen herumzuleiten und die wenigen hoheitlichen Kräfte so im Raum zu dislozieren, dass Angriffe rechtzeitig unterbunden werden können. Um diese Verbesserung zu einem vertretbaren Aufwand zu erreichen, werden im Fachkreis Maritime Sicherheit zurzeit die Möglichkeiten einer Einbindung der zivilen Schifffahrt in einem Netzwerk zur Lagebilderstellung mittels mobil auf den Schiffen einsetzbarer Sensoren geprüft.

Es ist ohne Frage, dass eine nachhaltige Lösung des Pirateriepoblems nur durch eine tragfähige Stabilisierung der Staaten in dieser Region geschehen kann. In der Zwischenzeit müssen jedoch Wege zur Verbesserung der Seesicherheit in diesem Gebiet gefunden werden. Die Ansätze der sicherheitstechnischen Industrie können hierzu einen wichtigen Beitrag leisten. Eine singuläre Antwort auf die Herausforderungen der Pirateriekriminalität wird es nicht geben. Stattdessen werden Lösungen immer aus einer Mischform der aufgezeigten Parameter bestehen. Um hier die richtige Gewichtung zu erarbeiten, befindet sich der Fachkreis Maritime Sicherheit im engen Dialog mit Ministerien, Reedern, Versicherern und Industrieverbänden.

# The Magazine for Europe's Security and Defence Community

Published by Hartmut Bühl, Editor in Chief, Brussels

THE MAGAZINE FOR EUROPE'S SECURITY AND DEFENCE COMMUNITY

Winner of the European Award 2011 for Citizenship, Security and Defence


**This magazine, a product of the Pro Press Publishing Group, Berlin, offers a platform for discussion on Security and Defence Policy in its various aspects. With its current circulation of 6.450 copies it makes a vital contribution to the Common Security and Defence Policy (CSDP).**

Since its very first edition in 2008 this magazine has combined the civil and military aspects of Security and Defence Policy, adopting what was later in 2009 laid down as the "comprehensive approach" in the Lisbon Treaty.

The EU has demonstrated that it has the political, civil and – with certain limitations – the military capabilities to contribute to the settlement of conflicts, and that it is co-operable with the United Nations and NATO as a reliable partner peace for crisis prevention, crisis management and humanitarian aid. By developing authentic relations with the United States of America and Russia, the other two major security players in the transatlantic region, the EU has become an important player in global security. But the current financial crisis with deep cuts in the national budgets could jeopardize strategic projects and capabilities.

By linking the magazine to the Pro Press Publishing Group's three most important annual conferences in Europe on Security and Defence:

- the **"European Congress on Disaster Management"** (www.civil-protection.com),
- the **"European Police Congress"** (www.european-police.eu) and
- the **"Congress on European Security and Defence"** (www.www.euro-defence.eu),

Hartmut Bühl has succeeded in creating a veritable platform for community-building among readers and participants from Europe and beyond.

**Further Information about the magazine: www.magazine-the-european.com**

## Authors of 12th issue No 1/2012

**"A politico-philosophical analysis of NATO"**

**Dr Henri-Paul Hude,**
Philosopher and Director Center for Military Ethics, Coëtquidan

**"Facing Iran: Stepped-up pressure just might work"**

**Emily B. Landau,**
Director of the arms control program, Institute for National Security Studies (INSS), Tel Aviv University

**"The European defence industry"**

**Jean Paul Herteman,**
CEO, Safran, Paris

## Subscription order: by Fax to +49(0)228 9709738

**Karin Dornbusch** · ***Advertising Manager*** · Phone: +49(0)228 9 70 97 40, E-Mail: subscription@euro-defence.eu

3 issues for one year, including postage and delivery:

☐ International subscription: 66,- Euro ☐ Subscription EU: 42,- Euro

Company: ..... VAT no.: .....

Address (Street, Zip-Code, Town, Country): .....

.....

Phone: ..... Fax: .....

E-Mail: ..... Date, Signature: .....

AFCEA Bonn e.V.

# 26. AFCEA Fachausstellung
# Informations- und Kommunikationstechnik

unter der Schirmherrschaft des Staatssekretärs im BMVg,
Herrn Stéphane Beemelmans

mit Vorträgen zum Thema

## Mobile Computing für den/im Einsatz

## 09./10. Mai 2012
## Stadthalle Bad Godesberg

**Ausstellende Firmen**

# Ausstellerliste AFCEA Fachausstellung 2012

| | Ausstellende Firma/Organisation | Stand-Nr. |
|---|---|---|
| 1 | ATM ComputerSysteme GmbH | G 2 |
| 2 | Atos IT Solutions and Services GmbH | Brunnensaal |
| 3 | Avitech AG | G 14 |
| 4 | BAKO Systemintegration GmbH & Co. KG | Z 13 |
| 5 | Bechtle GmbH & Co.KG, IT-Systemhaus Bonn | F 5 |
| 6 | Behörden Spiegel / ProPress Verlagsgesellschaft mbH | F 12 |
| 7 | Berner & Mattner Systemtechnik GmbH | P 10 |
| 8 | BGS Beratungsgesellschaft Software Systemplanung AG | G 10 |
| 9 | Bit Tradition GmbH | B 2 |
| 10 | BWI Leistungsverbund | G 13 |
| 11 | CASSIDIAN | Z 7 |
| 12 | CeoTronics AG | F 1 |
| 13 | Citrix Systems GmbH | P 7 |
| 14 | CONDOK GmbH | P 11 |
| 15 | CONET Business Consultants GmbH | F 10 |
| 16 | CONET Solutions GmbH | F 10 |
| 17 | Consinto GmbH | ZA 1 |
| 18 | Cordsen Engineering GmbH | F 6 |
| 19 | CPM Communication Presse Marketing GmbH | FR 2 |
| 20 | CSC | K 4 |
| 21 | Deutsche ELNO GmbH | Z 4 |
| 22 | Deutsche Gesellschaft für Wehrtechnik e.V. (DWT) | F 7 |
| 23 | DeviceLock Europe GmbH | P 2 |
| 24 | EGL Elektronik Vertriebs GmbH | T 3 |
| 25 | ETG – Elektronik + TEMPEST GmbH | FR 5 |
| 26 | EMC Deutschland GmbH | P 9 |
| 27 | ESG – Elektroniksystem- und Logistik- GmbH | G 1 |
| 28 | Esri Deutschland GmbH | G 6 - G 8 |
| 29 | Exelis Visual Information Solutions | G 6 - G 8 |
| 30 | ExperTeach GmbH | B 10 |
| 31 | Fraunhofer FKIE | F 8 |
| 32 | Fraunhofer IOSB | T 1 |
| 33 | FREQUENTIS Nachrichtentechnik GmbH | K 7 |
| 34 | Galleon Embedded Computing GmbH | B 6 |
| 35 | GBS TEMPEST & Service GmbH | P 12 |
| 36 | GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH | G 21 |
| 37 | Geosecure | G 6 - G 8 |
| 38 | GEOSYSTEMS GmbH | G 3 |
| 39 | GFN AG | P 3 |
| 40 | GPP Service GmbH & Co KG | K 5 |
| 41 | Green Data Systems GmbH & Co. KG | ZA 5 |
| 42 | Hardthöhenkurier | FR 3 |
| 43 | Hitachi Data Systems GmbH | T 2 |
| 44 | HP Deutschland | Z 11 |
| 45 | IABG-Industrieanlagen-Betriebsgesellschaft mbH | P 1 |
| 46 | IBM Deutschland GmbH | G 20, ZA 2 |
| 47 | ICOS Gesellschaft für Industrielle Communicationssysteme mbH | G 22 |
| 48 | Indra S.A. | G 14 |
| 49 | INFODAS GmbH | G 9 |
| 50 | Integer Solutions GmbH | K 8 |
| 51 | Intergraph SG&I Deutschland GmbH | G 3 |
| 52 | ITT Exelis | Z 1, ZA 3 |
| 53 | itWatch | G 19, E 1 |
| 54 | JK DEFENCE & SECURITY PRODUCTS GMBH | P 6 |
| 55 | Kontron AG | T 4 |
| 56 | Lachen helfen e.V. | E 2 |
| 57 | Liske Informationsmanagementsysteme | FR 4 |
| 58 | LOG GmbH | K 6 |
| 59 | Logic Instrument GmbH | Z 3 |
| 60 | Logica Deutschland GmbH und Co. KG | K 1 |
| 61 | Luciad | K 3 |
| 62 | Maibach Industrie-Plastic GmbH | Z 9 |
| 63 | Martin Yale International GmbH | ZA 4 |
| 64 | Microsoft Deutschland GmbH | F 9 |
| 65 | Mittler Report Verlag GmbH | P 4 |
| 66 | ML Consulting GmbH | F 13 |
| 67 | Mönch Verlagsgesellschaft mbH | FR 1 |
| 68 | Motorola Solutions GmbH | K 8 |
| 69 | ND SatCom Defence GmbH | Z 7 |
| 70 | Oracle Deutschland B.V. & Co. KG | T 5 |
| 71 | Overwatch Systems Ltd. | P 5 |
| 72 | Pan Dacom Direkt GmbH | T 6a |
| 73 | Pan Dacom Networking AG | T 6b |
| 74 | Panasonic Deutschland GmbH | Z 5 |
| 75 | PROCITEC GmbH | B 8 |
| 76 | promegis GmbH | P 5 |
| 77 | PWA Electronic Service- und Vertriebs- GmbH | Z 5 |
| 78 | Rockwell Collins Deutschland GmbH | Z 2 |
| 79 | roda computer GmbH | Z 8 |
| 80 | Rohde & Schwarz Vertriebs-GmbH | G 18 |
| 81 | rola Security Solutions GmbH | G 16 |
| 82 | Saab AB – Saab International Deutschland GmbH | Z 14 |
| 83 | SAP Deutschland AG & Co. KG | G 12 |
| 84 | Schnoor Industrieelektronik GmbH & Co. KG | G 5 |
| 85 | Schönhofer Sales and Engineering GmbH | G 6 - G 8 |
| 86 | SciEngines GmbH | B 9 |
| 87 | secunet Security Networks AG | G 15 |
| 88 | Secusmart | Z 10 |
| 89 | SELEX Communications GmbH | G 4 |
| 90 | Serco GmbH | G 11 |
| 91 | Software AG/IDS Scheer Consulting | K 2 |
| 92 | Sophos AG | F 6 |
| 93 | SQS Software Quality Systems AG | G 17 |
| 94 | SRH SAP Competence Center | B 1 |
| 95 | Steria Mummert Consulting AG | F 11 |
| 96 | Systematic | G 12 |
| 97 | systerra computer GmbH | Z 12 |
| 98 | takwak GmbH | B 7 |
| 99 | TASys GmbH | B 1 |
| 100 | TELEFUNKEN Radio Communication Systems GmbH & Co. KG | F 2 |
| 101 | Thales Deutschland | Z 6 |
| 102 | T-Systems International GmbH | F 4 |
| 103 | UWS Business Solutions GmbH | P 8 |
| 104 | VEGA Deutschland GmbH | F 3 |
| 105 | ZVEI – Fachverband Sicherheit | E 3 |

AFCEA Bonn e.V.

# 26. Fachausstellung

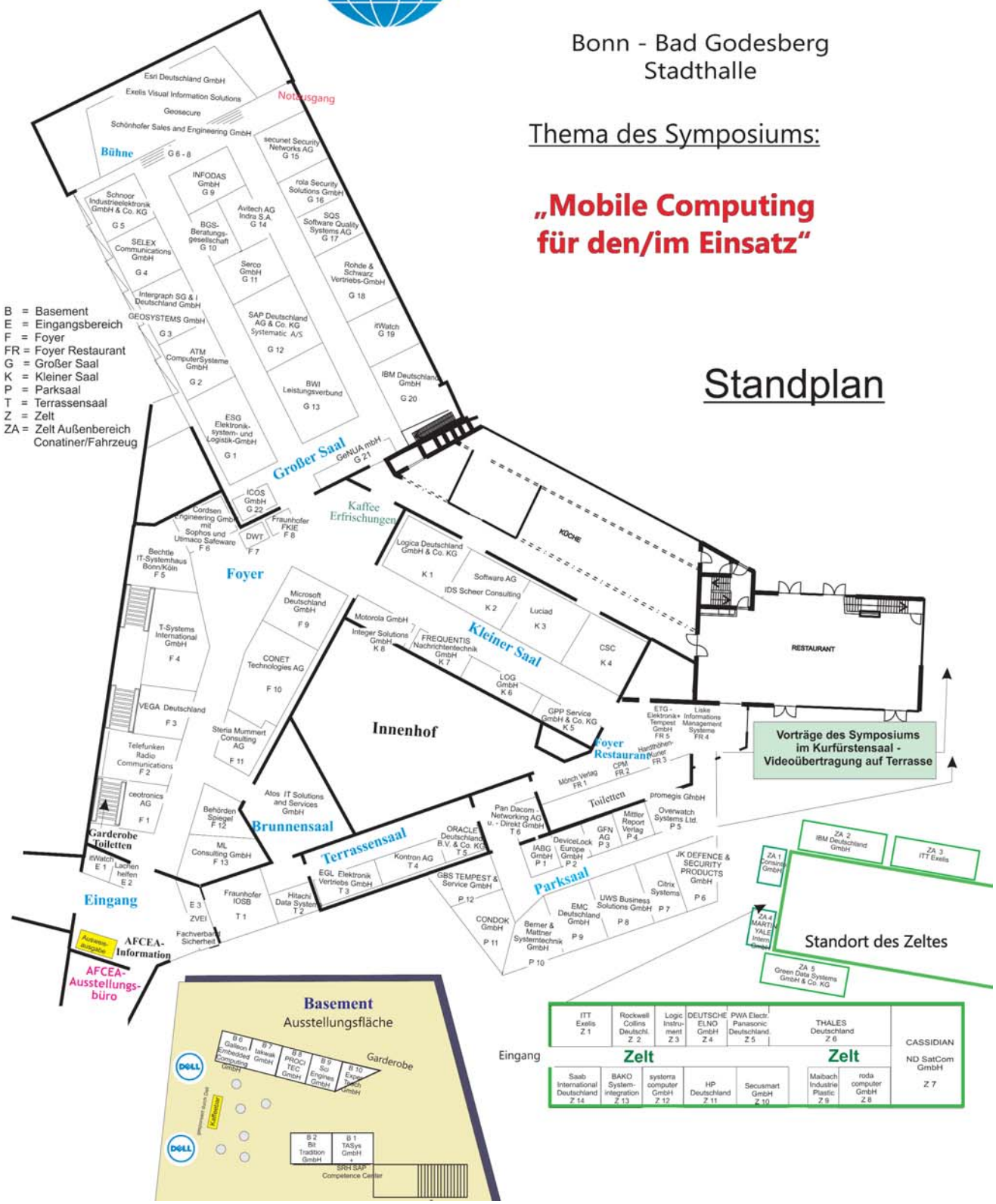
09. und 10. Mai 2012

Bonn - Bad Godesberg
Stadthalle

Thema des Symposiums:

**„Mobile Computing für den/im Einsatz"**

## Standplan



AFCEA Bonn e.V.

Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

# 26. AFCEA-Fachausstellung

## Informations- und Kommunikationstechnik

## Mobile Computing für den/im Einsatz

unter der Schirmherrschaft des Staatssekretärs in BMVg, Herrn Stéphane Beemelmans

**9. Mai 2012** **09:00 Uhr bis 18:00 Uhr Ausstellung · Vorträge im Kurfürstensaal**
**ab 18:00 Uhr Kölsch mit Musik**

**10:00 Uhr** **GenMaj Dipl.-Ing. Dipl.-Oek. Erich Staudacher,** Vorsitzender AFCEA Bonn e.V.
Begrüßung/Eröffnung der Fachausstellung

**10:10 Uhr** **Staatssekretär Stéphane Beemelmans,** BMVg
Grußwort

**10:30 Uhr** **MinDir Detlef Selhausen,** BMVg, AbtLtr Ausrüstung, IT, Nutzung
**„Neue Prozesse für Rüstung, Nutzung und IT“**

**14:00 Uhr** **Horst Flätgen,** Vizepräsident Bundesamt für Sicherheit in der Informationstechnik
**„Sicherheitsaspekte beim Mobile Computing“**

**10. Mai 2012** **09:00 Uhr bis 18:00 Uhr Ausstellung · Vorträge im Kurfürstensaal**

**10:00 Uhr** **BrigGen Dipl.-Ing. Klaus F. Veit,**
Vizepräsident Bundesamt für Informationsmanagement und Informationstechnik
**„Mobile ITK für den Einsatz der Bundeswehr – Teil der neuen IT-Strategie?“**

**14:00 Uhr** **BrigGen Dipl.-Kfm. Frank Leidenberger,** Deputy COS OPS KdoOpFüEinsKr
**„Erfahrungen aus dem Einsatz mit der mobilen ITK der Bundeswehr“**

**15:00 Uhr** **Lars Thomsen,** Zukunftsforscher
**„Mobile Computing auf dem Weg zu Smart Interaction – Szenarien und Prognosen 2012-2022“**

## 9./10. Mai 2012 · Stadthalle Bonn-Bad Godesberg

**Ausstellende Firmen**

**Eintritt zu Ausstellung und Vorträgen unentgeltlich**

Information: **AFCEA Bonn e.V.** · Borsigallee 2 · D-53125 Bonn · Internet: wwwafcea.de
Tel.: +49 228 9258252 · Fax: +49 228 9258253 · E-Mail: fachausstellung-afcea@gmx.com · buero@afcea.de

# AFCEA-Fachausstellung 2012

**Die folgenden Angaben wurden von den jeweiligen Anbietern geliefert.
Sie tragen für diese Eigenangaben und deren Wahrheitsgehalt die Verantwortung.**

## ATM ComputerSysteme GmbH — Stand: G 2

Advanced Technology for Military Forces
Die ATM ComputerSysteme mit Sitz in Konstanz am Bodensee ist ein global agierendes Technologieunternehmen für extrem robuste IT-Hard- und Softwarelösungen. Seit drei Jahrzehnten gehört die ATM zu den führenden Systemherstellern in der internationalen Sicherheits- und Verteidigungsindustrie und ist langjähriger Partner der Bundeswehr.
Am Stand G2 präsentieren wir Ihnen unsere IT-Solutions, die seit Jahren in den Bereichen Luft, Land und Wasser erfolgreich eingesetzt werden – national sowie international.
Auf Heeresebene zeigen wir Ihnen Systeme, die sowohl für den Einsatz in Rad- und Kettenfahrzeuge konzipiert sind als auch für den abgesessenen Betrieb in Form eines Micro-Kommunikationsservers.
Überdies stellen wir Ihnen Software vor, die einzelne Komponenten bis hin zur gesamten IT-Ausstattung des Fahrzeugs auf ihre Funktionsfähigkeit überprüft und somit maximale Qualität gewährleistet. Wir freuen uns auf ein persönliches Gespräch mit Ihnen.
Weitere Informationen zu uns und unserem Leistungsspektrum finden Sie unter www.atm-computer.de. Kontakt: ATM ComputerSysteme GmbH, Max-Stromeyer-Straße 116, D-78467 Konstanz, Jörg Sczesny, E-Mail: Joerg.sczesny@atm-computer.de, Tel.: 07531/808-4208, Mobil: 0171/3357778, Fax: 07531/808-4363, www.atm-computer.de

## Atos IT Solutions and Services GmbH — Stand: Brunnensaal

Atos ist ein internationaler Anbieter von IT-Dienstleistungen mit einem pro forma Jahresumsatz für 2010 von 8,6 Milliarden Euro und 74.000 Mitarbeitern in 42 Ländern. Atos ist weltweiter IT-Partner der Olympischen Spiele, zählt weltweit zu den zehn größten IT-Dienstleistern und ist im Markt für Managed Services der fünft grösste Anbieter.
Das Verteidigungsgeschäft ist weiterhin ein wichtiger Markt für Atos. Der seit langer Zeit bestehende enge und partnerschaftliche Dialog mit der Bundeswehr soll ausgebaut werden.
Atos präsentiert auf der AFCEA seine Lösungskompetenz bei Entwicklung und Betriebsunterstützung von einsatzfähigen IT-Plattformen (insbesondere Führungsinformationssystemen) und bietet Informationen zu Technologietrends.

## Avitech AG — Stand: G 14

Avitech AG ist seit über 10 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfoSysBw. Unsere Kompetenz liegt vor allem im Bereich der Aeronautischen und Hindernis Datenbanken, Luftfahrtkarten, Radarvideokarten sowie Flugplan- und Pilotenbriefingsysteme. Darüber hinaus bieten wir Meldungsvermittlungs- und Kommunikationssysteme sowie On-Line Data Interchange Lösungen zwischen Zivilen und Militärischen Flugsicherungskontrollstellen an. Die Avitech Produkte werden Bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an mehr als 100 Standorten genutzt. Dies beinhaltet auch die Schnittstelle zur zivilen Flugsicherung und zur Agentur Eurocontrol. Auf der diesjährigen AFCEA zeigen wir Produkte, die im FSInfoSysBw eingesetzt werden und die flächendeckende Datenversorgung mit Aeronautischen und Hinderdaten Daten sicher stellen wird.

## BAKO Systemintegration GmbH & Co. KG — Stand: Z 13

Konkrete Anwendungen fordern innovative und einsatzgerechte Lösungen.
BAKO Produkte und Dienste bereiten Ihre Anwendung basierend auf Ihrer gewohnten EDV- bzw. Funktionsumgebung auf die härtesten Bedingungen und Umwelteinflüsse weltweit vor und das an Land, auf See oder in der Luft. Unsere Erfahrung im Bereich mobiler und verlegbarer Systemlogistik unterstützt Sie, Ihren Einsatz bestmöglich durchzuführen.
Unsere Kundenbasis hat zwei Dinge gemein. Sie benötigen hochempfindliches Equipment in extremen Bedingungen. Und Sie haben entdeckt, dass BAKO die Antwort auf die Anforderungen, die diese Bedingungen darstellen, technologisch lösen kann.
**Neu 2012:** BAKOM, mobile Kommunikationslösungen von BAKO

## Bechtle IT-Systemhaus Bonn/Köln — Stand: F 5

Das Bechtle IT-Systemhaus Bonn/Köln gehört zur Bechtle AG, die mit rund 60 Standorten, 13 Lösungs- und Competence Centern sowie einem Umsatz von 2 Mrd. Euro zu einem der führenden Systemintegratoren in Deutschland zählt. Seinen mehr als 75.000 Kunden aus Industrie, öffentlichen Auftraggebern und Finanzmarkt bietet Bechtle herstellerneutral ein lückenloses Angebot rund um die IT-Infrastruktur. Unsere zentralen Lösungsthemen: Client Management, Server & Storage, Networking Solutions, Virtualisierung, IT-Security und Software.
Bechtle ist seit Jahren mit einem spezialisierten Geschäftsbereich Öffentliche Auftraggeber erfolgreich und bietet seinen Kunden in diesem Segment unter anderem den Einkauf ihrer IT über die maßgeschneiderte Online-Beschaffungsplattform bios® government.
Weiterführende Informationen – auch zum Rahmenvertrag IT-Plattform 2./3. Rechnerebene der Bundeswehr – erhalten Sie an unserem Stand F5.
Mehr zu Bechtle unter www.bechtle.com

## Behörden Spiegel – die Zeitung für den Öffentlichen Dienst — Stand: F 12

Der Behörden Spiegel begleitet die öffentliche Verwaltung sowie den Modernisierungsprozess bei der Bundesverwaltung, den Ländern und Kommunen und den Sicherheitskräften. Deutschlands größte und älteste Zeitschrift für den Staat, seine Beschäftigten, seinen Einkauf und seine Modernisierungsfähigkeit zeigt Monat für Monat in journalistisch kritischer und unabhängiger Berichterstattung Wege zu mehr Effizienz in der staatlichen Verwaltung auf.
Der Behörden Spiegel ist ein meinungsbildendes Medium und veranstaltet Kongresse, zu denen Sie weitere Informationen unter folgenden Quellen finden: www.effizienter-staat.de; www.e-nrw.info; www.european-police.eu; www.euro-defence.eu; www.disaster-management.eu; www.best-age-conference.com.
Abonnenten des Behörden Spiegel können zudem das digitale Angebot Behörden Spiegel Online kostenlos beziehen (E-Government Newsletter, Newsletter Netzwerk Sicherheit, Newsletter Defence, Newsletter Verwaltung kompakt und Newsletter geodata kompakt).
www.behoerdenspiegel.de

## Berner & Mattner Systemtechnik GmbH — Stand: P 10

**Sicherheits- und missionskritische Software effizient entwickeln**
Berner und Mattner ist als strategischer Entwicklungspartner spezialisiert auf Spezifikation, Entwicklung und Test von missions- und sicherheitskritischen elektronischen Steuersystemen und deren Software.
**Entwicklung kompletter Softwarepakete zum Festpreis**
- Embedded Systems, PC
- Komplexe HMIs

**Systeme für Wissenschaft und Raumfahrt**
- ECSS-Standards

**Normenkonforme Entwicklungsprozesse**
- DO-178B, IEC 61508
- MIL STD 882

**Technologie- und Prozessberatung**
- DOORS, SysML, UML
- SCADE, MATLAB/Simulink
- V-Modell-XT, CMMI
- CD&E

**Kontakt:**
Berner & Mattner Systemtechnik GmbH, Erwin-von-Kreibig-Str. 3, 80807 München, Tel.: +49 (0)89 608090-0, Fax: +49 (0)89 6098182, info@berner-mattner.com, www.berner-mattner.com

## BGS Beratungsgesellschaft Software Systemplanung AG — Stand: G 10

**Unser Erfolg ist der Erfolg unserer Kunden – seit 30 Jahren!!**
***Cloud Computing ist ...***
die innovative Form einer Infrastruktur und Dienste-Plattform auf Basis von IT-Standards (SOA / ITIL). Wir präsentieren eine **Secure Digital Cloud Anwendung am Beispiel einer mobilen Geodatenanwendung.** Denn im militärischen Kontext hält dieser Technologieansatz seinen Einzug. Lassen Sie sich die Sicht der BGS AG zu diesem Thema im militärischen Kontext vorstellen!
***Der ILS Cluster der ...***
BGS unterstützt die Bundeswehr, die wehrtechnische Industrie, nationale und multinationale Rüstungsagenturen sowie NATO-Partner bei der Optimierung der Lebenswegkosten von Systemen unter Anwendung der Methode „Logistic Support Analysis (LSA)“. Dieser Ansatz wurde mit dem Themennetzwerk METIS verknüpft. Als Tochterfirmen der DATAGROUP bieten BGS und Consinto das gesamte Spektrum der ILS aus einer Hand.
***Weitere Themen sind die ...***
Datenaufbereitung (Vorbereitung nach SASPF), Materialdaten in der Zusammenarbeit Bundeswehr und Industrie, logistische Führungssysteme und Sicherheitslösungen.
**Standorte:** Mainz, Köln/Bonn, Wilhelmshaven, Hamburg, München, Berlin, Wien
www.bgs-ag.de

## Bit Tradition GmbH — Stand: B 2

Bit Tradition GmbH Beltronic & Tradition Industrial Technology spezialisiert sich auf das Design, die Entwicklung und die Herstellung von robus-

ten mobilen Computern, Notebooks, Tabletts und LCD Displays, die unter höchst anspruchsvollen Umweltbedingungen arbeiten, ohne die ergonometrische Designarbeit einzuschränken.
Der Widerstand gegen Feuchtigkeit, Staub, Stoß und Vibrieren wird durch die komplizierte und einzigartige Technik der Elektronik sowie eine Einschließung aller Bit Tradition Produkte erreicht. Beruhend auf den Grundsätzen von ISO 9001 ruht der Erfolg der beweglichen Lösungen von Bit Tradition auf den Grundlagen des starken Designs und der Zuverlässigkeit.
We build computers for your office, wherever your office is.

## BWI Leistungsverbund — Stand: G 13

Die BWI ist der strategische Partner für die Informations- und Kommunikationstechnik (IuK) der Bundeswehr. Als Leistungsverbund mit den Gesellschaften BWI Informationstechnik, BWI Systeme und BWI Services modernisiert die BWI die nichtmilitärische IuK der Bundeswehr und übernimmt Management wie Betrieb der gesamten Infrastruktur von den Rechenzentren über WAN/LAN bis hin zur IT-Plattform und der Telekommunikation. Die BWI entwickelt und betreibt die Zentralen Dienste der Bundeswehr, sie ist zudem für die Pflege und Änderungen der Systeme in Nutzung (SinN) zuständig. Zentrale Serviceleistungen und ein bundesweiter Vor-Ort-Service garantieren der Bundeswehr einen flächendeckenden Service aus einer Hand. Bei der AFCEA-Fachausstellung 2012 informiert die BWI über den aktuellen Status im IT-Projekt HERKULES und über aktuelle Vorhaben im Bereich IT-Sicherheit.

## CASSIDIAN — Stand: Z 7

Cassidian, eine Division des EADS-Konzerns, ist einer der weltweit größten Anbieter globaler Sicherheitslösungen und -systeme, der zivile und militärische Kunden als Systemintegrator und Lieferant wertschöpfender Produkte und Dienstleistungen unterstützt. Hierzu zählen Flugsysteme (Flugzeuge und unbemannte Plattformen), boden- und schiffsgestützte sowie teilstreitkräfteübergreifende Systeme, Aufklärung und Überwachung, Cybersecurity, sichere Kommunikation, Testsysteme, Flugkörper, Dienstleistungen und Supportlösungen. Im Jahr 2010 erwirtschaftete Cassidian mit rund 28.000 Mitarbeitern einen Gesamtumsatz von € 5,9 Milliarden.
EADS ist ein weltweit führendes Unternehmen der Luft- und Raumfahrt, im Verteidigungsgeschäft und den dazugehörigen Dienstleistungen mit einem Umsatz von € 45,8 Mrd. im Jahr 2010 und über 121.000 Mitarbeitern. Zu EADS gehören die Divisionen Airbus, Astrium, Cassidian und Eurocopter.
**Cassidian,** Landshuterstrasse 26, D-85716 Unterschleißheim, www.cassidian.com

## CeoTronics AG — Stand: F 1

**Professionelle Kommunikationssysteme – Mehr als nur Headsets**
CeoTronics ist führender Systemanbieter von mobilen digitalen Audio-/Video-Funk-Netzen und -Endgeräten für den professionellen Einsatz. Mehr als 72.000 Hör-/Sprechsysteme zum Anschluss an die digitalen Tetra-/Tetrapol-Funkgeräte wurden bereits verkauft. Nutzen Sie dieses Know-how in der Kommunikationszubehör-Anpassung für die Umstellung vom Analog- zum Digitalfunk.
**Leistungsführerschaft im Premiumsegment**
CeoTronics hat sich seit 1985 in der Spitze der Qualitäts- und Leistungs-Pyramide positioniert und ist zuverlässiger Lieferant von Polizei, Bundespolizei, Militär, Nachrichtendiensten und der Industrie.
**CeoTronics AG,** Audio • Video • Data Communication, Adam-Opel-Str. 6, 63322 Rödermark, Germany, Tel.: +49 6074 8751-0, Fax: +49 6074 8751-676
verkauf@ceotronics.com
www.ceotronics.com

## Citrix Systems — Stand: P 7

Citrix Systems, Inc. (NASDAQ:CTXS) verändert die Art und Weise, wie Menschen, Unternehmen und die IT im Cloud-Zeitalter zusammenarbeiten. Mit führenden Cloud-, Collaboration-, Netzwerk- und Virtualisierungstechnologien unterstützt Citrix mobile Arbeitsmodelle und neue Cloud-Angebote. Mehr als 250.000 Unternehmen setzen weltweit auf Citrix und profitieren von flexiblen und jederzeit zugänglichen IT-Angeboten. Insgesamt 75 Prozent aller Internetnutzer kommen täglich direkt oder indirekt mit Citrix-Lösungen in Kontakt. Citrix pflegt Partnerschaften mit über 10.000 Firmen in 100 Ländern. Der jährliche Umsatz betrug 2,21 Milliarden US-Dollar in 2011. Weitere Informationen unter www.citrix.de

## CONDOK GmbH — Stand: P 11

Die CONDOK GmbH ist ein Systemhaus für Redaktionelle Logistik und bietet ihren Kunden ein breites Leistungsspektrum rund um das Thema Redaktionelle Logistik. Neben der Spezialisierung auf die Erstellung von IETD nach S1000D und S2000M werden vielfältige und umfangreiche Technische Dokumentationen, Bebilderte Teilekataloge, Technische Übersetzungen und Computer Based Trainings erstellt. Weitere Schwerpunkte der CONDOK sind die Bereiche der Produkt- und Betriebssicherheit sowie das Product Lifecycle Management gemäß den ILS-Prozessen der S3000L.
Mit mehr als 80 Mitarbeitern in Kiel, Hamburg und Koblenz unterstützt die CONDOK mit umfangreichen logistischen Dienstleistungen die Bundeswehr sowie eine große Anzahl von Unternehmen der Wehrtechnik und der zivilen Industrie.

## CONET Solutions GmbH & CONET Business Consultants GmbH — Stand: F 10

CONET ist seit mehr als 20 Jahren mit partnerschaftlicher Zusammenarbeit, hoher Dienstleistungsqualität und zielgerichteter IT-Unterstützung ein zuverlässiger Wegbegleiter der Bundeswehr.
Während die CONET Solutions GmbH zahlreiche SinN-Verfahren, Fach- und Führungsinformationssysteme, Kommunikationsarchitekturen und IT-Infrastrukturen betreut und weiterentwickelt, bündelt die CONET Business Consultants GmbH breites Beratungs- und Prozesswissen rund um die SAP-Implementierungen der Bundeswehr.
**CONET präsentiert an seiner Mobil-Nutz-Bar:**
"Mobiler Zugriff auf alle relevanten Daten" – Für die Handlungsfähigkeit im Einsatz ist der direkte Zugang zu Führungs- und Informationssystemen unerlässlich. CONET zeigt in Teststellungen "zum Anfassen", wie mobiler Zugriff auf die Business Intelligence von SASPF über moderne Touchpads schon heute funktioniert.
www.conet.de

## Consinto GmbH — Stand: ZA 1

Consinto steht für die Kernkompetenzen Consulting, Systemintegration und Operation. Als Full Service IT-Dienstleister mit mehr als 30 Jahren IT- und Branchenexpertise bieten wir für den Defence-Bereich unsere ILS Suite "consILSs", die die ASD Spezifikationen S1000D, S2000M und S3000L nahtlos mit Ihrem ERP- und PLM-Systemen verbindet.
Das AMOSS Service & Competence Center (ASCC) steht Ihnen mit Consinto-Experten bei allen Fragen rund um das Thema Integrated Logistics Support (ILS) jederzeit zur Verfügung.
Unsere Lösungen und Produkte, auch für die mobile Instandhaltung, sind "AMOSS 2000", die führende ASD S2000M konforme Softwarelösung für die Ersatzteillogistik mit spezieller Ausprägung "AMOSS light" für den Mittelstand und "L-BASE", die ML-STD-1388-2B konforme Softwarelösung für die Entwicklung einer logistischen Datenbasis und zur optimalen Unterstützung des LSA Prozesses.

