39. AFCEA FACHAUSSTELLUNG

World Conference Center Bonn | 12./13. Mai 2026

Der Treffpunkt der IT-Community Bundeswehr und BOS

AFCEA Bonn e.V.

INFOS & THEMEN

PROGRAMM | **INDUSTRIEVORTRÄGE** | AUSSTELLER

Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

2026

Vernetzt denken und sicher Handeln

AFCEA Bonn e.V.

INHALTSVERZEICHNIS

Programm | Industrievorträge

39. AFCEA FACHAUSSTELLUNG
World Conference Center Bonn
12./13. Mai 2026

Inhalt Seite

PROGRAMM

Vorträge der Keynotes und Symposien finden
im ehemaligen Plenarsaal des Bundetages statt

DIENSTAG 12. Mai 2026 **9:00–18:00 Uhr Ausstellung**

9:50 Uhr **Begrüßung/Eröffnung 39. AFCEA Fachausstellung**
Generalmajor Armin G. Fleischmann (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.)

10:00 Uhr **Grußwort Guido Déus**
(Oberbürgermeister der Bundesstadt Bonn)

10:10 Uhr **Keynote General a. D. Jörg Vollmer**

18:00–22:00 Uhr **Get-together AFCEA Fachausstellung 2026**
AFCEA Bonn e.V. lädt Besucher und Aussteller ein zu Kölsch und Snacks auf der **„Rheinebene“** des World Conference Center Bonn

MITTWOCH 13. Mai 2026 **9:00–17:00 Uhr Ausstellung**

10:00–11:00 Uhr **Digital Defense Debate**
Organisation und Moderation: **Emerging Leaders der AFCEA Bonn e. V.**

11:05–12:00 Uhr **Start-up Pitch & Panel Session**
Moderation: **Emerging Leaders der AFCEA Bonn e. V.**
Ablauf: Impulsvortrag (circa 10 Minuten) mit aktuellem Sachstand zur Durchlässigkeit von Innovation in der Bundeswehr
Beginn der Pitch-Session mit 4 Start-ups (2 Minuten Pitch), die anschließend im Rahmen einer Fishbowl-Diskussion von der Jury und interaktiv mit dem Publikum bewertet werden.

14.30 Uhr **Keynote: Brigadegeneral Michael Peter Jäger** (Abteilungsleiter I, BAAINBw)
„Aktuelles aus dem BAAINBw“

14:50 Uhr **Grußwort: Konteradmiral a. D. Massimo Esposito**
(Geschäftsführer AFCEA Europe)

Anschließend **Abschluss Symposium und Schlusswort**
durch **Generalmajor Armin G. Fleischmann** (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.)

17.00 Uhr **Ende der Fachausstellung**

SYMPOSIEN UND INDUSTRIEVORTRÄGE

Übersicht | Zeitplan

12. Mai 2026

	Slot Nr:	incl. Live-Aufzeichnung Plenarsaal Bundestag	Slot Nr:	Vortragssaal ADDIS ABEBA 3
09:00		Eröffnung u. KeyNote 1		
09:30				
10:00				
10:30				
11:00				
11:05–11:30	1	ELBIT	15	:em engineering
11:35–12:00	2	PROSTEP	16	Elma
12:05–12:30	3	Capgemini	17	NVIDIA
12:35–13:00	4	Sophos	18	RUAG
13:05–13:30	5	Scotty	19	Best Systeme
13:35–14:00	6	Deutsche Telekom	20	ARX Robotics
14:05–14:30	7	abat AG	21	]init[
14:35–15:00	8	dainox	22	Willert
15:05–15:30	9	CGI	23	Eraneos
15:35–16:00	10	Data Warehouse	24	Service Now
16:05–16:30	11	Rheinmetall	25	Google
16:35–17:00	12	Plath	26	Safran Germany
17:05–17:30	13	IABG	27	IBM
17:35–18:00	14	Getac	28	Genua

13. Mai 2026

	Slot Nr:	incl. Live-Aufzeichnung Plenarsaal Bundestag	Slot Nr:	Vortragssaal ADDIS ABEBA 3
09:00				
09:30				
10:00		KeyNote 2 Defence-Debate		
10:05–10:30				
10:35–11:00				
11:05–11:30	29	ELA StartUp-Pitches	35	Trend Micro
11:35–12:00	30		36	Thales
12:05–12:30	31	21strategies	37	AIRBUS
12:35–13:00	32	HP Enterprise	38	HAT.tec
13:05–13:30	33	Pexip	39	Materna Virtual
13:35–14:00	34	Motorola	40	rasdaman
14:30		KeyNote 3		
15:00				
15:30				
16:00				
16:30				
17:00		Ende der Fachausstellung 2026		

AFCEA APP

Entdecken Sie die Fachausstellung über unsere **Web-App** mit nur einem Fingertipp.

Mit der Event-Web-App auf Ihrem Homescreen haben Sie **alle Informationen** jederzeit griffbereit.

- Standpläne
- Programm
- Aussteller
- Informationen
- Favoriten

und mehr ...

Scan me

INDUSTRIEVORTRÄGE
sortiert nach Ausstellern

Vortragsthemen und Details auf Folgeseiten (in Reihenfolge der Startzeiten je Saal)

AUSSTELLER	SLOT-NR.	DATUM	UHRZEIT	ORT
:em engeneering	15	12.5.2026	11:05-11:30	Saal „Addis Abeba 3“
]init[	21	12.5.2026	14:05-14:30	Saal „Addis Abeba 3“
21strategies	31	13.5.2026	12:05-12:30	Plenarsaal
abat AG	7	12.5.2026	14:05-14:30	Plenarsaal
Airbus	37	13.5.2026	12:05-12:30	Saal „Addis Abeba 3“
ARX Robotics	20	12.5.2026	13:35-14:00	Saal „Addis Abeba 3“
Best Systeme	19	12.5.2026	13:05-13:30	Saal „Addis Abeba 3“
Capgemini	3	12.5.2026	12:05-12:30	Plenarsaal
CGI	9	12.5.2026	15:05-15:30	Plenarsaal
Dainox	8	12.5.2026	14:35-15:00	Plenarsaal
Data Warehouse	10	12.5.2026	15:35-16:00	Plenarsaal
Detecon	6	12.5.2026	13:35-14:00	Plenarsaal
ELA Digital Defense Debate	29	13.5.2026	11:05-11:30	Plenarsaal
ELA Startup-Pitches	30	13.5.2026	11:35-12:00	Plenarsaal
Elbit	1	12.5.2026	11:05-11:30	Plenarsaal
Elma	16	12.5.2026	11:35-12:00	Saal „Addis Abeba 3“
Eranos	23	12.5.2026	15:05-15:30	Saal „Addis Abeba 3“
Genua	28	12.5.2026	17:35-18:00	Saal „Addis Abeba 3“
Getac	14	12.5.2026	17:35-18:00	Plenarsaal
Google	25	12.5.2026	16:05-16:30	Saal „Addis Abeba 3“
HAT.tec	38	13.5.2026	12:35-13:00	Saal „Addis Abeba 3“
HP Enterprises	32	13.5.2026	12:35-13:00	Plenarsaal
IABG	13	12.5.2026	17:05-17:30	Plenarsaal
IBM	27	12.5.2026	17:05-17:30	Saal „Addis Abeba 3“
Materna Virtual	39	13.5.2026	13:05-13:30	Saal „Addis Abeba 3“
Motorola	34	13.5.2026	13:35-14:00	Plenarsaal
Nvidia	17	12.5.2026	12:05-12:30	Saal „Addis Abeba 3“
Pexip	33	13.5.2026	13:05-13:30	Plenarsaal
Plath	12	12.5.2026	16:35-17:00	Plenarsaal
Prostep	2	12.5.2026	11:35-12:00	Plenarsaal
Rasdaman	40	13.5.2026	13:35-14:00	Saal „Addis Abeba 3“
Rheinmetall	11	12.5.2026	16:05-16:30	Plenarsaal
RUAG	18	12.5.2026	12:35-13:00	Saal „Addis Abeba 3“
Safran Germany	26	12.5.2026	16:35-17:00	Saal „Addis Abeba 3“
Scotty	5	12.5.2026	13:05-13:30	Plenarsaal
ServiceNow	24	12.5.2026	15:35-16:00	Saal „Addis Abeba 3“
Sophos	4	12.5.2026	12:35-13:00	Plenarsaal
Thales	36	13.5.2026	11:35-12:00	Saal „Addis Abeba 3“
Trend Micro	35	13.5.2026	11:05-11:30	Saal „Addis Abeba 3“
Willert	22	12.5.2026	14:35-15:00	Saal „Addis Abeba 3“

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
1	11:05 Uhr	Plenarsaal

Elbit Systems™

ELBIT SYSTEMS DEUTSCHLAND GMBH & CO. KG

Jan Erbe

Digitale Kommunikation im Einsatz

Moderne militärische Operationen sind in hohem Maße von einer leistungsfähigen digitalen Kommunikation abhängig. In hochdynamischen Einsatzszenarien müssen Zielmeldungen innerhalb weniger Sekunden erfasst, bewertet und an das geeignete Wirkmittel übermittelt werden. Diese Anforderungen stellen Kommunikationssysteme vor erhebliche technische und operative Herausforderungen. Bandbreiten- und Latenzbeschränkungen können Echtzeitentscheidungen erheblich beeinträchtigen – insbesondere in umkämpften Einsatzumgebungen, in denen elektronische Kampfführung, Störungen oder infrastrukturelle Einschränkungen auftreten.