## Cordsen Engineering GmbH — Stand: F6

**CORDSEN Engineering GmbH** entwickelt und fertigt eine breite Palette an militärisch gehärteten (Ruggedized) Workstations und Peripheriegeräten nach MIL-STD-810F / MIL-STD-461E, für mobilen und stationären Einsatz, sowie abstrahlsichere (TEMPEST) Produkte nach SDIP 27 Level A / COMSEC Zone 0, wie Workstations, Server, TFT-Displays ab 19", FO-Hubs, Drucker und Scanner.
Eine Reihe von Standardprodukten sind auf der NRPL gelistet, teilweise auch vom DCSSI für den nationalen (französischen) Einsatz zertifiziert.
Wir verfügen über zwei TEMPEST/EMV-Labore: Für Zulassungsmessungen nach SDIP 27 Level A/B/C, sowie für Zulassungsmessungen und KMVs nach dem Zonenmodell.
Als Dienstleistungen bieten wir u. a. Platform-Testing an.
Vorgestellt werden: TEMPEST und Rugged Produkte.
Cordsen Engineering GmbH, Am Klinggraben 1, D-63500 Seligenstadt, Tel.: 06182-9294-0, Fax: 06182-9294-45, www.cordsen.com

## CPM Communication Presse Marketing GmbH — Stand: FR 2

Die CPM Communication Presse Marketing GmbH wurde 1989 als Dienstleistungsgesellschaft für Publikationen, Tagungen und Studien in ausgewählten Marktsegmenten gegründet. In enger Zusammenarbeit mit vornehmlich militärischen Stellen und der Wirtschaft veranstaltet CPM nationale und internationale Fachtagungen und Kongresse (zum Teil mit begleitender Ausstellung).
Zu unseren Publikationen gehören:

- cpm-forum als themenorientierte wehrtechnische Dokumentationen mit jährlich ca. 8 Publikationen
- "Log.Net" als Forum über Logistik im öffentlichen Sektor
- Taschenbuch "Deutsche Bundeswehr – Folge 4 (2012)" als aktuelles Nachschlagewerk über die deutschen Streitkräfte
- Taschenbuch "Die Ausrüstung der Bundeswehr" – nächste Folge Ende 2012.
- Bundeswehr-Standortposter (DIN A1): Heer, Luftwaffe, Marine und Streitkräftebasis.

info@cpm-st-augustin.de

## CSC — Stand: K 4

CSC zählt mit rund 98.000 Mitarbeitern zu den weltweit führenden Dienstleistungsunternehmen im Bereich der Informationstechnologie (IT). Mit seinen maßgeschneiderten Lösungen und Services unterstützt CSC seit über 50 Jahren seine Kunden.
CSC beweist seine Expertise weltweit in zahlreichen Partnerschaften mit namhaften Kunden. Unter anderem betreibt das Unternehmen seit 1959 als Partner der NASA die sicherheitskritischen Systeme der Raumfahrtbehörde und ist seit über 20 Jahren vertrauensvoller Partner der Bundeswehr und wehrtechnischen Industrie.
Zu den CSC-Schwerpunktthemen im Verteidigungsumfeld gehören:

- Vernetze Operationsführung
- Transformation der Streitkräfte
- IT-Sicherheit

- Informationsmanagement
- Prozessorganisation
- Obsoleszensmanagement

CSC verfolgt den Markttrend und entwickelt entsprechend strategische Themen gemäß den Anforderungen seiner Kunden.
Auf der diesjährigen Fachausstellung präsentiert CSC Mobility-Lösungen aus dem militärischen und zivilen Umfeld. Die CSC-Vertreter stellen unter anderem ein Border-Control-Szenario unter Nutzung der Smart-Technologie (Devices) sowie Mobile-IT-Security-Lösungen vor. Zudem zeigen die Experten verschiedene Anwendungsszenarien anhand von Beispielapplikationen sowie Zubehör, das den Einsatz von Tablet-PCs oder Smartphones im Feld ermöglicht.
Weitere Informationen unter: http://www.csc.com/de/defense
**Kontaktdaten:** CSC, Valoisplatz 2, 26382 Wilhelmshaven, Telefon: 04421.9479.50

## Deutsche ELNO — Stand: Z 4

Zur AFCEA Ausstellung 2012 stellt die Fa. DEUTSCHE ELNO Netzwerkknoten und Audiozubehör für militärischen Einsatz vor.

- Kleinvermittlungen auf IP-Basis für Sprache (VoIP) und Daten
- Leicht, robust und wetterfest
- Kompatibel zu existierenden VoIP Strukturen (SIP + H.323)
- WLAN Systeme
- IP-Feldtelefone

mit Anschlußmöglichkeit von Netzen und Teilnehmern

- IP
- GSM
- Funk
- Eurocom
- ISDN
- Analog

Weiter Informationen finden Sie auf unserer Homepage www.deutsche-elno.de
**Kontakt:** DEUTSCHE ELNO GMBH, Schleissheimer Str. 90 a, 85748 Garching/München

## DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT) — Stand: F 7

Die DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. wirkt als neutrale Dialog- und Informationsplattform für Fragen der Sicherheits- und Verteidigungspolitik, der Wehr- und Sicherheitstechnik sowie der Verteidigungswirtschaft.
Die DWT und ihre Tochtergesellschaft, die Studiengesellschaft der DWT mbH (SGW) führen Entscheidungsträger aus Politik, Wirtschaft, Industrie und Dienstleistungssektor, Bundeswehr/Bundeswehrverwaltung, anderen Behörden/Organisationen mit Sicherheitsaufgaben (BOS) sowie Wissenschaft, Forschung und Öffentlichkeit zusammen, um Ausrüstungs- und Ausstattungsfragen der Bundeswehr unter Berücksichtigung nationaler und internationaler Interessen und Rahmenbedingungen zu erörtern.
In der Fläche wird die DWT in zahlreichen regional wirkenden Sektionen und in Wehrtechnischen Arbeitskreisen tätig.

## DeviceLock Europe GmbH — Stand: P 2

**DeviceLock®** Inc. ist seit 16 Jahren als internationaler DLP-Lösungsanbieter technologischer Spitzenreiter in der Datenflusskontrolle und unerlässlich in der IT-Sicherheit&Compliance. Mit der Vertriebszentrale in San Ramon (Kalifornien) und Niederlassungen in Deutschland, Italien, UK sowie Businesspartnern in über 40 Ländern, bietet DeviceLock eine globale Vertriebs-&Supportstruktur. Internationale Entwicklungslabore sind der Garant für eine innovative, vollumfängliche und gehärtete DLP-Solution mit Funktionsbereichen für die Kontrolle aller Ports und Kommunikationsprotokolle, der vollständigen Contentfilterung mit kurzen Implementationszeiten und geringen Anschaffungs-&Wartungskosten. Weltweit wird DeviceLock bei Militär&Polizei, im Finance&Public-Sektor und globalen Industrie-&Handelskonzernen in über 60.000 Organisationen auf mehr als 4 Millionen abgesicherten Clients erfolgreich eingesetzt.
www.devicelock.de, +49.2102.89211-0.

## EGL GmbH — Stand: T 3

Die Firma **EGL Elektronik Vertrieb GmbH** ist seit über 25 Jahren spezialisiert auf die Umrüstung von handelsüblichen Geräten gemäß dem Zonenmodel der BSI.
**Als Prüfgruppe F8 ist sie für die Zertifizierung von Zonengeräten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen.**
Eine Erweiterung um ein zweites BSI zugelassenes Labor wurde 2007 durchgeführt.
Somit ist die Firma EGL in der Lage, die Entwicklungszeiten und die Produktion kundenorientiert zu optimieren.
Für namhafte Firmen, Behörden, Bund und NATO ist die Firma **EGL Elektronik Vertrieb GmbH** der Partner für die Planung und Durchführung von Projekten im IT-Sicherheitsbereich.

## Elektronik + Tempest GmbH — Stand: FR 5

Elektronik + Tempest GmbH nutzt zwei vom BSI zugelassene Labore, um sich des Problems "Tempest" – also "kompromittierender Abstrahlung" anzunehmen. Hier ist es die Aufgabe der ETG, IT-Equipment entsprechend der Vorgaben des BSI, nämlich eine Abstrahlung zu vermeiden, umzubauen und per Vermessung den Nachweis zu führen, dass diese Maschinen den Schutzrichtlinien des BSI entsprechen. Die hohe Qualifikation unserer Ingenieure und Maschinen ermöglicht es der ETG beste Ergebnisse dabei zu erzielen und dem Kunden durch qualifizierte Beratung sowohl Kosten zu sparen, als auch "funktionierende" Lösungen für den Schutz von vertraulichen Daten anbieten zu können. Dieses Problem betrifft die Öffentliche Hand ebenso wie die Wirtschaft.
**Kontakt:** Gerhard Friedrichs, Bonhoefferstrasse 7, 49356 Diepholz, Tel.: 05441 6102, Mobil: 0151 2415 1898

## EMC Deutschland GmbH — Stand: P 9

**EMC Deutschland GmbH** unterstützt Firmen dabei, den maximalen Nutzen aus ihrem Informationsbestand zu ziehen – von der Entwicklung über den Aufbau bis hin zur Verwaltung von flexiblen, skalierbaren und sicheren Informationsinfrastrukturen. Zusammen mit Cisco und VMware treibt EMC im Rahmen der Virtual Computing Environment Coalition (VCE) die Entwicklung und Realisierung von durchgängig virtualisierten Unternehmens-informationsinfrastrukturen voran und bietet Lösungen zur Implementierung einer Private Cloud. Solche optimierten Infrastrukturen sind die Grundvoraussetzung, um Informationen intelligent wie effizient zu speichern, zu schützen und zu verwalten. Dadurch können die bei der Verwaltung von Informationen anfallenden potenziellen Risiken vermieden und Kosten reduziert werden.
**www.emc2.de**

## ESG Elektroniksystem- und Logistik-GmbH — Stand: G 1

Seit fast fünf Jahrzehnten entwickelt, integriert und betreibt die ESG IT- und Elektroniksysteme für Militär, Behörden und Industrie. Im Umfeld IT und Kommunikation bieten wir maßgeschneiderte Lösungen in den Bereichen Führungs- und Einsatzsysteme, Nachrichtengewinnung und Aufklärung, Geo-IT, Simulation und Training sowie Logistik. Mit unserer Expertise in den Themen Aufklärung, Führung, Wirkung und Unterstützung decken wir die gesamte Kette der vernetzten Operationsführung über alle Befehlsebenen ab. Mit unseren Logistikleistungen sorgen wir für eine hohe Verfügbarkeit und Wirtschaftlichkeit dieser Systeme im Einsatz.
Auf der diesjährigen AFCEA präsentieren wir eine Auswahl unserer mobilen IT-Lösungen für den Einsatz.
**Kontakt:** ESG Elektroniksystem- und Logistik-GmbH, Livry-Gargan-Str. 6, 82256 Fürstenfeldbruck, Homepage: www.esg.de, Ansprechpartner Alexandra Spann, E-Mail: itk@esg.de, Tel.: 089/9216-0, Fax: 089/9216-2631

## Esri Deutschland GmbH — Stand: G 6 – G 8

Die Esri Deutschland GmbH mit Sitz in Kranzberg bei München ist eine Firma der Esri Deutschland Group GmbH und vertreibt als Distributor und Systemhaus die Produkte von Esri Inc. exklusiv über elf Standorte in Deutschland und der Schweiz. Esri unterstützt die Anwender mit einem breit gefächerten Schulungs-, Support- und Consultingangebot und dem gesamten Erfahrungsreichtum von mehr als 450 Mitarbeitern der Esri Unternehmensgruppe.
Für das Marktsegment BOS hat Esri Deutschland GmbH eine eigene Niederlassung in Bonn aufgebaut, die den BOS Bereich in Deutschland und der Schweiz betreut.
In der Esri Unternehmensgruppe ergänzt seit Januar 2012 die Geosecure Informatik GmbH am Standort Bonn das Leistungsspektrum durch die Fokussierung einer Professional Services Abteilung speziell für den BOS Bereich mit eigenen Lösungsbausteinen.

## EXELIS Visual Information Solutions — Stand: G 6 – G 8

Besuchen Sie den Gemeinschaftsstand von EXELIS VIS und ESRI und erfahren sie mehr über die brandneue ENVI Version 5.0, die hochperformante Lösung für Rasterbild- und Geodatenanalyse. Militärische Anwender weltweit extrahieren damit wertvolle Informationen aus ihren Satelliten- und Luftbildern. Die neuen ENVI-Funktionalitäten, welche von EXELIS VIS vorgestellt werden, integrieren automatisierte Bildanalysen einfach und schnell in den gesamten GIS-Arbeitsablauf. Sehen Sie bei Live-Demonstrationen, wie Sie aus ihrer ArcToolbox direkt auf die Bildanalyse-Werkzeuge von ENVI zugreifen können. Die Plattformunabhängigkeit und offene Architektur stellen höchste Effizienz und Interoperabilität sicher. Dadurch werden wichtige Bereiche der Verteidigung und Sicherheit mit einem durchgängigen Lösungskonzept verbunden: Mehr unter: www.exelisvis.com

## ExperTeach GmbH — Stand: B 10

Die ExperTeach GmbH ist einer der führenden IT-Weiterbildungsanbieter mit Fokus auf die Bereiche Telekommunikation und High-End-Networking. Hauptsitz ist Dietzenbach bei Frankfurt. Im Verbund mit leistungsstarken Partnern bieten wir Kurse an 15 Standorten an. Das Trainings-Portfolio umfasst die deutschsprachige Eigenproduktlinie ExperTeach Networking sowie Original-Kurse von etwa 30 namhaften Herstellern. Selbstverständlich unterstützen wir Sie bei allen einschlägigen Zertifizierungen.
Neben dem offen angebotenen Kursportfolio setzen wir maßgeschneiderte Weiterbildungsprojekte um. Durch unsere Kompetenz in den Bereichen E-Learning, Netzwerk-Consulting, Technische Dokumentation und Übersetzung können wir dabei nahezu jeden Sonderwunsch

erfüllen. Vom Blended-Learning-Konzept bis zur mehrsprachigen Weiterbildungsmaßnahme – die individuelle Lösung ist unsere besondere Stärke.

## Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE — Stand: F 8

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE entwickelt Systeme für den Bereich der Sicherheit und Verteidigung, mit denen Informationen gewonnen, übertragen, analysiert und verarbeitet werden können. Die Ergebnisse können als Grundlage für Entscheidungsprozesse genutzt werden. Das Vorgehen in den einzelnen Projekten spiegelt dabei stets ein "Denken vom Einsatz her" wider. Ein Beispiel ist das im Einsatz befindliche "Einsatzmeldewesen der Bundeswehr". Hierüber werden täglich Informationen ausgetauscht und Meldungen, Weisungen und Anträge von Nutzern mit vielfältigen Kompetenzen über Führungsebenen hinweg kommuniziert. Die Prozesse orientieren sich an der unterschiedlichen Verantwortung der beteiligten Dienststellen. Der aktuelle Stand wird im Rahmen der Ausstellung präsentiert.

## Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB — Stand: T 1

Das Fraunhofer IOSB mit seinen Hauptstandorten in Karlsruhe und Ettlingen verfügt über ein einzigartiges, durchgängiges Kompetenzspektrum von der Objekt- und Atmosphärenphysik über die Optik, die Sensorphysik, die Bild- und Signalauswertung bis hin zur Informations- und Wissensverarbeitung sowie der Mensch-Maschine-Systemtechnik. Ein Schwerpunkt für wehrtechnische Anwendungen liegt in der Auswertung und Fusion vernetzter, abbildender Sensoren wie z.B. Infrarot-, Laser-, Radar- oder von Videosequenzen. Nachrichtengewinnung und Aufklärung als Teil einer vernetzten Operationsführung ist dabei ein besonders wichtiges Anwendungsfeld. Weitere Arbeitsgebiete am IOSB sind z.B. Bauwerkserfassung, multisensorielle Ferndiagnose, Fahrzeugführungsassistenz und Warnsensorik.
**Ansprechpartner:** Dr. Jürgen Geisler, Fraunhoferstraße 1, 76131 Karlsruhe, Tel.: +49 (0) 721 6091 262, verteidigung@iosb.fraunhofer.de
**Kontakt:** Dipl.-Ing.Sibylle Wirth, Leiterin Presse und Öffentlichkeitsarbeit, Fraunhoferstr. 1, D-76131 Karlsruhe, sibylle.wirth@iosb.fraunhofer.de, Tel.: 0721 6091 300, Mobil: 0173 640 58 06, Fax: 0721 6091 413, www.iosb.fraunhofer.de

## FREQUENTIS Nachrichtentechnik GmbH — Stand: K 7

**Frequentis** bietet individuelle, hochverfügbare Lösungen für Defence & Security in den streitkräftegemeinsamen Marktsegmenten Militärische Flugsicherung, Einsatz- und Operationsführung, Taktische Netzwerke, Überwachung und Aufklärung sowie Nationale Sicherheit und Grenzschutz. Zum umfangreichen Lösungs- und Produktportfolio gehören Kommunikations- und Informationssysteme sowie integrierte Gefechtsstandslösungen. Hohe Verlässlichkeit, innovative Mensch-Maschine-Schnittstellen und zukunftsweisende Technologien sichern Kundenzufriedenheit und Wettbewerbsfähigkeit, wobei die verlässliche Partnerschaft über den gesamten Produktlebensweg aufrechterhalten wird. Frequentis verfügt über vielfältige und langjährige internationale Kundenbeziehungen, insbesondere zur Deutschen Bundeswehr sowie zu NATO- und EU-Staaten. Speziell für die Vernetzte Operationsführung wird eine "Network Enabled Service Suite" als skalierbares Lösungskonzept angeboten. Verschiedene Dienste aus dem eigenen Portfolio, aus Legacy-Systemen oder Commercial-of-the-Shelf-Produkten können damit zu bedarfsgerechten, kosteneffizienten und leistungsfähigen Lösungen kombiniert werden.

## Galleon Embedded Computing GmbH — Stand: B 6

Galleon Embedded Computing liefert integrierte High Performance Datenrecorder und FPGA basierende Datenerfassungssysteme für den Einsatz in Applikationen wie UAVs oder militärischen Fahrzeugen. Der Rugged Recorder XSR ist nur 15 x 17 x 10 cm groß, kann als Gigabit Ethernet, als serial FPDP Recorder oder als Rugged Server konfiguriert werden. Er bietet einen GPS Empfänger und Verschlüsselung. Die SSD Speicherkapazität der Wechselspeichereinheit kann bis zu 4 TB betragen.
Der rugged Mission Computer XSR ist ausgestattet mit einem i7 Prozessor. Über XMC Schnittstellen können analoge Frontends (125 MHz – 3,6 GHz) mit optionalen Downconvertern integriert werden.
Wir bieten Langzeitverfügbarket, Life-Cycle- und Obsolescence Management.
**Kontakt:** Stephan Troesch, Geschäftsführer, Galleon Embedded Computing GmbH, Ganghoferstr. 66e, D-80339 München, Tel.: +49 89 4520508-20, Fax: +49 89 4520508-99, Mobile: +49 151 55788301, stroesch@galleonembedded.de, www.galleonembedded.de

## GBS TEMPEST & Service GmbH — Stand: P 12

Die GBS GmbH, mit Sitz in Diepholz, ist ein offiziell anerkanntes und vom Bundesamt für Sicherheit in der Informationstechnik zertifiziertes Unternehmen. Für das Geschäftsfeld TEMPEST, verfügt die GBS GmbH über zwei firmeneigene, BSI geprüfte Tempestlabore. Neben der Berechtigung zur Durchführung von Zonenkurzmessungen ist die GBS GmbH auch offiziell eine vom BSI anerkannte Prüfstelle für Zulassungsmessungen nach SDIP 27 Level A, Level B und Level C (International) und dem Zonenmodell (National).
**Adresse:** von-Braun-Straße 6, D-49356 Diepholz, Tel.: +49 5441 9758-100, Fax: +49 5441 9758-129, Homepage: www.gbs-tempest.de, E-Mail: info@gbs-tempest.de

## GeNUA mbH — Stand: G 21

**GeNUA sorgt für sichere VS-Datenkommunikation**
Für die Datenkommunikation bis zur Stufe VS-NfD bietet GeNUA zwei hochsichere Lösungen: die Firewall & VPN-Appliance GeNUScreen und das Mobile Security Device GeNUCard – beide mit VS-NfD-Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI). GeNUScreen ist für den stationären Einsatz ausgelegt und umfasst ein VPN-Gateway zur zuverlässigen Verschlüsselung sensibler Daten sowie eine Firewall zur Kontrolle von Netzwerk-Schnittstellen. Die kompakte GeNUCard wird dagegen mit dem Laptop verbunden und ermöglicht mobilen Anwendern oder Mitarbeitern im Home Office den verschlüsselten Austausch von VS-NfD-Daten. Beide Systeme werden über eine zentrale Management Station administriert und können komfortabel in großen Stückzahlen eingesetzt werden. Darüber hinaus ermöglichen wir mit Hochsicherheits-Gateways den Datenaustausch an Rot-Schwarz-Schnittstellen.
GeNUA mbH, Domagkstraße 7, 85551 Kirchheim bei München, Tel.: +49 89 991950-0, www.genua.de

## Geosecure Informatik GmbH — Stand: G 6 – G 8

Geosecure ist ein 100prozentiges Tochterunternehmen der Esri Deutschland Group und als Anbieter von GIS Lösungen im BOS Umfeld tätig. Die Fokussierung auf militärische und BOS relevante Anforderungen und das tiefgehende Verständnis der auftretenden Fragestellungen garantiert die höchstmögliche Lösungskompetenz auf diesem sensiblen und anspruchsvollen Sektor. Geosecure Lösungen basieren auf der bewährten Esri ArcGIS und ArcGIS Server Technologie, ergänzt durch eigene Lösungsbausteine.

## GEOSYSTEMS GmbH — Stand: G 3

GEOSYSTEMS ist Lösungsanbieter und Softwarevertriebsunternehmen mit herausragender Kompetenz und mehr als 20 Jahren Erfahrung im Geoinformations-Workflow für sicherheitsrelevante Aufgaben. Als Partner von Intergraph® bietet GEOSYSTEMS die ERDAS® Softwareprodukte und maßgeschneiderte Systeme. ERDAS wird weltweit im Defence-Bereich erfolgreich für die Auswertung hochauflösender Luft- und Satellitenbilddaten, wie auch UAV-Daten eingesetzt. Objekterkennung, Veränderungsnachweise, Höhenmodellgenerierung, Gebäude-Erkennung, Kartenerstellung: Diese Aufgaben werden mit ERDAS Produkten kostensparend gelöst. Geoprocessing im Web eröffnet neue Möglichkeiten für eine rasche, flexible Datenverarbeitung. Unsere kompletten Geodatenmanagementsysteme berücksichtigen alle spezifischen Sicherheits- und Vertraulichkeitsrichtlinien. Die Datenverteilung erfolgt über den derzeit schnellsten Bilddatenserver.
Weitere Informationen finden Sie unter: www.geosystems.de

## GFN AG — Stand: P 3

Die GFN AG ist ein bundesweit tätiges Bildungsunternehmen – AZWV zertifizierter Microsoft Gold Partner, Novell Platinum Partner sowie zertifizierter Partner des Linux Professional Institute. Am Firmensitz in Heidelberg und in den Niederlassungen Hamburg, Berlin, Köln, Koblenz, Mannheim, Darmstadt, Stuttgart, Nürnberg, München, Donaueschingen und Kassel bietet das Unternehmen hochwertige Trainings und Zertifizierungen an.
Die GFN AG eröffnet Menschen durch qualifizierte Weiterbildungen neue Zukunftsperspektiven. Durch die optimale Kombination verschiedener Lernmethoden und -inhalte entstehen innovative Konzepte. Die Spezialisten der GFN AG unterstützen Firmenkunden, Quereinsteiger und Arbeitssuchende in allen Fragen der Förderung.
Näheres zur GFN AG und ihrem Weiterbildungsangebot erfahren Sie unter www.gfn.de.

## GPP Service GmbH & Co. KG — Stand: K 5

**Projekte gemeinsam zum Erfolg führen**
Sie haben ein Ziel. Wir helfen Ihnen dabei es zu erreichen. Schnell, sicher, ohne Umwege.
Seit über 30 Jahren sind wir als kompetente und engagierte Spezialisten für IT-Dienstleistungen im militärischen und privatwirtschaftlichen Bereich etabliert.
Unsere Kompetenzen liegen besonders in den Bereichen

- Systemtechnische Begleitung,
- Independent Validation and Verification (IV&V),
- V-Modell,
- GPP Web-Services zur Projektabwicklung,
- IT-Sicherheit,
- Projektbezogene IT-Sicherheitskonzepte sowie
- Prozess-Simulation.

Besuchen Sie uns im Internet unter www.gpp-service.de oder treffen Sie uns persönlich auf der AFCEA Fachausstellung – wir freuen uns auf Sie!
**GPP Service GmbH & Co. KG**, Kolpingring 18 a, 82041 Unterhaching, Fax: 089/61304-111, www.gpp-service.de, Dr. Stefan Krempl, S.Krempl@gpp-service.de, Tel.: +49 89/61304-209, Steffi Rudel, S.Rudel@gpp-service.de, Tel. +49 89/61304-228

## Green Data Systems GmbH & Co. KG — Stand: ZA 5

**Green Data Systems (GDS)** ist spezialisiert auf Hitachi Converged Computing und Container-Rechenzentren.
Ein Schwerpunkt beim Converged Computing ist die Virtualisierung von SAP-Umgebungen. Neben den Komplettlösungen bietet GDS die Möglichkeit, die SAP-Infrastruktur inklusive Services zu kaufen oder pro SAP-User pro Monat abzurechnen.
Die Container-Rechenzentren sind Komplettlösungen, die bis zur schlüsselfertigen Inbetriebnahme inklusive TÜV-Abnahme eine effektive, flexible RZ-Alternative darstellen. Sie verfügen über die relevanten RZ-Standards und Sicherheitsanforderungen und sind ausgestattet mit Kühlung, Zugangskontrolle, Feuerlöscheinrichtungen, USV, Notstromaggregaten sowie Standard 19-Zoll Racks. Auch für die Container-Lösungen bietet GDS vom klassischen Kauf bis hin zu Nutzungsmodellen mit monatlicher Abrechnung flexible und attraktive Kauf-Alternativen an. **www.greendatasystems.de**

## Hardthöhenkurier — Stand: FR 3

Der **Hardthöhenkurier** ist ein periodisch erscheinendes Magazin, das sich seit 1984 mit aktueller Berichterstattung nicht nur an die Soldaten der Bundeswehr wendet, sondern auch an die Mitglieder des Deutschen Bundestages, die politische und militärische Führung des Bundesministeriums der Verteidigung und die Entscheider der Beschaffungsebene. Der **Hardthöhenkurier** versteht sich als **Bindeglied der Bundeswehr zur wehrtechnischen Industrie und Wirtschaft.**

**Der Hardthöhenkurier informiert regelmäßig über:**

- Sicherheitspolitische Rahmenbedingungen
- Die Einsätze der Bundeswehr
- Aktuelle Vorhaben der Streitkräfte
- Neuerungen in der Wehrtechnik
- Aktuelles aus der Rüstungsindustrie
- Aktuelles aus den Dienststellen der Bundeswehr
- Aus- und Weiterbildung von Offizieren / Unteroffizieren und deren Einsatz in den Streitkräften.
- u.v.m.

Weitere Informationen auf **www.hardthoehenkurier.de.**

## Hitachi Data Systems GmbH — Stand: T 2

Hitachi Data Systems bietet branchenweit führende Informationstechnologien, Services und Lösungen für einen überzeugenden Return on Invest (ROI) sowie Return on Assets (ROA) und verschafft Unternehmen somit einen nachweisbaren wirtschaftlichen Mehrwert. Der Vision einer virtualisierten, automatisierten, cloud-fähigen und nachhaltigen IT folgend, senken die Lösungen von Hitachi Data Systems die IT-Kosten und erhöhen gleichzeitig die Agilität. Mehr als 5.300 Mitarbeiter weltweit in über 100 Ländern helfen dabei, diese Vision Wirklichkeit werden zu lassen. Die größten Unternehmen der Welt, darunter mehr als 70 Prozent der Fortune-100-Unternehmen sowie über 80 Prozent der Fortune-Global-100-Unternehmen, vertrauen auf die Produkte, Services und Lösungen von Hitachi Data Systems. Daten bewegen unsere Welt – Informationen sind die neue Währung. Für weitere Informationen besuchen Sie www.hds.de.

## HP Deutschland — Stand: Z 11

Seit fast 70 Jahren unterstützt HP Menschen, Unternehmen und Organisationen weltweit bei der sinnvollen Nutzung von Technologie. Dazu entwickelt HP neue Konzepte und Ideen, um intuitiv bedienbare Produkte und zuverlässige Services bereitzustellen. Wir möchten, dass Menschen weniger Zeit brauchen, um sich mit Technologie zu befassen, und mehr Zeit haben, um sich mit den Dingen zu beschäftigen, die ihnen wichtig sind.
**Ansprechpartner:** Tobias Bahlinger, tobias.bahlinger@hp.com, Tel.: 0151 1475 1666

## IABG — Stand: P 1

Als führendes europäisches Technologieunternehmen mit den Automotive, InfoKom, Verkehr, Umwelt & Energietechnik, Luftfahrt, Raumfahrt und Verteidigung & Sicherheit konzipieren und entwickeln wir sichere, moderne und innovative Netz- und Systemarchitekturen, realisieren Prototypen und begleiten die Einführung bis zur Abnahme.
Unsere Lösung Referenzumgebung Dienste (RuDi) erweitert die Serviceorientierten Architekturen um einen hochmodernen Anteil und schafft die Voraussetzung für den Einsatz dienstorientierter Architekturen in taktischen Bereichen der Bundeswehr.
Auf dem Gebiet hochmobiler, sicherer Netze gestattet unsere HiMoNN-Lösung die Nutzung breitbandiger Anwendungen (Sprache, Daten, Video) sowie die Anbindung an eine vorhandene Netzinfrastruktur, z.B. über unseren Teleport (SatCom-Services) .
Wir unterstützen Sie in allen Bereichen der IT-Sicherheit bei der Etablierung eines effektiven Risiko- und Sicherheitsmanagements.
**IABG mbH,** Einsteinstrasse 20, 85521 Ottobrunn, Tel.: +49 89 6088-2030, Fax: +49 89 6088-4000, info@iabg.de, www.iabg.de

## IBM Deutschland GmbH — Stand: G 20, ZA 2

IBM ist einer der weltweit größten Anbieter von Informationstechnologie und B2B-Lösungen. IBM und Partner bieten den Kunden eine komplette Produktpalette an innovativer Informationstechnologie an: von der Hardware, Software über Dienstleistungen, inklusive Beratungsleistungen, und komplexe Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten sowie Finanzierungskonzepten. Mit hohen Investitionen in die Forschung will IBM auch weiterhin Schrittmacher in der Entwicklung neuer Technologien und Lösungen bleiben.
Mit ihrer diesjährigen Kernbotschaft "Smarter Defense – Mobile Führungsfähigkeit mit durchgängig integrierten Lösungen erreichen" adressiert IBM die besonderen Anforderungen an die Führungsfähigkeit im mobilen Umfeld.
"Mobile Computing" ist gerade im sensitiven Umfeld von Streitkräften weit mehr als nur die Einführung innovativer, mobiler Endgeräte. Vielmehr basiert die "Mobile Führungsfähigkeit" auf sicheren, durchgängigen und integrierten technischen Lösungen, von der stationären Plattform über verlegbare Anteile bis hin zum mobilen Endgerät und bietet somit eine qualitativ neue Stufe der Führungsfähigkeit.
www.ibm.de
**Kontakt:** IBM Deutschland GmbH, Gorch-Fock-Str. 4, D-53229 Bonn, Oliver Seifried, E-Mail: Oliver.Seifried@de.ibm.com, Tel.: +49-7034-15-1931, Mobile: +49-151-16704848

## ICOS GmbH — Stand: G 22

Als konzernunabhängiger Hersteller von maßgeschneiderten Systemlösungen für industrielle und wehrtechnische Anwendungen beliefert ICOS seit 1992 die wehrtechnischen Systemhäuser mit gehärteten Kommunikations-Rechnern, Servern, Laptops, hochauflösende Displays (HEL) und IT-Komponenten sowie Software-Lösungen, speziell Visualisierungs- und Kommunikationsanwendungen.
Unter Einsatz handelsüblicher IT-Produkte (COTS-Produkte) ergänzt mit spezifischen mechanischen und elektronischen Eigenentwicklungen in Form von Mikrokontroller-basierenden intelligenten Überwachungs- und Steuereinheiten ist ICOS in der Lage, eine den projektspezifischen Anforderungen entsprechende Systemlösung auch für Comsec-Zone 1 Anwendungen zu realisieren.
Die Systeme werden zum Beispiel in der kettengetriebenen Panzerhaubitze PzH2000, im TPZ Fuchs ABC, in U-Booten und LKW-Sheltern erfolgreich eingesetzt, ganz aktuell bei FüInfoSys-Heer und FüInfoSys-Heer-HEL.

## Indra S.A. — Stand: G 14

Indra S.A. ist der führende Spanische Elektronik Konzern, der sich in den letzten 30 Jahren zu einer multinationalen weltweit operierenden Verteidigungs- und Sicherheitstechnologiefirma entwickelt hat. In Deutschland wird Indra durch sein Tochterfirma Avitech AG, Friedrichshafen, vertreten.
Indra nutzt ihre eigene Forschung und Entwicklung, um weltweit eine führende Rolle im Markt der hochentwickelten elektronischen Systeme aufzubauen. Die Grundlagen dafür bilden 31,000 hochqualifizierte Mitarbeiter in über 110 Ländern.
Im Jahr 2010 lag der Umsatz bei ca. EUR 2,575 Mrd, ein Drittel davon im internationalen Markt. Die Indra Verteidigungs- und Sicherheitslösungen werden u.a. in Deutschland, Frankreich, Finnland, Portugal, den USA, Neuseeland, Indien und Brasilien verwendet.
Die Angebotspalette erstreckt sich dabei von Radaren, über elektronische Kampfführung und Aufklärung, Selbstschutz, Kommunikation, Führungssystem, Überwachung, Simulation bis zum Weltraumsegment.

## INFODAS GmbH — Stand: G 9

**INFODAS** ist seit 1974 als unabhängiges und herstellerneutrales Software- und Beratungsunternehmen ein verlässlicher Partner der Bw. Dieses Wissen ist in unsere **langjährige Beratungs- und Lösungskompetenz** in den Bereichen **IT-Sicherheit** sowie **Informations- und Kommunikationssysteme** eingeflossen. Kernkompetenzen sind:

- SDoT®/RSGate®, sicherer, kontrollierter Informationstransfer an Rot-/Schwarz-Übergängen
- SDoT® Labelling Service, zulassungsfähige Kennzeichnung und Auswertung von Security Labeln
- Offline Systemprüfung, die Prüfsoftware zur Erkennung fehlerhafter Baugruppen in komplexen Umgebungen wie FüInfoSys, Fahrzeugen usw.
- SAVe®, die IT-Sicherheitsdatenbank mit integrierten Sicherheitsvorgaben ZDv 54/100
- Informationssicherheitsberatung und Erstellung von Sicherheitskonzepten
- Planung/Realisierung komplexer Informationssysteme, Netzwerke und IT-Plattformen
- Projekt-, Anforderungs-, Nutzungs-, Konfigurations- und Qualitätsmanagement sowie Beratungsleistungen und Analysen im Bereich NATO CCIS
- Hardware/Software-Integration in Kabinen, Fahrzeugen und TULBs.

www.infodas.de – vertrieb@infodas.de
Kontakt: INFODAS GmbH, Rhonestraße 2, D-50765 Köln, Thorsten Ecke, t.ecke@infodas.de, Tel.: 0221 709 12-35, Mobil: 0151 16 22 09 54, Fax: 0221 709 12-86, www.infodas.de

## Integer Solutions GmbH — Stand: K 8

Die Integer Solutions GmbH ist Anbieter von IT-Produkten und Lösungen rund um das Thema Identifikation und Automatisierung. Dies beinhaltet Beratung, Programmierung, Integration und Service aus einer Hand.
Das Produktportfolio umfasst u.a.:

- Mobile Datenerfassung lokal oder im Außendienst
- Lagerverwaltungssysteme
- SAP Anbindungen
- Individuell angepasste Softwarelösungen
- Kennzeichnungs- und Barcodelösungen
- Datenerfassungstechnologien
- RFID Technologien
- Service und Support

Integer Solutions unterstützt dabei alle gängigen Softwareumgebungen wie SAP, AS/400,

Brain, Baan, Unix und Windows in den unterschiedlichsten Branchen.
Das breit gefächerte Partnernetzwerk und die langjährige Erfahrung bilden eine solide Basis für die Lösungen und Dienstleistungen.
**Anschrift:** Integer Solutions GmbH, Küchlerstrasse 1, 61231 Bad Nauheim, www.integer-solutions.com
**Ansprechpartner:** Herr Olav Reimers, Tel.: +49 6032 34956-0, Fax +49 6032 34956-77, E-Mail: info@integer-solutions.com.

## Intergraph SG&I Deutschland GmbH — Stand: G 3

Intergraph ist einer der führenden internationalen Anbieter raumbezogener Lösungen für die öffentliche Verwaltung, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Verteidigung und Nachrichtenwesen, Transport/Verkehr, Photogrammetrie und Fernerkundung, Versorgungs- und Entsorgungswirtschaft sowie Telekommunikation. ERDAS, jetzt ein Teil von Intergraph SG&I, bietet integrierte Produkte für Photogrammetrie & Fernerkundung sowie GIS-Daten-Management und -Verteilung. Unsere Kunden vertrauen auf Intergraphs Lösungen zur Aufbereitung umfangreicher, komplexer Datenmengen in Form aussagekräftiger, visueller Darstellungen. Damit lassen sich zeit- und situationsgerecht wichtige Entscheidungen treffen, von denen tagtäglich das Wohlbefinden und die Sicherheit von Millionen von Menschen rund um den Globus abhängig sind.
Weitere Informationen finden Sie unter: www.intergraph.de

## ITT Exelis — Stand: Z 1, ZA 3

ITT Exelis ist ein neues Unternehmen, das 2011 aus der Teilung des ITT Konzern in drei unabhängige börsennotierte Unternehmen hervorging und mit mehr als 20.000 Beschäftigten, im Jahr 2010 einen Umsatz von 5,9 Mrd. USD erwirtschaftet hat. ITT Exelis liefert integrierte Lösungen für Bereiche der militärischen und inneren Sicherheit weltweit.
Das Unternehmen hat vier Bereiche mit folgenden Schwerpunkten:
**Electronik Systeme:** Taktische Funksysteme, Radar, Elektronischer Kampf, Secure Smartphone
**Geospatiale Systeme:** Payload für Satelliten, Sensoren für UAV und Helikopter, militärisches GPS sowie Nachtsichtausrüstung
**Informationssysteme:** Flugsicherungssysteme, Cyber Warfare, Lösungen zur militärischen und zivilen Nutzung des Weltraums
**Missions Systeme:** Komplettes Dienstleistungsangebot für den Betrieb, Wartung und Vorortunterstützung militärischer Anlagen im Einsatzland und Heimatland

## itWatch — Stand: E1, G 19

**itWatch** steht für innovative IT-Sicherheit "made in Germany".Endgeräte Sicherheit, Data-Loss-Prevention, Verschlüsselung und Kostenreduktion des IT-Betriebes stehen im Fokus.
Im Public Sector bieten die patentierten, **itWatch** Sicherheitslösungen durch ihre weltweiten Alleinstellungsmerkmale viele Vorteile – gerade in der inneren Sicherheit. Hohe Anforderungen von Nachrichtendienst, Militär (Einsatz bis GEHEIM und NATO-restricted) und Polizei werden ebenso erfüllt , wie solche von Standard-Büro-Arbeitsplätzen und Spezialprojekten. Mit großen Installationen weit über 100.000 Lizenzen, stellen die **itWatch**-Lösungen ihre Stabilität und Effizienz täglich unter Beweis.
Alle **itWatch**-Produkte werden, frei von Hintertüren und ohne Zukauf von Teil- oder Gesamtlösungen, im Hause **itWatch,** in Deutschland, entwickelt, getestet und weltweit über Partner vertrieben.

## JK DEFENCE & SECURITY PRODUCTS GMBH — Stand: P 6

Die JK DEFENCE & SECURITY PRODUCTS GMBH steht seit über 20 Jahren für Qualität und Zuverlässigkeit im Bundeswehrgeschäft. Lag in der ersten Dekade der Schwerpunkt in der Beschaffung ausländischer Luftfahrzeugteile für die deutsche Luftwaffe, beschäftigen wir uns heute auch mit der Beschaffung und Integration von militärischen Funksystemen.
Als Deutschland-Vertretung des größten Herstellers von militärischen Funkgeräten **Harris-RF** bieten wir die komplette Bandbreite von portablen und stationären Funk- und Aufklärungsgeräten an. Ob als Hand-Held oder Man-Pack, modular oder fest eingebaut in gepanzerten Fahrzeugen, Booten oder Schiffen: Wir haben immer eine hauseigene Lösung für Kommunikation und Aufklärung. Zum Beispiel das Software Defined Radio PRC-117/G welches bestehende und zukünftige Wellenformen in einem Frequenzbereich von 30MHz bis 2GHz abdecken kann.

## Kontron AG — Stand: T 4

Kontron ist Embedded Computer Lieferant für militärische Anwendungen. Wir bieten Ihnen starke Entwicklungs- und Fertigungsressourcen im eigenen Hause und eine große Basis an militärischen Computer Basisprodukten auf Board- und System-Level. Inklusive maßgeschnittenem Softwaresupport. Unsere Standardprodukte lassen sich leicht auf Ihren spezifischen Bedarf anpassen – sei es für ihre Applikationsanforderung, für offizielle Militär-Programme oder für gänzlich neue Wehr-Technologien.
Wir arbeiten mit unseren Kunden und Partnern sehr individuell und dem Bedarf entsprechend zusammen. Unsere jahrzehntelange Erfahrung mit militärischen Projekten und die damit verbundenen Anforderungen an die Einhaltung von Standards sowie unser umfangreiches Produktportfolio gibt Ihnen die Sicherheit, dass wir stets höchsten Anforderungen gerecht werden.
**Kontakt:** Frau Ingrid Einsiedler, Dipl. Wirtsch. Ing (FH), Marketing Manager, Kontron AG, Oskar-von-Miller-Str. 1, D-85386 Eching, Germany, Phone: +49 (0)8341 803 357, Fax: +49 (0)8341 803 40 499

## Lachen Helfen e.V. — Stand: E 2

**Eine Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten.**
"Lachen Helfen e.V." wurde 1996 durch Soldaten im Einsatz in Kroatien gegründet und ist seit 1998 ein eingetragener, als gemeinnützig anerkannter Verein, mit dem Ziel, Kinder in Kriegs- und Krisengebieten zu unterstützen. Dies geschieht u. a. durch den Wiederaufbau bzw. Bau von Kindergärten, Schulen und Gesundheitszentren. Der Bedarf wird in den Einsatzländern (EUFOR, KFOR und ISAF) durch Soldaten vor Ort erkundet, die Ausführung wird begleitet und überwacht, so wird verhindert, dass Gelder in falsche Hände geraten. Größere Projekte werden vorab mit dem Einsatzführungskommando in Potsdam abgestimmt.
Im Verein sind Mitglieder, sowie ehemalige und aktive Soldaten und Polizisten ehrenamtlich tätig. Die Geschicke des Vereins werden von der Bundesgeschäftsstelle in der Bergischen Kaserne in Düsseldorf aus gelenkt. Das Spendenaufkommen fließt zu 90% in die Projekte ein.
Seit Frühjahr 2009 ist die Polizei in den Verein integriert, eine sehr sinnvolle Kooperation aufgrund der Tatsache, dass sie mit der Bundeswehr häufig im selben Einsatzland Dienst leistet. Der Bundesminister der Verteidigung, der Generalinspekteur, der Wehrbeauftragte sowie viele andere unterstützen "Lachen Helfen e.V." bereits aktiv. Ein Großteil des Sponsorings bestreiten Wirtschaft und Industrie. Ein wertvoller Teil der Vereinsarbeit liegt aber auch in den Händen unserer Standortrepäsentanten. Mehr unter www.lachen-helfen.de.

## Liske Informationsmanagementsysteme — Stand: FR 4

**Liske Informationsmanagementsysteme** ist Produzent von Informations- und Wissensmanagementsystemen. Mit **MIRAKEL®** steht dafür eine eigene Entwicklungsplattform und Produktpalette zur Verfügung. **MIRAKEL®** verarbeitet und ermöglicht den Zugriff auf Informationen aus Papier, elektronischen Dateien, Mailsystemen wie Outlook oder LOTUS, Internetseiten und Datenbanken. Der direkte Zugriff auf die Informationen in den Originaldateien erfolgt über ein sehr leistungsfähiges, fehlertolerantes Textretrival. Einsatz in konventionellen Netzwerken, im Intranet und Internet.
Zu den auf der Entwicklungsplattform **MIRAKEL®** angebotenen Leistungen gehören die

- Beratung, Installation, Schulung und Wartung zum Einsatz der Standardprodukte
- Analyse und das Reengineering von Informationsprozessen
- Konzipierung, Entwicklung, Anpassung und Implementierung von Informations- und Wissensmanagementsystemen

## LOG GmbH — Stand: K 6

Die LOG GmbH hat sich seit ihrer Gründung 1987 zu einem international anerkannten Logistikberater mit starker Umsetzungsorientierung entwickelt – wir sind der Spezialist für sichere, individuelle logistische **Lösungen** in den Geschäftsfeldern Logistics Consulting, Concepts & Coaching, Life Support, Product Lifecycle Management, Engineering Support und Data Management. Wir verfügen über umfassendes Know-how in Logistikprozessen und stehen für hohes Qualitätsbewusstsein (zertifiziert nach DIN EN ISO 9001:2008), Sicherheit, technologische Innovationen, Zukunftsorientierung und Methodenkompetenz. Unser Ziel ist es, zusammen mit den Kunden praxisgerechte Lösungen zu erarbeiten, die langfristig zukunftsfähig sind und wirtschaftliche Vorteile verschaffen. Mit unserem ganzheitlichen Beratungsansatz - von der ersten Analyse und Beratung über die Erstellung von Konzeptionen und die Umsetzung bis hin zum Service und Support - bieten wir SOLUTIONS FOR YOUR SUCCESS aus einer Hand.
An Stand K 6 präsentieren wir Ihnen einen Ausschnitt aus diesem umfangreichen Lösungsspektrum.
**Ansprechpartner:** LOG GmbH, Volker Reiser, Leiter Marketing & Vertrieb, Adenauerallee 131a, 53113 Bonn, Tel.: +49 228 4107-142, Fax: +49 228 4107-121, Mobil: +49 171 41 20 688, Mail: Volker.Reiser@LOGmbh.de, http://www.LOGmbh.de

## Logic Instrument GmbH — Stand: Z 3

**Logic Instrument** bietet individuelle hochrobuste Hardwarelösungen im Bereich robuster mobiler und tragbarer Computer, sowie außentauglichen Displays.
Mit mehr als 20 Jahren Entwicklungs- und Markterfahrungen, Standorten in Frankreich, den USA und Deutschland, sowie einem engen, weltweitem Partnernetzwerk ist die Logic Instrument Gruppe ein solider und kompetenter Partner für Projekte mit oder ohne zusätzlichen Sonderlösungen. Nennenswert ist hier die Auslieferung von 7000 full-ruggedized Notebooks an Lockheed Martin, Zulieferer des US-Militärs.
Mehr Informationen finden Sie auf unserer Homepage: www.logic-instrument.com

## Logica Deutschland GmbH & Co. KG — Stand: K 1

Logica ist mit 41.000 Mitarbeitern in 40 Ländern ein führender Anbieter von IT- und Beratungsdienstleistungen mit den Kernmärkten Skandinavien, Großbritannien, Frankreich, den Niederlanden und Deutschland. Das Unternehmen ist erfolgreich in allen Bereichen der IT-Dienstleistungen, bei Beratung und Outsourcing von IT- und Geschäftsprozessen, sowie bei Systemintegration und Entwicklung von kundenspezifischen Lösungen. Logica unterhält enge Bezie-

hungen zu großen nationalen und europäischen Unternehmen und Institutionen, darunter zu mehreren Verteidigungsministerien, zur NATO und der EU. Unsere Mitarbeiter sind auch in NATO Missionen, z.B. ISAF, vor Ort.
In Deutschland ist Logica in 12 Städten und 2.000 Mitarbeitern, unter den Top-Ten der IT-Beratungs- und Systemintegrationsunternehmen gelistet. Bundeswehr und NATO zählen seit vielen Jahren zu unseren zufriedenen Kunden der Geschäftsstelle Köln/Bonn in Hennef.
In diesem Jahr präsentieren wir u.a. unsere Beiträge zu den nationalen und internationalen Führungsinformationssystemen FülnfoSys SK und NATO Document Handling System und Lösungen aus dem Bereich Mobile Computing.

## Luciad — Stand: K 3

Luciad bietet Softwarelösungen für die leistungsfähige Datenfusion, Visualisierung und Analyse von Erdbeobachtungsdaten. Die Softwarekomponenten von Luciad sind die Bausteine für unternehmenskritische ATC/ATM- und C4ISR-Systeme.
Das Flaggschiff von Luciad ist LuciadMap™, eine Softwarelösung, die von Systemintegratoren und OEM mühelos in ihre Systeme integriert werden kann. LuciadMap stellt das Framework und die Funktionen bereit, um ein hochwertiges Situationsbewusstsein zu erreichen, indem sehr effizient große Mengen statischer und beweglicher Daten verwaltet werden, die über geografische Informationen gelegt werden. Diese können Landkarten, Satellitenbilder und Geländeerhebungsdaten in vielen unterschiedlichen Formaten und Referenzen umfassen.
Für mehr Informationen besuchen Sie bitte www.luciad.com oder kontaktieren Sie uns unter Info@luciad.com

## Maibach Industrie-Plastic GmbH — Stand: Z 9

Hochwertige elektronische und mechanische Baugruppen fordern sicheren Schutz während des Betriebes, der Lagerung und des Transports.
Die Firma Maibach Industrie-Plastic GmbH entwickelt und fertigt seit 30 Jahren hochwertige Behälter aller Größen, die Packgüter gegen mechanische und klimatische Einflüsse schützen:

- 19“ Transport- und Betriebsbehälter nach militärischen Normen mit und ohne Klimatisierung.
- Gerätegehäuse für den Einsatz im Freien und in Gebäuden.
- Transport- und Lagerbehälter nach VG 95613 und AEPP-1 / AEPP-2.
- Schwerlast-Großcontainer nach MIL-STD-810 und ATA 300.
- Entwicklung, Dokumentation, Herstellung und Test von Geräte-Verpackungen.
- Beratung bei der Umsetzung von militärischen und zivilen Verpackungsanforderungen.