Gleichzeitig wächst die Zahl vernetzter Sensoren, Plattformen und Geräte rapide. Die steigende Dichte an Netzwerkknoten erhöht nicht nur die Systemkomplexität, sondern auch die potenzielle Angriffsfläche für Cyberangriffe. Hinzu kommt eine immer stärker verdichtete Spektrumsnutzung: Mehrere Kommunikationsnetze im selben geografischen Raum führen zu Interferenzen, Frequenzkonflikten und erschweren eine effiziente Nutzung begrenzter Funkressourcen. Vor diesem Hintergrund zeigt der Beitrag, wie moderne Funk- und Kommunikationsarchitekturen diesen Herausforderungen begegnen können. Mit jahrzehntelanger Erfahrung in Kurzwellenkommunikation, adaptiven Funklösungen sowie modernen Routing-Architekturen stellt Elbit Systems Deutschland resiliente und sichere Kommunikationssysteme für anspruchsvolle Einsatzumgebungen zur Verfügung. Die Technologien – von leistungsfähigen Funkgeräten über Kommunikationsserver bis hin zu spezialisierten Modems – stehen „off the shelf“ zur Verfügung. Als Technologiepartner kombiniert das Unternehmen globale Innovationskraft mit Entwicklung, Fertigung und Support „Made in Germany“, um leistungsfähige Kommunikationslösungen für die Anforderungen der Bundeswehr bereitzustellen.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
2	11:35 Uhr	Plenarsaal

PROSTEP integrate the future

PROSTEP GRUPPE

Martin Holland

Von der Anforderung zur Einsatzreife: Beschleunigung von Verteidigungsprogrammen durch Digital Engineering, Digital Thread und das Konzept Digital Twin

Wie bringen wir Verteidigungsprogramme bei wachsender Systemkomplexität schneller, sicherer und nachvollziehbar in die Einsatzreife? Der Vortrag zeigt, wie integriertes Digital Engineering, ein gelebter Digital Thread und Digitale Zwillinge genau das ermöglichen.

Organisationen stehen vor der Herausforderung, steigende Systemkomplexität, Interoperabilitäts- und Sicherheitsanforderungen sowie Nachweis- und Compliance-Pflichten zu beherrschen und heterogene Systemwelten zu integrieren.

Dieser praxisorientierte Vortrag vermittelt Erfahrungen aus internationalen Programmen, in denen offene Architekturen und kollaborative Lifecycle-Ansätze erfolgreich umgesetzt wurden. Es wird gezeigt:

> wie der DoD Modular Open Systems Approach (MOSA) genutzt wird, um Integrated Digital Environments (IDE) aufzubauen und Datenintegrität über den gesamten Produktlebenszyklus sicherzustellen;

> wie im Sinne der DoD Digital Engineering Strategy (DoDI 5000.97) ein „Digital Thread" aufgebaut wird, um kritische Informationen – beginnend bei Anforderungen entlang des Systems-Engineering-V-Modells – über alle Lebenszyklusphasen hinweg zu verknüpfen und so eine hohe Datenintegrität und Konsistenz sicherzustellen.

> wie Digitale Zwillinge als Basis für Lebenszyklustransparenz dienen und Use Cases wie vorausschauende Instandhaltung (Predictive Maintenance) sowie erhöhte Einsatzbereitschaft (Mission Readiness) ermöglichen können.

Der Vortrag vermittelt konkrete Einblicke, wie nachhaltige Digital-Engineering-Umgebungen aufgebaut und Joint-Venture-Kooperationen wirksamer gestaltet werden können, um Resilienz und Wettbewerbsfähigkeit in Verteidigungsprogrammen zu steigern.

Mit mehr als 30 Jahren Erfahrung in Enterprise Architecture Management (EAM), Product Lifecycle Management (PLM) und Application Lifecycle Management (ALM) unterstützt die PROSTEP Gruppe Regierungen, Industrie und Joint Ventures dabei, digitale Strategien in operative Fähigkeiten zu übersetzen – vom Konzept bis zum wirksamen Betrieb.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
3	12:05 Uhr	Plenarsaal

CAPGEMINI DEUTSCHLAND GMBH

Marc Akkermann (Vice President, Head of Public Defense, Capgemini Deutschland)
Christopher Gaube (Country Lead Defense, Capgemini Deutschland)

Code over Steel: Der entscheidende Hebel für Fähigkeitsaufbau bis 2030

Um den Anforderungen einer gesamtstaatlichen Verteidigung gerecht zu werden, müssen Fähigkeiten nicht nur schneller, sondern vor allem softwarezentriert entwickelt und betrieben werden. Während Hardware weiterhin essenziell bleibt, entscheidet künftig die Geschwindigkeit, mit der softwarebasierte Fähigkeiten an neue Lagen, Bedrohungen und Einsatzumfänge angepasst werden kann. Ein verkürzter „Soldier Feedback Loop" – also die unmittelbare Rückkopplung operativer Nutzer in die Weiterentwicklung – wird damit zum zentralen Erfolgsfaktor moderner Fähigkeitsentwicklung für unsere Streitkräfte.

Wir zeigen, wie Software Defined Defense diesen Ansatz bereits heute ermöglicht: durch digitalisierte Wertschöpfungsketten, ein Cloud Kontinuum bis in die letzte Meile, souveräne Software-Factories und den sicheren Einsatz von KI. Capgemini bringt dafür die Verbindung aus tiefem Software Engineering, Hardware Verständnis und Beratungs Expertise mit – sowie jahrzehntelangen Erfahrungen aus anderen Industrien, in denen agile, datengetriebene Entwicklungsmodelle längst Standard sind.

So unterstützen wir sowohl öffentliche Organisationen im Geschäftsbereich des BMVg als auch die Defense Industrie dabei, Fähigkeitsentwicklung zu beschleunigen, Interoperabilität zu verbessern und die Zusammenarbeit zwischen staatlichen Akteuren und Industriepartnern nachhaltig zu stärken.

Weil Software künftig über Einsatzfähigkeit entscheidet. Im Vortrag zeigen wir, wie der Soldier Feedback Loop verkürzt, Fähigkeiten softwarezentriert entwickelt und die Zusammenarbeit zwischen Bundeswehr und Industrie beschleunigt werden kann. Wer Software Defined Defense verstehen will, muss hier dabei sein.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
4	12:35 Uhr	Plenarsaal

SOPHOS TECHNOLOGY GMBH

Marcel Bornhöfft

Cyberlage 2026: Aktuelle Bedrohungen und Wege zu belastbarer Cyber Resilienz

In dieser Präsentation wird die sich wandelnde Cybersecurity Landschaft aus einer strategischen Perspektive beleuchtet und aufgezeigt, wie dynamische Bedrohungen das organisatorische Risiko zunehmend prägen.

Der Vortrag zeichnet ein klares, übergeordnetes Lagebild der Bedrohungslandschaft und zeigt auf, welche Schritte erforderlich sind, um den Wandel von einer überwiegend reaktiven Sicherheitsorganisation hin zu einem proaktiven, resilienten und durchgängig risikoorientierten Ansatz zu vollziehen.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
6	13:35 Uhr	Plenarsaal

DEUTSCHE TELEKOM GESCHÄFTSKUNDEN GMBH

Dr. Nico Feller | Frank Rauschenbach

Digitale Souveränität sichern: Wehrtaugliche IT-Architekturen 2035

Digitale Souveränität ist keine technologische Option mehr, sondern eine strategische Notwendigkeit. Sicherheitskritische Organisationen stehen vor der Grundsatzfrage, wie ihre IT-Architekturen gestaltet sein müssen, um Einsatzfähigkeit, Resilienz und Handlungsfreiheit dauerhaft zu gewährleisten – und zugleich gewachsene Legacy-Strukturen abzulösen.

Wehrtaugliche IT-Architekturen 2035 erfordern neu gedachte Prozesse, Plattformen und Governance-Modelle. Im Fokus stehen robuste, souveräne und interoperable Systeme, die flexibel modernisierbar sind, prozessual sauber verankert und organisatorisch nachhaltig betreibbar. Entscheidend ist dabei nicht nur die Technologie, sondern das Zusammenspiel aus hochsicheren Plattformen, klar definierten Architekturprinzipien, verbindlichen Standards und einer belastbaren Governance-Struktur.

Die Defense Cloud wirkt in diesem Kontext nicht als isoliertes Infrastrukturprojekt, sondern als strategischer Enabler für eine integrierte, zukunftsfähige IT-Landschaft. Dieser Vortrag zeigt, wie sicherheitskritische Organisationen Komplexität reduzieren, Legacy-Systeme schrittweise transformieren und durch konsistente Architektur- und Governance-Ansätze langfristige Souveränität erreichen. Im Mittelpunkt steht die strategische Neuausrichtung der Enterprise IT – mit einem realistischen Transformationspfad bis 2035.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
5	13:05 Uhr	Plenarsaal

SCOTTY GROUP AUSTRIA GMBH

Dr. Joachim Kalcher (CEO)

Secure Communication

Scotty ist eine Technologieplattform für sichere, zuverlässige und hochverfügbare Kommunikation in sicherheitskritischen Umgebungen. Das System wird von zivilen und militärischen Organisationen weltweit genutzt, um unter allen Umständen Informationen auszutauschen und ein gemeinsames Lagebild zu schaffen. Das Hauptziel von Scotty ist es, Informations- und Kommunikationssysteme bereitzustellen, die auch unter schwierigen Bedingungen funktionieren. Dabei können Daten über Kabel-, Funk- oder Satellitennetzwerke übertragen werden und sind für Einsätze an Land, auf See und in der Luft geeignet.

Ein zentrales Element ist das gemeinsame Lagebild (Common Operational Picture – COP). Dieses ermöglicht es Entscheidungsträgern, Informationen aus verschiedenen Quellen – etwa Kameras, Sensoren oder Einsatzkräften – zusammenzuführen und in Echtzeit auszuwerten. Dadurch können schneller fundierte Entscheidungen getroffen werden.

Wichtige Produkte und Technologien

1. Scotty Extended Connect: Echtzeit-Kommunikation zwischen Einsatzkräften und Entscheidern/Integration von Video- und Datenströmen über verschiedene Netzwerke

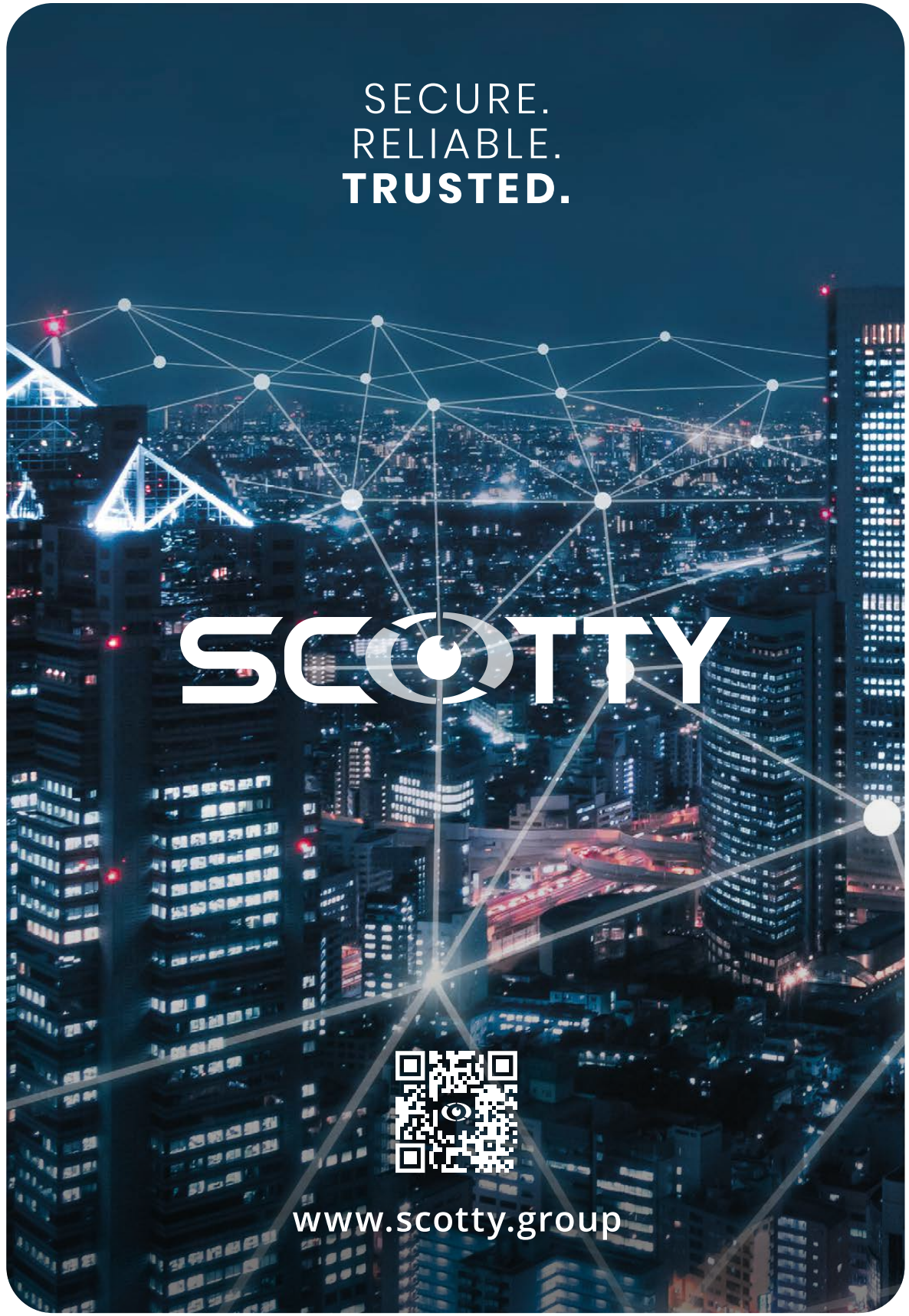
2. Scotty Multimodal Connectivity: Resiliente Netzwerke mit redundanten Knoten/Automatische Übernahme bei Ausfall einzelner Komponenten

3. Scotty Una Omnia: Modulares Kommunikationssystem/Anpassbar mit Komponenten wie Video-Codecs, Funkmodulen, Netzwerk-Switches oder CPU-Boards

4. Scotty Video Conference: Sichere Videokonferenzlösungen für klassifizierte Umgebungen/Kommunikation bis zur Sicherheitsstufe „NATO-geheim“ möglich

5. Scotty Secure End-Point: Sichere Endgeräte für Daten-, Video- und Sprachkommunikation/Verschlüsselte Netzwerkanbindung und Integration von Sensoren oder Kameras

6. Scotty Silentio: Abhörsichere Besprechungsräume („Raum-im-Raum“)/Schutz vor akustischen und elektromagnetischen Abhörversuchen



Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
7	14:05 Uhr	Plenarsaal

ABAT AG

Karsten Schmidt (Senior Consultant) | Martin Schönborn

Resiliente Lieferketten – robuste, IT-gestützte Prozesse für verteidigungsfähige Logistik

Die stark gestiegenen Bedarfe an Rüstungsgütern sowie der politische Fokus auf die Wehrhaftigkeit der NATO stellen Streitkräfte, Infrastrukturbetreiber und die Rüstungsindustrie vor neue Herausforderungen. Produktions-, Lager- und Transportkapazitäten müssen kurzfristig skaliert werden, bei gleichzeitigem Aufbau resilienter Supply Chains im Defence-Umfeld.

In diesem Vortrag befassen wir uns mit Erkenntnissen und Standards von bewährten und gestützten Prozessen für das Supply Chain Management aus der Automobilindustrie und leiten hieraus konkrete Handlungsfelder für Rüstungsindustrie und Streitkräfte ab. Dabei werden die spezifischen Anforderungen, Eigenschaften und Voraussetzungen der Bundeswehr und ihrer Ausrüster berücksichtigt.

Im SAP-Kontext haben sich unternehmensübergreifende Echtzeittransparenz, belastbare Prognosemodelle und eine hohe Datenqualität entlang von Produktion, Instandhaltung sowie Intra- und Interlogistik als zentrale Erfolgsfaktoren für resiliente Supply Chains etabliert.

Der gezielte und maßgeschneiderte Transfer dieser bewährten Automotive-Ansätze in den Defence-Bereich ermöglicht eine nachhaltige Stärkung der Versorgungssicherheit – insbesondere durch verbesserte Planbarkeit, höhere Reaktionsgeschwindigkeit und erhöhte Robustheit gegenüber Störungen.

Im Rahmen dieses Vortrags stellen wir konkrete Erfahrungen aus SAP-Projekten im Automotive- und Defence-Umfeld vor und zeigen anhand praxisnaher Beispiele, wie sich diese Ansätze erfolgreich auf die Verteidigungslogistik übertragen lassen – mit messbarem Beitrag zur Versorgungssicherheit und Resilienz militärischer Supply Chains.

Neben den zentralen Aufgaben hinsichtlich der physischen Infrastruktur sind wir davon überzeugt, dass resiliente Supply Chains auch auf schnelle, korrekte und lieferkettenübergreifende Informationsflüsse angewiesen sind.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
8	14:35 Uhr	Plenarsaal

DAINOX GMBH

Dipl.-Inf. (FH) Bernd Kohler | Dr. Artavazd Tarhanjan | Dr. Christopher Metter

Vernetzungsfähigkeit im Einsatzgebiet aufs Neue definieren und differenzieren

In unserem Vortrag werden die aktuellen, qualitativen und quantitativen Herausforderungen der netzwerk-technischen Protokollwelt im Einsatzgebiet zum Erlangen der Vernetzungsfähigkeit sowie der aufgewerteten Resilienz im Einklang mit den multinationalen Vorgaben wie FMN vorgestellt, analysiert und evaluiert.