**Kontakt:** E-Mail: info@maibach-ipg.de, www.maibach-ipg.de

## Martin Yale International GmbH — Stand: ZA 4

**Ein Pionier der Informationssicherung– intimus® *CRYPTO***
Was die Löschung vertraulicher Daten auf Endpoint-Medien angeht, verlassen sich unsere Kunden auf unsere weitreichende Erfahrung. Was vor mehr als 50 Jahren mit dem Reiswolf begonnen hat, ist heute eine Produktpalette für alle Belange der Informationssicherung. Der Name intimus®, lateinisch für den engsten Vertrauten, ist dabei Programm. Dank langjähriger Beziehungen zu Regierungen und Weltkonzernen sind wir mit unseren Forschungen und Entwicklungen den gesetzlichen Vorgaben und technischen Veränderungen immer einen Schritt voraus. Die jüngste Generation von Hochsicherheits-Aktenvernichtern ist seit Juli 2011 NSA-zugelassen (NSA/CSS-Spezifikation 02-01).
Leistungsspektrum:

- Aktenvernichter in allen gängigen Sicherheitsstufen
- Großanlagen für die Vernichtung von digitalen Datenträgern und Dokumenten
- Disintegratoren
- Degausser
- Data Grinder
- Secure Erase

## Microsoft Deutschland GmbH — Stand: F 9

Vernetzte Operationsführung erfordert sichere, zuverlässige und leistungsfähige Plattformen, bei denen die IT-Systemintegration die Basis stellt. Anforderungen und Systeme in der vernetzten Operationsführung unterliegen einem schnellen Wandel. Die Integration der Systeme muss vereinfacht und auf eine durchgängige Plattform gebracht werden, um dieser Herausforderung besser begegnen zu können. Die MS Produktpalette bietet eine hochintegrative Plattform, welche die Streitkräfte dabei unterstützt, die Systemintegration von der Kerninfrastruktur bis hin zur Applikationsplattform zu erleichtern. Auf dem Stand F9 zeigen wir Lösungen, wie die menschliche Führungsleistung durch permanente gegenseitige Vernetzung auf Basis von SharePoint und System Center verbessert werden kann.
**Kontakt:** Frank Grotheer, Holzmarkt 2a, 50676 Köln, E-Mail: frankgro@microsoft.com, Tel.: 0221/8010-0

## Mittler Report Verlag GmbH — Stand: P 4

Im Mittler Report Verlag sind heute alle Aktivitäten gebündelt, die der Report Verlag sowie die Bonner Niederlassung des Verlages E.S. Mittler & Sohn in der Vergangenheit unter dem Dach der Gruppe Tamm Media separat verantwortet haben. Das Portfolio umfasst alle bisherigen Publikationen und Dienstleistungsangebote beider Verlagshäuser: Zeitschriften, Broschüren, Informationsdienste und Fachtagungen. Dazu zählen insbesondere die aus der Zusammenführung der Zeitschriften “Europäische Sicherheit” und “Strategie & Technik” entstandene und in vertraglich geregelter Zusammenarbeit mit dem Bundesministerium der Verteidigung herausgegebene unabhängige Monatszeitschrift “Europäische Sicherheit & Technik”, die internationale Schwesterzeitschrift “European Security and Defence”, die Fachzeitschrift “MarineForum”, die Broschürenreihen “Wehrtechnischer Report” und “Sicherheitstechnischer Report” sowie die Informationsdienste “Mittler-Brief” und “Wehrwirtschaft”. www.mittler-report.de

## ML Consulting Schulung, Service & Support GmbH — Stand: F 13

**ML Consulting – Ihr Bildungsdienstleister Nr. 1!**
Die ML Consulting ist seit mehr als 20 Jahren einer der führenden Bildungsanbieter. In großen Bildungsprojekten sind wir leistungsstarke Partner öffentlicher Auftraggeber und Unternehmen aller Branchen. Wir bieten unseren Kunden maßgeschneiderte Lösungen und eine kontinuierliche individuelle Betreuung. Im Rahmen zahlreicher Ausbildungsprojekte wie den Kompetenzzentren IT (KIT), dem Projekt SASPF und bei der Realisierung von Fernausbildung sind wir Partner der Bundeswehr. Mit mehr als 350 festen und freien Mitarbeitern verfügen wir als mittelständisches Unternehmen über hervorragendes Know-how in den Bereichen ERP-Projekte, Informationssicherheit, Servicequalifizierung sowie IT- und Soft Skills-Training. Nähere Informationen zu unserem Leistungsangebot finden Sie im Internet unter www.mlconsulting.de .

## Mönch Verlagsgesellschaft mbH — Stand: FR 1

Die Verlagsgruppe Mönch mit einer Vielzahl regionaler und internationaler Printmedien für Verteidigung, Sicherheit und Wehrtechnik sorgt schon seit länger als 50 Jahren für Transparenz und gediegene Kontaktpflege im Verteidigungsmarkt. Die mediale Verbindung zu Kunden, Entscheidern und Meinungsbildnern ist neben der deutschen Sprache (durch die Zeitschrift WEHRTECHNIK) in Englisch, Spanisch, Italienisch, Türkisch und Arabisch möglich. Der Großteil der Publikationen ist inhaltlich auf die Gesamtstreitkräfte abgestellt. Spezialausgaben behandeln das aktuelle Geschehen in allen anderen Disziplinen der Wehrtechnik und Sicherheitspolitik. Sie reflektieren die Entwicklungen in den Streitkräften, Beschaffungsorganisationen, Beschaffungsprogrammen, der Verteidigungsindustrie und in den Unternehmen weltweit.
www.mpgbonn.de

## Motorola Solutions GmbH — Stand: K 8

Motorola Solutions ist ein führender Anbieter von geschäfts- und sicherheitskritischen Kommunikationslösungen und -services für Unternehmen und Behörden. Durch wegweisende Innovationen in der Kommunikationstechnologie und sein umfassendes Portfolio nimmt Motorola Solutions weltweit eine Vorreiterrolle ein und versetzt Kunden in die Lage, in entscheidenden Momenten ihr Bestes zu geben.
Das Portfolio umfasst:

- Robuste mobile Computer zur Datenerfassung in Echtzeit
- Robuste Barcodescanner für jeden Einsatzbereich
- RFID (Radio Frequency Identification)
- Lizenzpflichtiger und kommerzieller Funk
- WLAN Infrastruktur für In- und Outdoor
- Professional Services: Netzwerksicherheit, Systemintegration sowie Remote Management von Netzen und Geräten

## ND SatCom GmbH — Stand: Z 7

ND SatCom, seit März 2011 ein Tochterunternehmen von Astrium (Teil des EADS Konzerns), ist ein führender globaler Anbieter von satellitenbasierten Breitbandnetzen, VSAT-Systemen, Bodenstationen und den dazugehörigen Komponenten und Softwarelösungen. Die innovativen Technologien werden weltweit von Regierungen, dem Militär sowie in den Bereichen Fernseh- und Rundfunkübertragung, der Telekommunikation und von Unternehmen eingesetzt.
Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist das deutsche Unternehmen ein zuverlässiger Partner für die schlüsselfertige Lieferung maßgeschneiderter und sicherer Netzwerklösungen.
ND SatCom ist weltweit durch regionale Vertriebs- und Servicebüros vertreten.

## Oracle Deutschland B.V. & Co. KG — Stand: T 5

Oracle entwickelt Hardware und Software, die für den Einsatz in allen Branchen optimal aufeinander abgestimmt sind.
Strategisch hat sich Oracle darauf ausgerichtet, Lösungen komplett, offen und integriert zu entwickeln, so dass die einzelnen Produkte untereinander und mit anderen auf Standards basierende Komponenten kompatibel sind.
In über 145 Ländern der Welt nutzen mehr als 380.000 Kunden die fertigen Unternehmensanwendungen von Oracle oder entwickeln für ihre individuelle Anforderungen aus den Standardkomponenten passende Lösungen. Im letzten Geschäftsjahr erzielte Oracle weltweit mit über 108.000 Mitarbeitern einen Umsatz von 35,6 Milliarden US-Dollar.
Mehr als 100 Kunden im Verteidigungssektor nutzen heute schon auf **commercial off-the-shelf** (COTS) Lösungen von Oracle.

## Overwatch® Systems Ltd. — Stand: P 5

Overwatch®, a strategic business of Textron Systems Advanced Systems, an operating unit of Textron Systems, is an industry leader in imagery analysis and geospatial intelligence solutions. Our flagship software products, GIV® and RemoteView™, provide high-powered image exploitation and mapping for tactical users. Defense and intelligence communities around the world trust Overwatch's software for its positioning accuracy and efficient workflows.
Overwatch understands automatic feature extraction, with proven results through our Feature Analyst™ and LIDAR Analyst® software extensions for ArcGIS®. These products rapidly and accurately collect vector feature data from high-resolution satellite imagery and airborne LIDAR data.
See www.overwatch.com for more information.

## Pan Dacom Networking AG – Pan Dacom Direkt GmbH — Stand: T 6

**Pan Dacom – Partner der Bundeswehr**
Pan Dacom Networking AG ist ein mittelständisches konzern- und herstellerunabhängiges Unternehmen mit den beiden Bereichen Systemintegration und Pan Dacom Direkt. Als Systemintegrator, Dienstleister und Hersteller für Networking und Informationstechnologie ist Pan Dacom eines der führenden Unternehmen. Mit dem Hauptsitz in Dreieich bei Frankfurt verfügt Pan Dacom über eine deutschlandweite Flächendeckung und europäischen Geschäftsverbindungen.
**Mobile Kommunikationnetze**
Hightech-Netzwerklösungen mit den dazugehörigen Dienstleistungen im Service und Professional Service Bereich. Mit dem eigenen Network Operartion Center (NOC) erbringt Pan Dacom Managed Service Dienstleistungen und Remote Monitoring Services. Je nach Wunsch werden einzelne Leistungen bis hin zu einer ganzheitlichen Erbringung aller Leistungen durch Pan Dacom erbracht, wie beispielsweise die Entwicklung der Mobilen Kommunikationsnetze auf Basis der gängigen Industriestandards.
http://www.pandacom.de/
**Kontakt:** Pan Dacom Networking AG, Dreieich Plaza 1B, 63303 Dreieich, Telefon: +49-6103-932-0, Fax: +49-6103-932-400, E-Mail: info@pandacom.de
Pan Dacom Direkt GmbH, Dreieich Plaza 1B 63303 Dreieich, Telefon: +49-6103-932-333, Fax: +49-6103-932-444, E-Mail: kontakt@pandacomdirekt.de

## Panasonic Deutschland GmbH — Stand: Z 5

**Panasonic** entwickelt und fertigt in eigenen Produktionsstätten besonders energieeffiziente widerstandsfähige Mobile Computing Produkte – von robusten Outdoor-Notebooks über Business-Laptops bis hin zu Tablet-PCs.
Höchsten Ansprüchen an Mobilität, Leistungsfähigkeit und Widerstandsfähigkeit werden Toughbook Geräte durch besondere Schutzmaßnahmen, geringes Gewicht und besonders lange Akkulaufzeiten gerecht.
Weder Wasser, Staub, Stürze oder Erschütterungen (IP65, MIL-STD-810G, MIL-STD-461E) können den Modellen der Schutzklasse „Full-Ruggedized" etwas anhaben. Selbst in extremen Temperaturbereichen von -20° bis +60° Celsius bleiben sie zuverlässig im Einsatz.
Nicht von ungefähr sind Toughbooks die weltweit führenden Robust-Notebooks, die bei einer Vielzahl von Polizei-, Armee- und Spezialkräften eingesetzt werden.
Speziell für die Personenidentifizierung wurde das CF-U1 mit PIMD-Modul entwickelt: der handliche UMPC mit OCR-Erkennung, RFID-Leser und optionalem Fingerabdruckscanner ist die ideale Lösung für Grenzkontrolleure, Polizeistreifen und Sicherheitskräfte.
Weitere Informationen finden Sie unter: www.toughbook.de

## PROCITEC GmbH — Stand: B 8

Die PROCITEC GmbH ist ein weltweit agierendes hoch spezialisiertes Software-Unternehmen im Bereich Nachrichtentechnik und Informationstechnologie.
Wir konzipieren, entwickeln und implementieren Softwareprodukte und Systemlösungen zur Erfassung und Aufklärung von:
- HF/VHF/UHF-Funk
- Satellitenkommunikation
- Laserkommunikation
- Richtfunk

Unsere Lösungen sind offene, skalierbare und erweiterbare Softwaresysteme. Von der manuellen Analyse bis zur vollautomatischen Inhaltsgewinnung decken wir die wichtigsten Schritte der Signalverarbeitung ab:
- Signaldetektion und - klassifikation
- Demodulation und Dekodierung
- Signalaufzeichnung
- Signalanalyse
- Sprachverarbeitung

Wir sind langjähriger Partner der deutschen Sicherheitsbehörden: von der Idee über die Definition bis hin zum erfolgreichen Roll-Out komplexer Systeme.
**Kontakt:** PROCITEC GmbH, Rastatter Str. 41, 75179 Pforzheim, Tel.: +49 7231/15561-0, E-Mail: o.themann@procitec.de, www.procitec.de

## promegis GmbH — Stand: P 5

Als Spezialist für Geoinformatik, digitale Bildverarbeitung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen für Geoinformationssysteme, Image Analysis Produkte sowie fachspezifische Systemlösungen für die Bereiche öffentliche Verwaltung, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Verteidigung, Wirtschaft und Industrie. Darüber hinaus unterstützen wir unsere Kunden bei der Umsetzung umfangreicher IT-Projekte.
Die promegis setzt auf innovative und gleichzeitig zukunftssichere Lösungen und steht Ihnen mit langjähriger Erfahrung bei der Realisierung komplexer, integrationsfähiger Systemlösungen zur Seite. Als deutscher Vertriebs- und Entwicklungspartner der Firma Overwatch Systems bieten wir Ihnen die volle Bandbreite der High-End GIS und Image Analysis Lösungen.
Weitere Informationen finden Sie auf unserer Homepage unter www.promegis.de.
Kontakt: **promegis,** Gesellschaft für Geoinformationssysteme mbH, Breslauer Straße 31, D-49324 Melle, Klaus Scholle, klaus.scholle@promegis.de, Tel. +49 (0) 5422 9629 16, Mobil: +49 (0)173 2792721, Fax: +49 (0) 5422 9629 20, www.promegis.de

## PWA Electronic Service- und Vertriebs- GmbH — Stand: Z 5

PWA – Ihr Spezialist für Beratung, Vertrieb, Service und Support von gehärteten Notebooks, Komponenten und Peripherie für mobile Anwendungen.
Inzwischen blicken wir gemeinsam mit Panasonic Computer Products Europe auf eine Erfahrung von 16 Jahren zurück. Wir bieten für die Panasonic Toughbooks das komplette Sortiment an Unterstützung an: Neugeräte, Zubehör, Restposten, Ersatzteile, Service und Support. Seit September 2007 sind wir außerdem exklusiver Panasonic Service-Partner für Deutschland und Österreich.
Folgende Panasonic Toughbooks können Sie sich auf unserem Stand anschauen: CF-19, CF-31, CF-52 High Modell, CF-53, CF-H2, CF-U1, CF-C1, CF-D1, FZ-A1 – von Business-Ruggedized, über Semi-Ruggedized bis hin zu Full-Ruggedized.
Weitere Informationen finden Sie auf unserer Homepage www.pwa-electronic.de.