Für die Auswahl der Evaluierungskriterien ist es unerlässlich, ähnliche Fragestellungen zu einer robusten IP-Vernetzung beziehungsweise Eigenschaften der sogenannten Mobilen Ad-hoc Netzwerke (MANET) einzubeziehen. Trotz aller Unterschiede und Spezifika zu der militärischen Soll-Lösung sind vor allem zwei Ausprägungen von MANETs, namentlich VANETs (Vehicular Ad-hoc Networks) und FANETs (Flying Ad-hoc Networks), methodologisch und technologisch von Interesse, da sie wohlbekannte Anforderungen wie Dezentralität (Selbstorganisation), Mobilität (kontinuierliche Veränderung der Topologie) und Multi-Hop-Kommunikation berücksichtigen.

Im Fokus unserer Analyse stehen die militärische Vehicle-to-Vehicle (V2V) und Vehicle-to-Facility (V2F) Kommunikation auf IP-Basis, sowohl im Stand („Static, Parked Vehicle“) als auch in Bewegung („Mobile, At-The-Halt“). Die zentrale Herausforderung bei Verwendung dieser dynamischen und adaptiven Netzwerk-Topologien ist das Erreichen von konkreten Stabilitätsgrenzen zur Erfüllung der funktionell und technisch gestiegenen Leistungsansprüchen der IP-Kommunikation.

Durch mathematische Simulation (Warteschlangentheorie und Markov-Ketten) zeigen wir auf, dass eine allgemeingültige Patentlösung nicht existiert und nur einsatzspezifische Lösungsansätze erfolgsversprechend sind. Ferner ist die Anbindung an die zentralen HQ im Einsatzgebiet (V2F) unter den Beschränkungen durch den Vermaschungsgrad ein zentraler Einflussfaktor für die Fahrzeugdichte. Um diesen Herausforderungen zu begegnen, werden auch Lösungsansätze wie spezielle Planungsregeln zur Steuerung der IP-Lastweiterleitung (Software-defined Control, Forwarding & Management Planes) adressiert.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
10	15:35 Uhr	Plenarsaal

DATA-WAREHOUSE GMBH

Dr. Alexander Löw (CEO)

Post Quantum – Internationaler Status, Handlungsempfehlungen und Lessons Learned für Defence und Sicherheit

Neben KI is Quantum Computing mit seinen Randbereichen Post Quantum und Quantum Security im Betrieb und in der Regulierung angekommen. Weltweit bereiten sich die Unternehmen und Behörden auf dieses Thema vor. Weshalb wird dieses Thema so dringlich?

Der Vortragende beantwortet die drängenden Fragen zu diesem Thema gibt einen internationalen Überblick über den aktuellen Status im Bereich Post Quantum.

Anhand der aktiven internationalen Mitarbeit in Gremien wie der Post Quantum Migration Working Group des US NIST, im National Cybersecurity Center of Excellence, der Mitarbeit im PKI Consortium (eine internationale Non-Profit Organisation der Hersteller und Unternehmen im Bereich PKI und Kryptografie) werden Anregungen zur Optimierung der aktuellen Vorgehensweise gegeben.

Darüber hinaus werden Vorschläge für militärische Nutzer zur empfohlenen Vorgehensweise mit Handlungsempfehlungen und den Vor- und Nachteilen aus Projekten mit internationalen Organisationen gemacht.

Beispiele aus existierenden Projekten runden den Vortrag ab.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
9	15:05 Uhr	Plenarsaal

CGI DEUTSCHLAND B.V. & CO. KG

Jens Elstermeier (Vice-President Consulting Expert,
Head of Business Development & Strategy, Defense & Intelligence)

Organisationsübergreifende sichere Kommunikation: Wie HERMES als NATO-Projekt zur Resilienz und Gesamtverteidigung in Deutschland beiträgt

Im Rahmen der gesamtstaatlichen Verteidigung sind die digitale Souveränität und Mobilität militärischer Führungskräfte unverzichtbar. Das NATO-Projekt HERMES markiert hierbei eine strategische Abkehr von der rein standortgebundenen Kommunikation: Es ermöglicht der NATO-Kommandostruktur erstmals, orts- und zeitunabhängig auf hochsichere digitale Arbeitsumgebungen zuzugreifen, ohne Kompromisse beim Schutzniveau einzugehen.

Das Projekt trägt maßgeblich zur Resilienz bei, da es die Managed-Services-Expertise von CGI mit der bewährten SINA-Technologie vereint. Durch ein dediziertes Service Operation Center inklusive permanentem Monitoring und einem Ende-zu-Ende-gesicherten VPN stellt CGI eine durchgängige Führungsfähigkeit auch unter dynamischen Einsatzbedingungen sicher. Diese Innovation, die aus NRW heraus realisiert wurde, schließt die kritische Lücke zwischen höchster Sicherheitsarchitektur und mobiler Flexibilität. Damit leistet sie einen entscheidenden Beitrag zur technologischen Souveränität und zur globalen Reaktionsfähigkeit der NATO.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
11	16:05 Uhr	Plenarsaal

RHEINMETALL

RHEINMETALL

Dr. Timo Haas (CEO Rheinmetall Electronics GmbH, CDO Rheinmetall AG)

Battlespace Dominance is Digital – Sensor-to-Shooter Ketten im Realitätscheck

Die Digitalisierung moderner Streitkräfte wird häufig anhand eines einfachen und eingängigen Modells beschrieben: Der Sensor-to-Shooter-Kette. Sensoren erfassen Informationen, diese werden über Netzwerke verteilt, ausgewertet und führen schließlich zur Wirkung durch einen Effektor. In der Realität jedoch zeigt sich, dass genau diese Wirkungskette häufig an praktischen Herausforderungen scheitert.

Heterogene Systemlandschaften, proprietäre Schnittstellen und fehlende Interoperabilität zwischen Plattformen unterschiedlicher Hersteller erschweren die schnelle und zuverlässige Integration von Sensoren, Entscheidungsunterstützung und Effektoren. Gerade in hochdynamischen Einsatzszenarien führt dies zu Verzögerungen, Medienbrüchen und eingeschränkter operativer Wirksamkeit.

Der Vortrag zeigt auf, warum klassische „Kill Chain"-Modelle in der Praxis häufig an ihre Grenzen stoßen und weshalb moderne Gefechtsführung zunehmend softwarezentriert gedacht werden muss. Anhand konkreter Beispiele wird erläutert, wie offene und modulare Softwarearchitekturen einen entscheidenden Beitrag zur Integration komplexer Systemlandschaften leisten und dabei die Geschwindigkeit, Resilienz und Wirksamkeit moderne militärischer Operationen entscheidend erhöhen.

Im Mittelpunkt steht dabei Rheinmetalls Ansatz zur Orchestrierung der Sensor-to-Shooter-Kette durch eine offene Softwareplattform. Mit der Battlesuite und dem Tactical Core stellt Rheinmetall zentrale Softwarebausteine bereit, die als Integrations- und Orchestrierungsschicht zwischen Sensoren, Führungs- und Waffensystemen fungieren. Durch standardisierte Schnittstellen und die Einbindung von Partnerlösungen entsteht ein offenes Defence-Ökosystem, das eine flexible und skalierbare Integration unterschiedlicher Fähigkeiten ermöglicht.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
12	16:35 Uhr	Plenarsaal

PLATH GMBH & CO KG

Jakob Purrucker (Director Sales) | Sven Luettich (Head of Technology & Innovations)

Closing the gap – Meshed Unmanned EW Core

Im Kontext vernetzter militärischer Anwendungen gewinnt die passive Erkennung von Bedrohungen aus der Luft, insbesondere durch unbemannte Systeme und Flugkörper, zunehmend an Bedeutung. Angesichts der sich rasant entwickelnden Technologien im Bereich unbemannter Luftfahrzeuge (UAVs) und deren Anwendung in militärischen Konflikten, stellt sich die Frage, wie die effektive Überwachung und Gefahrenfrüherkennung optimiert werden kann. Der Vortrag „Closing the Gap – Meshed Unmanned EW Core" beleuchtet, wie durch die Integration von vernetzten, kleineren Aufklärungssystemen eine signifikante Reichweitenerhöhung und eine gezieltere Bedrohungsanalyse möglich sind.

Ein zentrales Konzept hierbei ist die Ergänzung oder Vernetzung bestehender aktiv Radarsysteme durch passive Aufklärungssystem, die es ermöglicht, Bedrohungen wie Drohnen oder feindliche Flugkörper zu erkennen, noch bevor eigene aktive elektromagnetische Signale versendet werden müssen. Dies bietet den Vorteil, dass die eigenen Systeme weniger angreifbar und schwerer zu orten sind. Durch den Einsatz eines „meshed" Netzwerks von kleinen, unbemannten Aufklärungseinheiten – sogenannte „Kleinstsysteme" – kann ein dynamisches und flächendeckendes Frühwarnsystem geschaffen werden, das auch in schwierigen, stark kontaminierten elektromagnetischen Umgebungen zuverlässig arbeitet.

Diese vernetzten Systeme arbeiten miteinander, um ihre Sensoren und Daten in Echtzeit auszutauschen, wodurch eine höhere Genauigkeit und Reichweite bei der Erkennung von Gefahren erzielt wird. Ein solches System ermöglicht es, nicht nur nahbereichsbezogene Bedrohungen frühzeitig zu identifizieren, sondern auch eine Erweiterung des Erfassungsradius über größere Entfernungen hinweg. Besonders bei der Drohnenabwehr oder der Bekämpfung von Luft-Boden-Raketen spielt die Integration solcher Netzwerke eine entscheidende Rolle.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
13	17:05 Uhr	Plenarsaal

IABG MBH

Maik Holzhey

Open-Source-Software (OSS) allein reicht nicht für digitale Souveränität!

Im Kontext der Bundeswehr setzt digitale Souveränität funktionierenden Wettbewerb auch mit Open-Source-Software voraus. Dieser beruht auf drei Säulen: einer breiten, internationalen Entwickler-Community, einer idealerweise unabhängigen Verwaltung der Urheberrechte (IPR) sowie einer vielfältigen staatlichen und privaten Finanzierung zur Sicherstellung einer unabhängigen Weiterentwicklung.

Neue Modelle der Vertragsgestaltung könnten dazu beitragen, das Spannungsfeld zwischen den komplexen Anforderungen der öffentlichen Beschaffung und den Interessen der Industrieorganisationen aufzulösen. Neben der Akzeptanz von Open-Source-Software (OSS) stellen faktische Abhängigkeiten eine zentrale Herausforderung dar. OSS-Lizenzen sollen fairen Wettbewerb ermöglichen, unterschiedliche Geschäftsmodelle zulassen und eine klare individuelle Wertschöpfung abbilden; der Trend geht dabei in Richtung permissiver Lizenzmodelle.

Der Vortrag orientiert sich an drei Leitfragen: Erstens, wer hält die Rechte an OSS? Während häufig unabhängige Organisationen als Rechteinhaber fungieren, zeigen Beispiele unternehmensgetragener Projekte Risiken durch Lizenzänderungen und daraus resultierende Community-Forks. Eine OSS-Lizenz allein garantiert keine unabhängige IPR-Struktur. Zweitens, wer trägt zu OSS bei? Der Open Source Contributor Index zeigt eine starke Dominanz nicht-europäischer Unternehmen, die Ausrichtung und Entwicklung der Projekte prägt. Drittens, wer finanziert die Entwicklung? Oft ist die Finanzierung stark konzentriert und bedingt dadurch faktische Abhängigkeiten.

Zusammenfassend ist Open Source notwendig, aber nicht hinreichend für digitale Souveränität, da Konzentrationen bei Rechten, Beiträgen und Finanzierung Wettbewerb und Unabhängigkeit beeinträchtigen können.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
14	17:35 Uhr	Plenarsaal

GETAC TECHNOLOGY GMBH

Stefan Döpp

Vom Soldaten zum Systemknoten: Digitale Befähigung des modernen Infanteristen

Moderne Operationen erfordern eine nahtlose Integration abgesessener Kräfte in vernetzte Führungs- und Informationssysteme. Der einzelne Infanterist entwickelt sich dabei zunehmend vom isolierten Missionsteilnehmer zu einem digitalen Systemknoten. Voraussetzung hierfür ist ein robuster, sicherer und jederzeit verfügbarer Zugang zu Lageinformationen, Sensorik und Kommunikationsnetzen. Diese digitale Befähigung wird durch widerstandsfähige robuste mobile Getac Computinglösungen ermöglicht.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
15	11:05 Uhr	Saal „Addis Abeba 3“

:EM ENGINEERING METHODS AG

Dr. Markus Krastel

Zukunftsorientierte IT-Architekturen für die Digitale Durchgängigkeit – von Model Based Engineering zum Digital Twin

Eine moderne, zukunftsorientierte IT-Architektur muss die vorherrschende Produktkomplexität im Product Lifecycle Management (PLM) ganzheitlich und durchgängig in Vertrieb, Entwicklung, Fertigung, Service und Betrieb adressieren. Nur durch konsistente, bereichsübergreifende Informationsflüsse können Unternehmen die steigenden Anforderungen mechatronischer und softwaredefinierter Produkte beherrschen.

Eine der zentralen Herausforderungen besteht darin, Produktarchitekturen, Varianten und Konfigurationen über den gesamten Lebenszyklus hinweg konsistent zu managen. PLM- (Product Lifecycle Management) und ALM-Systeme (Application Lifecycle Management) sind dabei häufig wenig integriert, was zu Medienbrüchen, redundanten Workarounds, mangelnder Datenqualität und begrenzter Skalierbarkeit führt.

Model-Based Engineering (MBE) und Model-Based Systems Engineering (MBSE) bieten wirkungsvolle Ansätze, um komplexe Anforderungen, Systemverhalten und Entwicklungsziele strukturiert zu erfassen. Durch die modellbasierten Beschreibungen lassen sich Entwicklungszeiten verkürzen, Wiederverwendung steigern und Kosten reduzieren. Dennoch fehlt in vielen Unternehmen eine durchgängige digitale Konsistenz zwischen Systemmodellen, Produktdaten, Stücklisten, Softwareversionen und den tatsächlichen Konfigurationsentscheidungen im Projekt.

Um den Digitalen Zwilling als digitale Repräsentation eines einzigen individuellen Produkts inkl. seiner Software zu realisieren, sind offene, vernetzte und modulare IT-Landschaften für nahtlose Informationsflüsse erforderlich. Der Einsatz von KI im Entwicklungsumfeld kann nur dann nachhaltig erfolgreich sein, wenn die zugrunde liegende Datenqualität jederzeit gewährleistet ist und damit keine Halluzinationen entstehen.

Die Präsentation zeigt anhand konkreter Praxisbeispiele, wie ein ALM/PLM-Framework ausgestaltet werden kann, dass die digitale Durchgängigkeit zur Realisierung eines Digitalen Zwillings unterstützt.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
16	11:35 Uhr	Saal „Addis Abeba 3“

ELMA ELECTRONIC

Christian Marez | Aksel Saltuklar

Unlocking the Potential of VNX+: High-Performance Embedded Computing for Next-Generation Defense Systems

The growing demand for real-time data processing, artificial intelligence, and advanced signal processing is fundamentally changing the requirements for modern defense platforms. Systems such as aircraft, unmanned platforms, and guided munitions increasingly require high computing performance while operating under strict constraints in size, weight, power consumption, and environmental resilience.

VNX+ technology, based on the VITA-90 standard, enables high-performance computing in an extremely compact and modular form factor. This allows powerful embedded computing solutions to be deployed in applications where traditional platforms were previously too large or too power intensive.

This presentation explores the potential of VNX+ and highlights how it enables new possibilities across a wide range of defense applications—from test and development systems to integration into highly size-constrained platforms such as rockets or airborne systems. Applications including AI inference, sensor fusion, and high-speed signal processing can be implemented directly at the system level while maintaining modularity and standardization.

Through the collaboration of Elma Electronic GmbH and Adlink GmbH, key challenges associated with deploying high-density computing systems in demanding environments are addressed. Advanced cooling concepts and rugged system architectures enable reliable operation even under extreme conditions. Beyond defense applications, this technology also offers significant potential for industries such as industrial automation, railway systems, and healthcare.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
17	12:05 Uhr	Saal „Addis Abeba 3“

NVIDIA GMBH

Michael Frings (Federal & Defense Lead)

Anwendung und Betrieb agentischer KI für die Verarbeitung klassifizierter Daten

Die Nutzung von Agentic AI und Retrieval-Augmented Generation (RAG) markiert einen Wendepunkt für Organisationen in klassifizierten Domänen. Diese Technologien ermöglichen es, komplexe Analysen zu automatisieren und über isolierte Datensilos hinweg fundierte Entscheidungen zu treffen. Der Einsatz in Hochsicherheitsbereichen erfordert jedoch Architekturen, die über herkömmliche On-Premises-Lösungen hinausgehen und strikte Anforderungen an digitale Souveränität, hardwarebasierte Isolation und zertifizierte Sicherheit erfüllen.Ein moderner Ansatz für souveräne KI-Anwendungen basiert auf einer tief integrierten Infrastruktur, die Sicherheit und Performance vereint:

Zertifizierte Sicherheitsarchitektur: Durch den Einsatz von NVIDIA BlueField-3 DPUs wird eine kryptografische Domänentrennung direkt auf Hardware-Ebene realisiert. Dieser „Zero Trust DPU Mode“ stellt sicher, dass selbst administratives Personal keinen Zugriff auf Klartextdaten hat und interne Bedrohungen effektiv minimiert werden.