## Rockwell Collins Deutschland GmbH — Stand: Z 2

Rockwell Collins Deutschland, mit Firmensitz in Heidelberg, beschäftigt über 500 Mitarbeiter. Unsere Kernkompetenzen, aufbauend auf eine 50-jährige Erfahrung, liegen in Entwicklung, Herstellung, Systemintegration, Vertrieb, Wartung und Instandhaltung von Kommunikations- und Navigationsgeräten, sowie Flugregel- und Wetterradarsystemen, Missionsrechnern und Ausrüstung für militärische und zivile Anwendungen.
Unsere Aktivitäten umfassen unter anderem:
- Avionik-Subsystem-Integration
- Geräte und Systemlösungen für UAS/ UAV
- Taktische Datenlink-Übertragungssysteme
- Funkgeräte für Luft- und Bodenanwendungen u. a. mit modernster SDR-Technologie
- Militärische Navigationssysteme für Schiffe und Fahrzeuge
- Modulare Rechnersysteme für militärische Anwendungen
- Entwicklung und Herstellung der TELDIX® Space Wheels (Präzisions-Schwungräder) für Satelliten

## roda computer GmbH — Stand: Z 8

roda computer GmbH ist spezialisiert auf die Entwicklung, Herstellung und den Vertrieb mobiler robuster Rechner. Das Portfolio besteht aus Notebooks, Handhelds, PDAs, Fahrzeugrechner, Displays und Sonderlösungen. roda ist Rahmenvertagspartner der Bundeswehr für gehärtete Notebooks. (RV R6645)
Die mobilen Rechner zeichnen sich aus durch:
- extreme Robustheit
- geringe EMV-Abstrahlung
- variable Schnittstellen
- modularem Aufbau
- Integrationsvielfalt in mobile Systeme
- reichhaltige Zubehörprodukte
- optimale Konfigurierbarkeit

NEU bei roda:
**19''/2®**
Das 19"/2-Format ist ein innovatives Produktdesign robuster IT für militärische Kommunikation. Das military off-the-shelf (MOTS) Format 19"/2® mit halbierten Abmessungen ermöglicht eine Reduzierung des Volumens um bis zu 75 Prozent der IT- und Kommunikationsausstattung. 19"/2 -Rechner, -Server, -Switch, und -Router in vielen Konfigurationsmöglichkeiten sind beliebig zu kombinieren, z.B. in einen Systemschrank oder Fahrzeugkabine.
**Ultra Mobile PC DB6**
Der 5" Handheld PC ist eine völlig neue PC-Entwicklung mit besonderer Unempfindlichkeit gegen Umwelteinflüsse. Der DB6 bietet Win-dows 7, Festplatte, lange Akkulaufzeit und große Schnittstellenvielfalt bei geringstem Gewicht.
**Kontakt:** roda computer GmbH, Landstr. 6, 77839 Lichtenau, Tel.: +49 (0 72 27) / 95 79-0, Fax: +49 (0 72 27) / 95 79-20, E-Mail: mail@roda-computer.com, Internet: www.roda-computer.com

## Rohde & Schwarz Vertriebs-GmbH — Stand: G 18

Die Rohde & Schwarz GmbH & Co. KG steht seit über 75 Jahren für Qualität und Präzision in den Bereichen Messtechnik, Rundfunk, sichere Kommunikation sowie Überwachungs- und Ortungstechnik.
Das Unternehmen unterstützt Hersteller in Entwicklung und Produktion elektronischer Geräte mit **Messtechnik** überall dort, wo es gilt, Signale zu generieren, zu analysieren, zu vermessen oder das Spektrum zu analysieren. Im Bereich Aerospace & Defense bündelt der

Konzern seine Kompetenz mit Messtechnik-Lösungen für Richtfunkstrecken, Radarsysteme und Satellitenkommunikation
Rohde & Schwarz liefert interoperable und leistungsfähige **Kommunikationssysteme,** die im Einsatz- oder Krisenfall die zeitnahe Koordination ziviler, behördlicher und militärischer Einsatzkräfte gewährleistet. Durch moderne Verschlüsselungsverfahren erfüllen die Lösungen des Unternehmens höchste Sicherheitsstandards. Für Unternehmen, Regierungsstellen, Bundeswehr und NATO entwickelt und produziert die Rohde & Schwarz SIT GmbH zudem **Kryptoprodukte** und -systeme.
Darüber hinaus entwickelt und produziert Rohde & Schwarz stationäre sowie mobile Systeme zur **Erfassung, Ortung und Analyse von Funkkommunikationssignalen.**

## rola Security Solutions GmbH — Stand: G 16

rola Security Solutions GmbH mit Sitz in Oberhausen zählt seit fast 30 Jahren zu den bedeutendsten Anbietern von IT-Lösungen im Bereich der Inneren und Äußeren Sicherheit sowie der nachrichtendienstlichen Aufklärung. Mit dem Software-Framework **rs*Frame*®** hat sich rola auf Lösungen für Informationsmanagement, vernetzte Fallbearbeitung sowie Auswertung und Analyse spezialisiert.
In der Variante **rs*IntCent*®** wird die Software im militärischen Umfeld für Auswertung und Lagefeststellung genutzt. Schwerpunkte bilden Informationszusammenführung und Informationserschließung sowie die Erzeugung dynamischer Lagebilder und die ebenengerechte Präsentation.
www.rola.com

## Saab AB – Saab International Deutschland GmbH — Stand: Z 14

**Saab AB**
For 75 years has Saab been challenging the laws of nature and pushing the boundaries of technology. Saab has extensive experience in defence systems, force protection and civil security technology – above, on and below the surface. Saab has operations and employees around the globe and constantly develops, adopts technologies in order to meet customers rapidly changing needs.
The following products will be on display at the Saab stand:
- Distributed Observation and Analysis Tool (AKKA)
- Widely Integrated Systems Environment (WISE)
- Rapid 3D Mapping™

**Saab AB**, Saab International Deutschland GmbH, Hochkreuzallee 1, DE-53175 Bonn, saab.deutschland@saabgroup.com, Tel.: +49 228 36 75 60, Fax: +49 228 3675 620, www.saabgroup.com

## SAP Deutschland AG & Co. KG — Stand: G12

SAP bietet in fast allen Bereichen Lösungen für die Bundeswehr an. Auf der diesjährigen AFCEA zeigen wir neben den streitkräftespezifischen Lösungen auf Basis der SAP® Business Suite auch hochspezielle Lösungen unserer Partner im Bereich der Führungsinformationssysteme und Nachrichtendienste.
Die vielseitigen Anwendungen der Branchenlösung SAP for Defense & Security unterstützen dabei die Prozessorientierung, reduzieren Kosten und erhöhen die Transparenz. Auch unser mobiles Lösungsportfolio erweitern wir ständig und bieten unseren Kunden umfangreiche, sichere und anwendungsnahe mobile Lösungen. Analytische Anwendungen stehen mit SAP HANA™ sehr performant zur Verfügung und können auf jedem mobilen Endgerät eingesetzt werden. Die Zukunft der mobilen IT beginnt an unserem Stand. Wir freuen uns auf Ihren Besuch!
Weitere Informationen finden Sie auf unserer Homepage unter www.sap.de/defense

## Schnoor Industrieelektronik GmbH & Co. KG — Stand: G 5

Schnoor Industrieelektronik ist ein führendes Unternehmen auf dem Gebiet der Funktechnik in Deutschland. Seit 1990 werden individuelle Funk- und Kommunikationslösungen für nationale und internationale Kunden aus namhaften Behörden und Unternehmen entwickelt.
Schwerpunkte sind: Öffentliche Sicherheit (Polizei, Feuerwehr, Bergwacht), Öffentlicher Verkehr (Zugfunk, Verkehrsleitung), Gebäudesicherheit (Industrie, Behörden), Maritime Sicherheit (Seefunk - SEACOM, SARCOM, NIF, NAVTEX).
Von der Planung und Projektierung über die Entwicklung kundenspezifischer Hard- und Software bis hin zu Fertigung, Inbetriebnahme und Support wird alles aus einer Hand geliefert.
**Unsere Kompetenzbereiche:**
- VoiP-Leitstellentechnik (Seenotrettung, Bergwacht, Küstenfunk)
- Funksysteme analog und digital (TETRA)
- Fahrzeug-Funkanlagen
- Universelle Bediengeräte (seewasserfest, handschuhbedienbar)

**Weitere Informationen:** www.Schnoor-INS.com

## Schönhofer Sales and Engineering GmbH (SSE) — Stand: G 6 – G 8

Das Unternehmen Schönhofer Sales and Engineering GmbH (SSE) ist ein herstellerunabhängiges System- und Softwarehaus mit den Schwerpunkten:
- Realisierung, Implementierung und Integration von Informations- und nachrichtentechnischen Systemen
- Konzeption, Beratung, Studien und Betrieb als systemtechnische Unterstützung
- Sonder- und Sicherheitstechnik in fahrzeuggebundenen Systemen

SSE unterstützt seit über 25 Jahren Kunden aus dem öffentlichen und gewerblichen Umfeld. Insbesondere im Umfeld von Behörden und Organisationen mit Sicherheitsaufgaben sowie der Bundeswehr ist SSE mit ihrem umfangreichen Know-how über den gesamten Lebenszyklus von Informations- und Kommunikationssystemen bekannt.
Seit Oktober 2010 sind wir darüber hinaus Channel Partner der i2 und bieten als Ergänzung zu unseren eigenen Lösungen die gesamte Analysis Produktlinie einschließlich
- Analyst´s Notebook
- iBase
- Analyst´s Notebook ESRI Edition

sowie Beratung und Support exklusiv für die Streitkräfte, Nachrichtendienste und alle anderen Behörden in Deutschland, Österreich und Luxemburg an.

## SciEngines GmbH — Stand: B 9

Die **SciEngines GmbH,** 2007 im Zuge des COPACOBANA (Cost-Optimized Parallel Code Breaker) Projektes gegründet, bietet FPGA-Lösungen für das Hochleistungsrechnen an.
SciEngines Computer ermöglichen insbesondere im Bereich der Kryptographie einen intelligenten und effizienten Einsatz der Ressourcen, mit i.d.R. Einsparungen von >95% der laufenden Kosten und 10-30x besserem Preis-Leistungsverhältnis. Auf kleinstem Raum (3 HE) und mit minimalem Stromverbrauch (650W) kann bis zu 20000 Rechenkerne Leistung bereitgestellt werden.
Potenzielle Anwendungen finden sich u.a. in
- Einsatzszenarien der Cyberwarfare,
- Überprüfung eigener IT-Sicherheit / Penetrationstests,
- dem Entschlüsseln von Dateien und Überwachung von Kommunikation,
- groß skalierter Datenfilterung und –aggregation.

www.SciEngines.com

## secunet Security Networks AG — Stand: G 15

**secunet – IT Security beyond expectations**
secunet ist Sicherheitspartner der Bundesrepublik Deutschland und einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Im engen Dialog mit Unternehmen, Behörden und internationale Organisationen entwickelt secunet leistungsfähige Produkte und fortschrittliche IT-Sicherheitslösungen. Damit sichert secunet nicht nur IT-Infrastrukturen für seine Kunden, sondern erzielt intelligente Prozessoptimierungen und schafft nachhaltige Mehrwerte.
Unsere Ausstellungsschwerpunkte:
- Desktop basierter AMN Client und SINA Virtual Workstation H (SINA CORE) im Kontext des Allied Mission Network und militärischer Führungsinformationssysteme
- Rocky III+ basierte SINA Workstation (SINA CORE M100R)
- SINA L3 Box H 200M

Ergänzende Informationen: www.secunet.com

## Secusmart — Stand: Z 10

Auf der diesjährigen AFCEA Fachausstellung präsentiert Secusmart jetzt eine weitere Hardware-Verschlüsselungslösung für kritische Kommunikationsbereiche auf Basis des Android Betriebssystems.
Unter dem Motto “Securing the world of mobile communication” stellt Secusmart im Außenzelt (Stand Z10) erstmals ihre hardware-basierte Krypto-Lösung SecuVOICE auf dem Android-Mobiltelefon Samsung Galaxy S II vor. SecuVOICE gewährleistet eine sichere Ende-zu-Ende-Kommunikation.
Mit der Entscheidung für Android orientiert sich Secusmart an den hohen Wachstumsraten des Betriebssystems für Mobilfunktelefone, dessen Marktanteil laut aktuellen Angaben von Gartner bei über 50 Prozent liegt. Ein Vorteil der Secusmart Secure-VoIP-Lösung ist die erprobte einfache Integration in bestehende TK-Infrastrukturen in Unternehmen und Behörden.

## SELEX Communications GmbH — Stand: G 4

Die SELEX Communications entwickelt, fertigt und integriert zuverlässige Kommunikationslösungen für Industrie, Sicherheitsbehörden und Militär. Durch die Einbindung modernster Informations- und Kommunikationstechnologie eröffnen die Lösungen von SELEX Communications dem Nutzer neue Anwendungsmöglichkeiten, die im Rahmen einer modernen militärischen Operationsführung notwendig sind. Hierbei folgen diese Lösungen den netzwerkübergreifenden, interoperationellen Forderungen nach Mobilität und Verfügbarkeit, basierend auf sicheren IP-Verbindungen.
Neben eingeführten Systemen wie Richtfunk, PRR, Glasfasertechnik und HF/VHF/UHF-Funk bietet die SELEX Communications auch neue Gerätefamilien, wie mobile Breitband IP- und SWave® SDR-Funksysteme, Multiservice-Anwendungen für Netzwerke sowie mobile Arbeitsplatzsysteme (verlegefähige Accessnetze) an.
Weitere Informationen finden Sie unter www.selexcom.de
**Kontakt:** SELEX Communications GmbH, Spinnerei 48, D-71522 Backnang, Bernd Broghammer, E-Mail: bernd.broghammer@selexelsag.com, Tel.: +49 (0)7191-378-512, Mobil: +49 (0)175-2711725, Fax: +49 (0)7191-378-500, www.selexcom.de

## Serco GmbH — Stand: G 11

**Beraten • Entwickeln • Integrieren • Umsetzen**
Serco: Partner der Bundeswehr

- Systemintegration: Serco mobilisiert Systeme und Komponenten für Out-of-Area-Einsätze.
- Elektromagnetische Verträglichkeit (EMV): Serco betreibt akkreditierte EMV-Zentren in Bonn und Ottobrunn und bietet höchste Kompetenz im gesamten EMV-Sektor.
- Systemunterstützung: Serco unterstützt die Bundeswehr als Dienstleister u.a. im Einsatz in den Bereichen Service, Ausbildung, Einsatzführungsdienst und Dokumentationserstellung.
- IT-Lösungen / Helpdesk: Serco konzipiert, realisiert und implementiert qualitätsgesicherte IT-Lösungen, die unter Nutzung modernster Infrastrukturen für den Kunden betrieben und unterstützt werden.
- Produkte: Serco bietet Produktlösungen für den mobilen Einsatz, wie zum Beispiel GPSE, MUP, RaDoClid, Solarthermie (Energie), SAC Box, TuLB und BTuLB, LWL-Feldstecker, ...

**Kontakt:** Serco GmbH, Justus-von-Liebig-Str. 18, 53121 Bonn, Telefon: 0228/6681-0, Fax: 0228/6681-777, info@serco.de, www.serco.de

## Software AG/IDS Scheer Consulting — Stand: K 2

**SYSTEMINTEGRATION UND DATENAUSTAUSCH**
**Verbinden Sie ihre mobilen Anwendungen, nutzen Sie vorhandene Daten und realisieren Sie Systemintegration mit einer universellen Integrationsplattform.**
Mit dem marktführenden ESB der Software AG beschleunigen Sie die Systemintegration und die Entwicklung neuer Systeme. Beginnend mit den administrativen Prozessen bis hin zur Integration verschiedener Waffensysteme gibt es unzählige Beispiele für den Bedarf Organisationseinheiten bzw. Systeme miteinander zu verbinden. Gerade in einer mobilen Systemumgebung gilt es verteilte, redundante Daten und unterschiedliche Datenformate in automatisierte Prozesse zu integrieren. Verknüpfen Sie jedes beliebige System und jede Anwendung schnell miteinander. Mit Model-to-Execute ist es jetzt möglich, in ARIS modellierte Prozesse automatisiert in ausführbare Programme zu überführen.

## Sophos AG — Stand: F 6

Sophos bietet zertifizierte Verschlüsselungs-, Mobile- und Endpoint-Security-Produkte sowie Lösungen für Internet-, E-Mail- und Netzwerksicherheit, die unabhängig vom Benutzer- und Unternehmensstandort einfach zu verwalten, installieren und einzusetzen sind.
Im Jahr 2011 erweiterte Sophos sein Leistungsspektrum um Netzwerksicherheitslösungen durch die Übernahme des Netzwerksicherheitsspezialisten Astaro.
Mit der kontinuierlichen Weiterentwicklung der SafeGuard- und Astaro-Produkte (z.B. Safe Guard Device Encryption und Astaro Security Gateway) und deren Zertifizierung sowie Zulassung wichtiger Komponenten durch das BSI unterstreicht Sophos das Engagement, auch weiterhin leistungsfähige und geprüfte Produkte für den öffentlichen Markt zu entwickeln und anzubieten.
Weitere Informationen finden Sie unter www.sophos.de

## SQS Software Quality Systems AG — Stand: G 17

**SQS – führend in Software-Qualität**
SQS ist der größte unabhängige Anbieter von Dienstleistungen zu Software-Qualitätsmanagement, -Qualitätssicherung und -Testen mit dem Schwerpunkt in Europa. 1982 in Köln gegründet, beschäftigt SQS rund 2.100 Mitarbeiter. Neben einer starken Präsenz in Deutschland und Großbritannien hat SQS weitere Tochtergesellschaften in der ganzen Welt. Im Jahr 2010 erwirtschaftete SQS einen Umsatz von 162,9 Millionen Euro.
Mit über 5.000 abgeschlossenen Projekten verfügt SQS über eine starke Kundenbasis, darunter die Hälfte der DAX-30-, nahezu ein Drittel der STOXX-50- und rund 20 FTSE-100-Unternehmen. Dazu zählen unter anderem Allianz, Beazley, BP, Centrica, Daimler, Deutsche Post, Generali, JP Morgan, Meteor, Reuters und Volkswagen sowie weitere Unternehmen aus allen Branchen.