Souveräne Infrastruktur: Eine schlüsselfertige Air-Gapped Private Cloud bildet das Fundament für den Betrieb ohne externe Netzwerkabhängigkeiten. Dies garantiert die volle Kontrolle über Daten, Modelle und Compliance-Vorgaben.

Optimierte lokale Inferenz: Mit Technologien wie NVIDIA NIM werden modernste KI-Modelle als containerisierte Mikroservices bereitgestellt. Die Inferenz erfolgt vollständig lokal und hardwarebeschleunigt, wodurch sichergestellt wird, dass klassifizierte Informationen den geschützten Raum niemals verlassen.

Modulare KI-Orchestrierung: Plattformen wie deepset Haystack fungieren als Steuerungsebene für den Aufbau und die Governance von Agenten-Systemen. Sie ermöglichen die Erstellung flexibler Pipelines für Aufgaben wie Dokumentenanalyse oder Krisenmanagement.

In der Praxis ermöglichen solche Systeme den Einsatz spezialisierter KI-Entscheidungsagenten. Diese arbeiten parallel als Interaktions-, Bewertungs- oder Beobachtungsinstanzen.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
18	12:35 Uhr	Saal „Addis Abeba 3“

RUAG AG

Christian Schlatter (Productmanager TaCom)

Resiliente Kommunikation für den „Tactical Edge“

Die moderne Gefechtsführung erfordert einen nahtlosen Informationsaustausch zwischen Führungsebenen, Sensoren und Effektoren – unabhängig von der verfügbaren Trägerinfrastruktur. Die dafür notwendige Digitalisierung der Kommunikation bis in den taktischen Edge sowie die damit verbundene technische Komplexität stellen eine besondere Herausforderung dar.

Dieser Vortrag beleuchtet am Beispiel des neuen mobilen Richtfunknetzwerks der Schweizer Armee, wie mit moderner All-IP-Technologie in Verbindung mit einem hohen Automatisierungsgrad die Digitalisierung des taktischen Edge erfolgreich gemeistert werden kann. Im Mittelpunkt steht der Einsatz spezieller Routing-Protokolle für die automatisierte und sichere Vernetzung heterogener taktischer Übertragungswege – von Funknetzen (CNR/SDR) über terrestrische Mobilfunknetze (5G) bis hin zu satellitengestützter Kommunikation (SATCOM).

Besonderes Augenmerk gilt dabei der einfachen Bedienung durch die Truppe. Es wird gezeigt, wie durch intelligente Systemarchitekturen und weitgehende Automatisierung die Inbetriebnahme, Überwachung und Wartung taktischer Kommunikationssysteme deutlich vereinfacht werden – sodass sich die Soldaten auf ihre Kernaufgaben konzentrieren können, anstatt komplexe Netzwerkkonfigurationen vornehmen zu müssen.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
19	13:05 Uhr	Saal „Addis Abeba 3“

BEST SYSTEME GMBH

Dipl.-Ing. (FH) Scharel Clemens (Leiter Entwicklung)

Don’t Panic: A Small Company’s Guide to Airworthiness

Warum Airworthiness für kleine Unternehmen kein Hindernis sein muss.

Die Anpassung eines hoch-performanten Netzwerk-Switches für den Einsatz in der Luftfahrt bringt besondere Herausforderungen mit sich, insbesondere wenn das Produkt die Umweltqualifikation nach RTCA DO-160G bestehen muss. Für kleine Unternehmen bedeutet dies nicht nur, das Produkt zu entwickeln, sondern gleichzeitig ein tiefes Verständnis für die vielschichtigen Testkategorien, Grenzwerte und Nachweisstrategien aufzubauen.

Dieser Vortrag beschreibt die Lessons Learned aus einem realen Projekt und zeigt, wie ein kleines Team die Anforderungen der relevanten DO-160-Abschnitte – von Temperatur- und Vibrationsumgebung über Stromversorgungsqualität bis zu Emissionen und Suszeptibilitäten – systematisch adressiert hat.

Welche Entscheidungen sich als besonders effektiv erwiesen haben, wo iterative Hardware- und Software-Anpassungen notwendig wurden und wie man trotz begrenzter Ressourcen eine saubere Prüfplanung, klare Testabdeckung und robuste Nachweisführung erreicht zeigt dieser Erfahrungsbericht.

Ziel des Beitrags ist es zu zeigen, dass auch kleine Unternehmen komplexe Elektronikprodukte – auch als Klein-Serie – erfolgreich zur Luftfahrttauglichkeit führen können – mit strukturiertem Vorgehen, technischem Pragmatismus und einem klaren Verständnis für die Wechselwirkungen zwischen Design und Umweltanforderungen.

Don’t panic: Airworthiness ist machbar!

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
20	13:35 Uhr	Saal „Addis Abeba 3“

ARX ROBOTICS

Julia Knittlmeier

UGVs als Enabler im Aufklärungs- und Wirkverbund

Ausgangslage und Relevanz: Das Gefechtsfeld der Zukunft ist über alle Domänen vernetzt, hoch dynamisch und geprägt von kurzen Innovationszyklen. Die Führungs- und Wirkdominanz entsteht weniger durch Plattformen als durch Software, Daten und Adaptierbarkeit.

Unbemannte Bodensysteme (UGVs) schließen dabei eine zentrale Fähigkeitslücke, da sie im Gegensatz zu luftgestützten Drohnen tagelang autonom im Einsatzraum verbleiben können, schwer zu detektieren sind und wetterunabhängig zuverlässig operieren. Mittels KI-gestützter Entscheidungsfähigkeit und durchschlagskräftiger Multiplizierbarkeit können schneller Informationen gesammelt, ausgewertet und in militärische Wirkung übersetzt werden.

Sie sind damit unverzichtbare Sensor- und Wirkmittelträgern im Multi-Domain-Aufklärungs- und Wirkverbund.

Software Defined Defense als Leitprinzip: Fähigkeiten entstehen überwiegend durch plattform-agnostische Software, die durch schnelle Innovationszyklen für kontinuierliche Fähigkeitensteigerung sorgt. Hardware-Komponenten spielen hierbei nur eine sekundäre Rolle, da sie als modularer Mobilitätsträger beliebig austauschbar sind. Masse, Skalierbarkeit und robuste Lieferketten sind die Grundlage für Durchhaltefähigkeit und finanzielle Tragfähigkeit. Das heißt aber auch, dass die notwendigen Beschaffungsprozesse angepasst werden müssen. Denn: Verzögerungen bedeuten Verlust realer Einsatzfähigkeit.

Kampferprobte Systeme: Auch konnten wir bei der HARAKA Storm Exercise erfolgreich den Multi-Domain Verbund testen. Mit über 48 Std. Operationszeit lieferten wir mit geringer Signatur konstant verwertbare Zieldaten an Loitering Munition Systeme– wetterunabhängig für eine 15/15 Trefferquote.

ARX Plattformen erzeugen durch dauerhafte Datenerfassung verwertbare operative Informationen- dort, wo es darauf ankommt.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
21	14:05 Uhr	Saal „Addis Abeba 3“

]INIT[AG

Siegfried Fassl

Die vernetzte Planungsgemeinschaft: Digitalisierung als Schlüssel der Zivil-Militärischen Zusammenarbeit

In einer veränderten sicherheitspolitischen Lage ist die Verteidigungsfähigkeit Deutschlands untrennbar mit der Effizienz ziviler und militärischer Verwaltungsprozesse verbunden. Die Zivil-Militärische Zusammenarbeit (ZMZ) steht vor der Herausforderung, im Spannungsfeld zwischen Landesverteidigung und kommunaler Gefahrenabwehr schnelle, rechtssichere und koordinierte Entscheidungen zu treffen.

Dieser Vortrag beleuchtet beispielhaft die Potenziale digitaler Ökosysteme, um die Schnittstellen zwischen Streitkräften und Verwaltung neu zu definieren. Das Ziel ist eine „Vernetzte Planungsgemeinschaft“, in der Informationen nicht mehr mühsam zwischen Behörden transferiert, sondern auf Basis gemeinsamer digitaler Standards geteilt werden. Im Fokus steht dabei die Frage, ob und wie bestehende IT-Infrastrukturen des Bundes und der Länder – etwa Geodaten-Services oder Register – synergetisch für Sicherheitsaufgaben genutzt werden können.

Potenziale einer digitalisierten ZMZ:

> Beschleunigte Abstimmungsprozesse: Durch digitale Workflows werden komplexe Verfahren von der ersten Bedarfsanmeldung bis zur finalen Genehmigung synchronisiert, wodurch wertvolle Zeit gewonnen wird.

> Effiziente Ressourcennutzung: Eine gemeinsame Datengrundlage verhindert Redundanzen und ermöglicht eine präzise Vorausplanung kritischer Infrastrukturen wie Versorgungs- und Verlegepunkte.

> Transparenz und Rechtssicherheit: Digitale Werkzeuge schaffen für beide Seiten – die militärischen Planer und die kommunalen Genehmigungsbehörden – eine nachvollziehbare und verlässliche Arbeitsbasis.

Ein konkreter Anwendungsfall für diese Vision kann die Plattform DiPlanung sein. Sie demonstriert beispielhaft, wie die Planung als kooperativer Prozess gestaltet werden kann. DiPlanung nutzt dabei konsequent das Prinzip des Dual Use: Es greift auf bewährte administrative Services zurück und transformiert sie in ein einsatzrelevantes Planungswerkzeug.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
22	14:35 Uhr	Saal „Addis Abeba 3“

WILLERT SOFTWARE TOOLS GMBH

Johannes Trageser (Executive Board)

KI-gestütztes Model-Driven Engineering für missionskritische Embedded-Systeme: System- und Softwaremodelle als autonome Engineering-Agenten

Moderne missionskritische Systeme – insbesondere im Verteidigungsbereich – werden zunehmend softwaredefiniert. Gleichzeitig bleiben Entwicklungsprozesse häufig über zahlreiche Werkzeuge, Artefakte und Disziplinen fragmentiert. Die Sicherstellung von Konsistenz, Nachvollziehbarkeit und Sicherheit über den gesamten Entwicklungsprozess hinweg – von der System- und Softwarearchitektur bis zur eingebetteten Implementierung – stellt weiterhin eine zentrale Herausforderung dar.

Model-Driven Engineering (MDE) adressiert diese Herausforderung, indem System- und Softwaremodelle als zentrale Engineering-Artefakte über den gesamten Entwicklungsprozess hinweg genutzt werden. Parallel dazu verändern KI-basierte Assistenzsysteme zunehmend die Interaktion von Entwicklern mit komplexen Engineering-Toolchains. In vielen aktuellen Ansätzen arbeiten KI-Systeme jedoch vor allem auf Dokumenten oder Quellcode – nicht auf den strukturierten System- und Softwaremodellen, die Architektur und Verhalten eines Systems definieren.

Dieser Vortrag stellt einen Ansatz vor, der Model-Driven Engineering mit modernen KI-Agentenarchitekturen verbindet. Durch die MCP-Fähigkeit (Model Context Protocol) eines Modellierungswerkzeugs werden System- und Softwaremodelle für KI-Agenten als strukturierte Wissensquelle zugänglich.

KI-Agenten können dadurch Architekturen analysieren, Verhaltensmodelle auswerten, Implementierungsartefakte generieren und direkt mit der Engineering-Toolchain interagieren.

Gerade im sicherheitskritischen Embedded-Umfeld entsteht damit ein neuer Ansatz für KI-unterstütztes Engineering: KI-Systeme arbeiten nicht mehr auf unstrukturierten Daten, sondern direkt auf formalisierten System- und Softwaremodellen. Der Vortrag zeigt, wie MCP-fähige Modellierungsumgebungen zu aktiven Komponenten innerhalb von KI-Ökosystemen werden und neue Möglichkeiten für Automatisierung, Analyse und Traceability im durchgängigen Embedded Software Engineering eröffnen.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
23	15:05 Uhr	Saal „Addis Abeba 3“

ERANEOS GERMANY GMBH

Dr. Martin Schössler (Partner Eraneos Defence)

Vernetzt denken, offensiv handeln: Gesamtstaatliche Verteidigung im Zeitalter permanenter Hybridangriffe

Permanente Hybridangriffe – von Sabotage an Unterseekabeln über GPS-Störungen bis zu Cyber und Desinformation – wirken bewusst unterhalb klassischer Schwellen und zielen auf Staat, Wirtschaft und kritische Infrastrukturen. Deutschland hat mit den Rahmenrichtlinien Gesamtverteidigung (RRGV) Leitplanken gesetzt; zugleich bestehen Lücken bei Interoperabilität, gemeinsamem Lage- und Führungsbild sowie Übungs- und Betriebskultur.

Lagebild und Learnings

Stefan D. Pauly, Flottillenadmiral a.D. und Senior Counsel bei Eraneos, verdichtet Erfahrungen aus operativen NATO-Kontexten und internationalen Vorreitern (Nordics, Taiwan, Ukraine): Total-Defence wird dort wirksam, wo Rollen klar sind, gesamtstaatlich geübt wird und Public-Private-Verbundsysteme über Datenräume und Operationsprozesse belastbar betrieben werden.

Eraneos als Enabler und Orchestrator

Der Schwerpunkt liegt auf der Übersetzung in umsetzbare, marktfähige Fähigkeitsbeiträge – anschlussfähig an Vorhaben auf Deutschland-, NATO- und EU-Ebene. Der Engpass ist selten das Konzept, sondern die Orchestrierung: Akteure zusammenbringen, Angebote präzise positionieren, Konsortien/Partnerschaften formen, Interoperabilität absichern und Zugang zu relevanten Entscheidern schaffen. Genau hier agiert Eraneos als Enabler für Akteure der europäischen Defence-Industrie: beschleunigter Markteintritt und Wachstum durch Go-to-Market, Positionierung, Partnering, Executive Access sowie gemeinsame Wachstumsstrategien entlang konkreter Fähigkeitsbedarfe. Eraneos verbindet Transformations- und Technologiekompetenz (Strategie, IT-Advisory, Data & AI) mit einem europäischen Netzwerk – und schafft so eine Skalierungsplattform vom Pilot bis in den robusten Betrieb.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
24	15:35 Uhr	Saal „Addis Abeba 3“

SERVICE NOW

Andreas Belschner | Stefan Hefter

Schutz kritischer Infrastrukturen im Krisen- und Konfliktfall

Moderne Konflikte zielen zunehmend auf kritische Infrastrukturen ab – Energienetze, Kommunikationsnetzwerke und Lieferketten. Wirksame Vorbereitung und Schutz erfordern mehr als physische Sicherheit: Sie verlangen Lagebewusstsein in Echtzeit, nahtlose Koordination zwischen Behörden und Kommandostellen sowie die operative Resilienz, um unter Druck wesentliche Dienste aufrechtzuerhalten.

In diesem Vortrag zeigen wir, wie die ServiceNow-Plattform zivile und militärische Akteure in Krisenszenarien und Konflikten verbinden kann und wie Workflow-Automatisierung die Betriebskontinuität sichert, wenn es darauf ankommt – von der Planung über Übungen und Trainings bis hin zu realen Konflikten. Ein konkreter Anwendungsfall, präsentiert von KPMG, veranschaulicht, wie dies in der Praxis aussieht.

Modern conflicts increasingly target critical infrastructure — energy grids, communication networks, and logistics chains. Effective preparedness and protection requires more than physical security: it demands real-time situational awareness, seamless coordination across agencies and commands, and the operational resilience to maintain essential services under pressure.

This session explores how the ServiceNow platform can connect civilian and military stakeholders in crisis scenarios and conflicts, and how workflow automation supports continuity of operations when it matters most - from planning, conducting exercises and trainings, to real live conflicts. A concrete use case presented by KPMG illustrates what this looks like in practice.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
25	16:05 Uhr	Saal „Addis Abeba 3“