## SRH SAP Competence Center — Stand: B 1

Als Bildungs- und Schulungspartner der SAP AG Walldorf qualifizieren wir seit mehr als 18 Jahren erfolgreich SAP-Berater und SAP Anwender in allen Bereichen rund um das Rechnungswesen, Personalwirtschaft und Logistik. Wir sind in Heidelberg, Mannheim, Köln, Stuttgart und Berlin mit unseren Standorten vertreten. Außerdem sind wir national und international, u. a. in den USA, mit unseren mobilen SAP Studios für unsere Kunden tätig.
In unseren Seminaren schulen wir ausschließlich auf original SAP®ERP Online-Trainingssystemen mit den original SAP®ERP Trainingsunterlagen. Zudem kommen zu unseren SAP®ERP Seminaren nur SAP-zertifizierte Trainer zum Einsatz.
Für Firmenkunden und die Bundeswehr entwickeln wir kundenindividuelle Schulungskonzepte. Von Projekt-Team-Training (z.B.Customizing) bis zur Anwenderschulung mit eigens für Ihr Unternehmen erstellten Schulungsunterlagen bieten wir Ihnen eine kompetente Begleitung bis über die erfolgreiche Einführung hinaus.
Als Partner der Bundeswehr schulen wir erfolgreich Soldaten/Innen vom SAP Key User bis zum zertifizierten SAP Berater (Solution Consultant). Aktuell führen wir auch verschiedene SAP Arbeitsgemeinschaften durch. Infos hierzu unter: www.Srh-SAPCC.de/Bundeswehr
Profitieren Sie von unserer Erfahrung
**Kontakt:** SRH SAP Competence Center, Frau Gloria-Tamara Raber, Neckarauerstr. 200, 68163 Mannheim, 0162-2661572, 06221-88-3740

## Steria Mummert Consulting AG — Stand: F11

Mit mehr als 35 Jahren Erfahrung in der Bereitstellung von Lösungen zählt Steria Mummert Consulting zu den zehn führenden Anbietern für Management- und IT-Beratung im deutschen Markt. Wir verfügen über umfassende Fachexpertise und haben viele ehemalige und erfahrene Soldaten sowie zivile Mitarbeiter in unserem Team, die sicherstellen, dass wir die Anliegen unserer Kunden aus dem Verteidigungs- und Sicherheitssektor bestens verstehen.
**Thematische Schwerpunkte AFCEA 2012:**

- Datenbereinigung und –aufarbeitung für SASPF
- Biometrische Authentifizierungsverfahren
- Virtualisierungsbeispiele auf Server- und Desktopebene
- IT-Servicemanagement (ITSM) auf Grundlage der Information Technology Infrastructure Library (ITIL)
- IT-Sicherheit. Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten und Informationen. Wirksame Sicherheitsmaßnahmen im Bereich Cyber Defence.

**Steria Mummert Consulting AG,** Hans-Henny-Jahnn-Weg 29, D-22085 Hamburg, Homepage: www.steria-mummert.de
**Ansprechpartner:** Holger Grube, Senior Manager Public Services, Tel.: +49 40 22703-0, Fax: +49 40 22703-3567, E-Mail: public-services@steria-mummert.de

## Systematic — Stand: G 12

Systematic ist ein unabhängiges, CMMI 5 zertifiziertes Software-Unternehmen, welches skalierbare Software-Produkte, Dienstleistungen und Projekte für die Streitkräfte, BOS und Systemintegratoren anbietet.
Systematic definiert IT-Beschaffung im Verteidigungssektor neu: Hier kommt ihre off-the-shelf Produktpalette zur Steuerung von Streitkräften, zur Lagedarstellung und militärischen Nachrichtenübermittlung, sowie für das Datenmanagement im Electronic Warfare und die hochmobilen Lösungen für das Gefechtsfeld zum Tragen. Darüber hinaus bietet Systematic Schulungen, Beratungs- und Integrations-Services in diesen hochspezialisierten Bereichen.
International arbeiten mehr als 100.000 Anwender in über 35 Ländern mit den effizienten Lösungen von Systematic. Zu den Kunden gehören Armeen, Marinen, Luftwaffen, Verteidigungsministerien, Systemintegratoren, Forschungs- und Entwicklungseinrichtungen sowie Handelsorganisationen.
Besuchen Sie uns an Stand G12 und lassen Sie sich unsere zukunftsweisenden Lösungen zeigen.

## Systerra Computer GmbH — Stand: Z 12

systerra computer GmbH ist Anbieter von Langzeit-verfügbaren, schock-/vibrationsfesten und MIL-konformen Rechner-, Speicher- und Netzwerkplattformen für den erweiterten Betriebstemperaturbereich.
Board- und Komplettsystem-Lösungen von systerra bewähren sich in zahlreichen mobilen und stationären Verteidigungs-Anwendungen am Boden, in der Luft und auf See.
Das Spektrum gehärteter COTS-Rechner basiert auf anerkannten Standards wie VME, VXI, VPX, NanoATR, PC/104, CompactPCI, ATCA und MicroTCA sowie Windows-, Linux und Echtzeit-Betriebssystemen.
Unsere robusten Ethernet Switches, Router und Marine Panel PCs sind u.a. nach DNV und GL zertifiziert.
Neben Standard-Produkten namhafter Hersteller wie Themis Computer und Moxa bietet systerra computer applikationsspezifische Sonderentwicklungen/Systemlösungen, in enger Zusammenarbeit mit Kunden und Partnern entwickelt.
Weitere Informationen: www.systerra.de

## takwak GmbH — Stand: B 7

Das tw700 vereint Smartphone, Outdoor-Navigation und Walkie Talkie in einem robusten, wasserdichten und staubgeschütztes Gerät (IP57). Dank 3,5-Zoll (8,9 cm) Touch-Display lässt es sich intuitiv bedienen und mit einer Akkulaufzeit von bis zu 12 Stunden ist es ein verlässlicher Begleiter.
Über das Topo-Kartenmodell lassen sich Kartenkacheln (ca. 70 x 100 Kilometer groß, Gutschein für eine Kartenkachel liegt bei) zielgenau auswählen. Zusätzlich ist das tw700 mit kostenfreien OSM-Karten weltweit nutzbar. Die Gruppennavigation zeigt Positionen aller Gruppenmitglieder an und eröffnet mit vielfältigen Interaktionsmöglichkeiten neue effektive Einsätze.
Das Android-Smartphone unterstützt mobile Unternehmenslösungen, Kommunikation, Datenaustausch und Internetzugang. Das Walkie Talkie ermöglicht die Verständigung, auch dort wo kein Telefonnetz verfügbar ist.

## TASys GmbH — Stand: B 1

Die TASys GmbH unterstützt Firmen in deren SAP und IT- Projekten.
SAP IS-DFPS, SAP A&D, SASPF
Unser umfangreiches Know-how in allen SAP-Modulen und langjährige Erfahrung mit den entsprechenden Strukturen, Prozessen und Aufgaben in Streitkräften und Industrie garantieren eine nachhaltige Ausbildung.
Ausbildung auf den Punkt gebracht beinhaltet bei uns:

- Ausbildungsbedarfsanalysen
- Planung, Konzeption und Organisation der Ausbildung
- Schulungsentwicklung, Dokumentationen
- prozessorientierte und arbeitsplatzbezogene Ausbildungen
- Produktivunterstützung, Coaching am Arbeitsplatz
- mobile Ausbildungseinrichtungen

- Virtualisierung
- Aufbau und Pflege von Schulungssystemlandschaften

Die TASys Akademie in Köln führt folgende Trainings durch: SAP, VMware, Cisco, Microsoft, Adobe, Linux, Typo3, PMI und ITIL.
www.TASys-it.de

## TELEFUNKEN RACOMS — Stand: F 2

TELEFUNKEN RACOMS entwickelt und vertreibt Funkkommunikationssysteme für moderne, sicherheitsrelevante und hochtechnologische Anwendungen. Für die militärische Nutzung steht ein breit gefächertes Angebot an taktischen und strategischen HF-Funksystemen, taktischen VHF-Funkgeräten und "high capacity"- UHF-Richtfunkgeräten zur Verfügung. Diese Systeme sind zu Lande, zu Wasser und in der Luft im Einsatz. Die Kompetenz von TELEFUNKEN RACOMS liegt nicht nur bei der Herstellung von hochperformanter Hardware, sondern auch im Bereich der Softwareentwicklung zur Integration verschiedenartigster Funkübertragungsprotokolle.
Neben dem Kerngeschäft der Funkkommunikation baut TELEFUNKEN RACOMS seine Geschäftstätigkeiten im Verteidigungsbereich (C4, Aufklärung, Schutz, Wirkung) spürbar aus und reagiert somit auf den wachsenden Bedarf der Bundeswehr an zuverlässigen und leistungsstarken Systemen zur Unterstützung der Auftragserfüllung in den Einsatzgebieten.
**Kontakt:** TELEFUNKEN Radio Communication Systems GmbH & Co. KG, Eberhard-Finckh-Str. 55, 89075 Ulm, info@tfk-racoms.com, www.tfk-racoms.com

## Thales Deutschland — Stand: Z 6

Thales Deutschland verfügt über eine hohe Produkt-, System- und Lösungskompetenz und ein umfangreiches Portfolio. Die Produkt-, System- und Lösungshighlights reichen von der Sensorik, insbesondere land- und seegestützten Überwachungsradaren, der Optronik sowie kombinierten Sensorsystemen über abhörsichere Multiband-Truppenfunksysteme bis hin zu komplexen Führungsinforations- und Aufklärungssystemen. Zum Angebot gehören auch taktische Funk- und Führungssysteme für den hochmobilen Einsatz, Software-defined Radio, Kommunikations- und Leitzentralen sowie Feldlagerschutz. Den Schwerpunkt der Marineaktivitäten in Deutschland bilden Über- und Unterwassertechnologien. Bei Führungs- und Waffeneinsatzsystemen für Seestreitkräfte entwickelt Thales sowohl Netzinfrastrukturen als auch Software. Kommunikations- und Ausbildungssysteme, taktische Datenlinks sowie Systeme zur taktischen Aufklärung und Datenauswertung gehören ebenfalls zum Leistungsspektrum. www.thalesgroup.com/germany

## T-Systems International AG — Stand: F 4

**Flexible Informations- und Kommunikationstechnik für die Bundeswehr.**
Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik (engl. kurz ICT) für multinationale Konzerne und öffentliche Institutionen.
**Kompetenter Partner der Bundeswehr.**
T-Systems unterstützt die Bundeswehr als erfahrener Partner für sichere und zuverlässige Lösungen rund um die Kernaufgaben Organisation, Aufklärung, Führung, Logistik und Kommunikation. Dabei liegt die besondere Kompetenz von T-Systems darin, handelsübliche Hard- und Softwarekomponenten so anzupassen, dass sie alle Anforderungen der Bundeswehr hinsichtlich Sicherheit, Echtzeitbetrieb und anderer Einsatzbedingungen erfüllen.
**T-Systems International GmbH**, Am Propsthof 51, 53121 Bonn, Tel.: 0228/181-42677, E-Mail: heiko.thiemann@t-systems.com, Internet: www.t-systems.de

## UWS Business Solutions GmbH — Stand: P 8

Die **UWS Business Solutions GmbH** (bis 2011 als Schneider System GmbH) ist ein unabhängiges, inhabergeführtes, mittelständisches Beratungs- und Dienstleistungsunternehmen und **unterstützt die Bundeswehr partnerschaftlich seit über 20 Jahren.** Wesentliche **Kompetenzen** liegen in den Feldern **Organisationsberatung, IT-Lösungen** und **Qualifizierung.**
**Schlagworte zu UWS-Dienstleistungen** sind:

- Standards wie ISO 9001, ITIL, IT-Service Management, PRINCE2
- Methoden wie eEPK, BPMN, NAV, IT-Architekturen, Projektmanagement
- Verfahren wie Lean Management, CPM, logistische DV-Verfahren
- Techniken und ganzheitliche Ansätze wie ECM, Webportale, BPM Tools
- Innovative Lösungen mit Wiki, Blogs, Social Networking, semantische Netze
- Technologien wie RFID, PHP, MS- und Notes-Entwicklungen
- Bundeswehr-Projekte im Bereich FüInfoSys, LogSys, Fernausbildung

www.uw-s.com

## VEGA Deutschland GmbH — Stand: F 3

VEGA Deutschland ist ein führendes Technologie- und IT-Services Unternehmen. Mit über 200 Mitarbeitern und 30 Jahren Erfahrung in der Realisierung komplexer IT-Projekte unterstützt VEGA ihre Kunden im Verteidigungsbereich bei der Gestaltung und Durchführung von Service-Prozessen in den Bereichen Personalwesen und Infrastruktur.
In diesem Jahr liegt unser Fokus für die AFCEA auf den Themen **e-Recruiting, Secure Server Management und IPv6.**
Umfangreiches Expertenwissen, Prozess-Know-how und hohe Umsetzungskompetenz versetzen uns in die Lage, mit innovativen Lösungen nachhaltig die Leistungsfähigkeit und Zielerreichung unserer Kunden zu optimieren.
**Kontakt:** VEGA Deutschland GmbH, Industriestr. 161, 50999 Köln, Tel: +49 (0)2236 748-0, E-Mail: info@vega-deutschland.de, www.vega-deutschland.de

## ZVEI-Fachverband Sicherheit — Stand: PE 3

Vernetzte Sicherheit ist ohne den Einsatz vorhandener und neuer Sicherheitstechnologien nicht denkbar. Hier liegt die innovative Kraft, die erforderlich ist, um innere und äußere Sicherheit ständig zu optimieren und den Bedrohungen von außen sowie den asymmetrischen Bedrohungen durch Terroristen und sonstigen Gefahren für die innere öffentliche Sicherheit mit intelligenter und innovativer Wehr-, Einsatz- und Sicherheitstechnik zu begegnen.
Der **Fachverband Sicherheit im ZVEI** – Zentralverband Elektrotechnik- und Elektronikindustrie e.V. – bündelt die vielseitigen Kompetenzen der Branche mit den drei Leitmärkte SAFETY (Schutz von Menschenleben, technische Sicherheit von Anlagen und Gebäuden), SECURITY (Schutz von Infrastruktur wie Flughäfen und Energieversorgung, Informationstechnik und Kommunikation sowie Bevölkerungs- und Katastrophenschutz) und DEFENCE (äußere Sicherheit) unter einem Dach.
Nur mit einer Strategie der Vernetzten Sicherheit, bei der politische Institutionen, Konzepte, Strategien und Instrumente der Sicherheitspolitik und des nationalstaatlichen und auch multinationalen Handelns ressortübergreifend abgestimmt, kohärent und koordiniert umgesetzt, wirkungsorientiert und nach Möglichkeit auch präventiv angelegt sind, kann Sicherheit und der Schutz der Gesellschaft in einer zunehmend vernetzten, globalisierten Welt verbessert werden. Sicherheit entwickelt sich vor diesem Hintergrund zu einem maßgeblichen wirtschaftlichen Standortfaktor.

# BSC·Berlin Security Conference

11th Congress on European Security and Defence

## Impressionen 2011


**Weitere Fotos und Informationen zum letzten Kongress finden Sie unter**

**www.euro-defence.eu**

BSC·Berlin Security Conference

11th Congress on European Security and Defence

# Europa und seine Nachbarn – gemeinsame Verantwortung für Stabilität

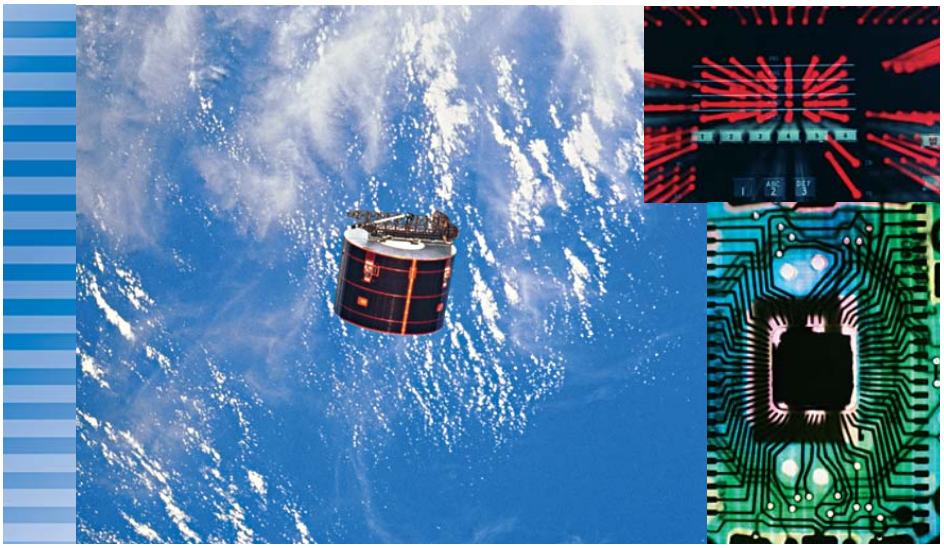
**27. – 28. November 2012**

**andel's Hotel & Convention Center Berlin**

Programm, Anmeldung und mehr Informationen:

**www.euro-defence.eu**

Foto: Bordignon V. Eurocorps



*Vorankündigung:*

# 27. AFCEA-Fachausstellung

# 24./25. April 2013

**www.afcea.de**