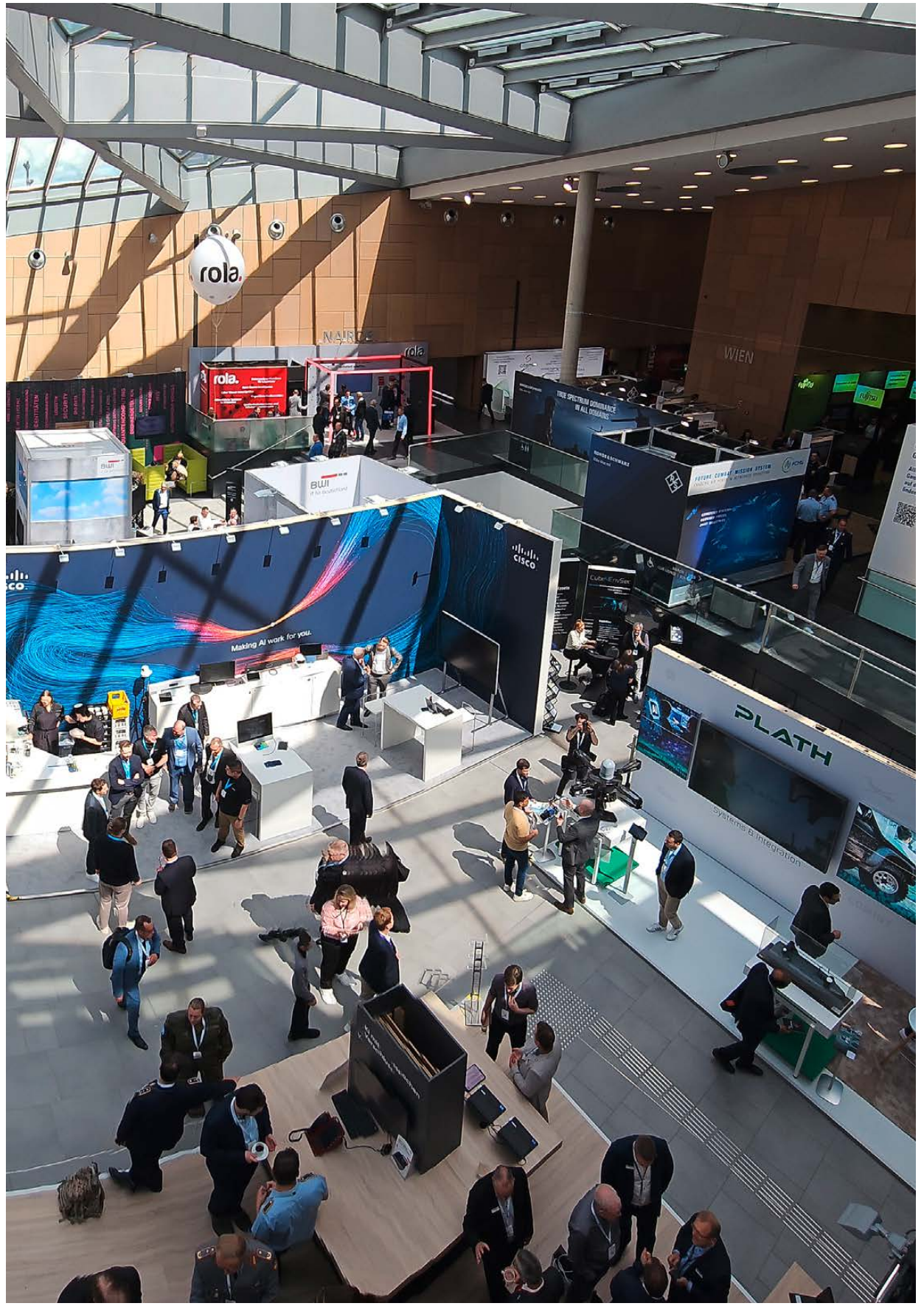
Google Cloud

GOOGLE GERMANY GMBH

Michael Hlevnjak (KAD Defence)

Souverän, resilient, skalierbar: Hybride Cloud-Lösungen als Rückgrat der digitalen Verteidigung

In modernen Konfliktszenarien entscheidet die Geschwindigkeit der Informationsverarbeitung über den Einsatzerfolg. Ob im stationären Rechenzentrum oder im abgesetzten Einsatzkontingent am „Tactical Edge“ – Streitkräfte benötigen hybride Cloud-Architekturen, die massiv skalieren und gleichzeitig ausfallsicher sind. Das Konzept des „Digital Sovereignty Mesh“ ermöglicht die sichere und souveräne Bereitstellung von Spitzentechnologien wie KI und Data Analytics über alle Einstufungsgrade hinweg. Wir demonstrieren in unserem Vortrag, wie hybride Cloud-Lösungen so orchestriert werden können, dass sie technologische Führerschaft garantieren, ohne Kompromisse bei der nationalen Souveränität und IT-Sicherheit einzugehen.



Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
26	16:35 Uhr	Saal „Addis Abeba 3“

SAFRAN ELECTRONICS & DEFENSE GERMANY GMBH

Thomas Pfister (Director Sales) | Jens Wachsmann (Senior Sales Manager)

Resilient positioning, navigation and timing solutions are key to operate in GNSS-Denied-Areas

Safran Electronics & Defense Germany, based in Murr near Stuttgart, is a leading provider of resilient Positioning, Navigation, and Timing solutions (PNT). One of the prerequisites in the sensor-effector operational network on the modern battlefield is maintaining the operational readiness of sensors and the ability of forces to act, even in GNSS-denied areas. In this context, resilient PNT plays a particularly important role. When units move in the field, they do so in a synchronized manner. They have highly accurate information on their own position, orientation to north, and a common timestamp.

If the GNSS signal is disrupted by jamming or spoofing, alternative systems must ensure that there are no limitations to operational capability. The first step is to detect jamming or spoofing at all, so that the soldier becomes aware that his positional data is being compromised. This is where technologies come into play that can distinguish very clear signals – as is the case with spoofing – from the usual, generally less precise GNSS signals. In the next step, navigation and synchronized timing must be maintained. This is done using Hemispherical Resonating Gyroscopes (HRGs), which determine geographic north with the help of the Earth's rotation. In addition, Inertial Navigation Units (INUs) play an important role. They represent self-position changes very precisely for a certain period of time. For synchronization of timing in GNSS-free environments, Safran offers atomic clocks and so-called time servers. If a GNSS signal drops out, atomic clocks in equipped dismounted units, ground vehicles, and aircraft continue to run in sync. As soon as the GNSS signal can be received without interference again, it once more becomes the main reference.

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
27	17:05 Uhr	Saal „Addis Abeba 3“

IBM DEUTSCHLAND GMBH

Julius Sommer | Sandra Pfetzing-Huber | Kolditz Steffen

Vom Datenstrom zur Entscheidungsfähigkeit. Wie softwarebasierte Architekturen MDO beschleunigen

Viele Daten, wenig Zusammenhang
Moderne Gefechtsfelder erzeugen enorme Mengen an Sensor- und Plattformdaten. Sie liefern kontinuierlich Informationen, verbleiben jedoch oft in isolierten Systemen. Sensoren erkennen Bedrohungen, Plattformen melden Ereignisse, Führungsstellen bewerten – jedoch ohne durchgängige Integration. Das Ergebnis: fragmentierte Lagebilder, obwohl technische Möglichkeiten weit darüber hinausgehen.

Vernetzte Daten statt isolierter Systeme
Der Vortrag zeigt, wie dieser Engpass überwunden werden kann. Ein SDD-Ansatz für MDO vernetzt Sensoren, Plattformen und Effektoren über offene, modulare Architekturen. Informationen werden dort verarbeitet, wo sie entstehen – am Sensor, auf Plattformen und in verteilten Rechenknoten. Durch Datenfusion, KI-Analyse und eine Edge–Fog–Cloud-Architektur entsteht ein echtzeitfähiges Lagebild. Interoperabilität steigt, Entscheidungszyklen verkürzen sich und vorhandene Fähigkeiten wirken im integrierten Verbund.

Nutzung verfügbarer Technologien
Statt auf langwierige Beschaffungen proprietärer Systeme zu setzen, nutzt der Ansatz verfügbare Technologien. Bewährte Software- und Datenplattformen, moderne KI-Methoden sowie Cloud- und Edge-Technologien bilden eine schnell integrierbare Basis. Entwicklungszeiten sinken und der Weg zur operativen Nutzung verkürzt sich deutlich.

Vom Konzept zur Architektur
Erleben Sie, wie sich ein leistungsstarker Technologieverbund aus Sensorik, KI und modernen Systemen praxisnah und sicher realisieren lässt. Wir zeigen, wie klare Architekturprinzipien Sicherheit, Resilienz und digitale Souveränität gewährleisten – ohne Innovation zu bremsen. Eine durchdachte Systemarchitektur sichert Integrationshoheit, Datenkontrolle und nationale Steuerung kritischer Funktionen. So entsteht eine skalierbare, zukunftsfähige Softwarearchitektur, die alle Technologien zu einem leistungsfähigen Gesamtsystem verbindet.

Seien Sie dabei und entdecken Sie, wie moderne Technologie souverän zusammenwächst!

Dienstag, 12. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
28	17:35 Uhr	Saal „Addis Abeba 3“

GENUA GMBH

Arnold Krille

Trau, schau, wem: Hybride Clouds für Resilienz und strategische Autonomie

Zero Trust erstreckt sich nicht nur auf Nutzer und (Client-)Geräte, gerade die letzten Jahre zeigen leider auch die Notwendigkeit, auf das Vertrauen im Bereich des Servers zu schauen. Das umschließt das Vertrauen in die Serversoftware und die zugehörigen Hersteller, aber auch die Hardware der Server und der Cloudinfrastruktur. Wir wollen einen Blick wagen, wie man mit geschickter Wahl der Technologien und des Systemdesigns Risiken minimiert oder mitigiert und auch unter schwierigen Bedingungen und außergewöhnlichen Lagen arbeits- und einsatzfähig bleibt.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
29	10:00 Uhr	Plenarsaal

AFCEA BONN E. V.

Emerging Leaders AFCEA Bonn e. V.

Digital Defence Debate: Multi-Domain Operations – vom Lagebild zur Wirkungskette

Multi-Domain Operations (MDO) zielen darauf ab, militärische Wirkung über alle Domänen hinweg zu synchronisieren – von Land, Luft und See über Cyber bis in den Weltraum. Entscheidend dafür ist ein gemeinsames Lagebild sowie ein sicherer und schneller Datenfluss zwischen Sensoren, Führungsstrukturen und Effektoren. Fragen der Datenhoheit, Datenfusion und eines resilienten Datenraums werden damit zum Fundament moderner Operationsführung. Das Panel diskutiert, wie durch Vernetzung, Orchestrierung und gemeinsames Wirken zwischen militärischen Akteuren, strategischer Planung und Industrie aus Informationen tatsächlich Wirkungsketten entstehen – und welche Voraussetzungen geschaffen werden müssen, damit Multi-Domain Operations in der Praxis funktionieren.

Multi-Domain Operations (MDO) sollen militärische Wirkung über alle Domänen hinweg ermöglichen – vorausgesetzt, Daten aus unterschiedlichen Quellen werden schnell zusammengeführt, geteilt und in Entscheidungen übersetzt. Doch wie gelingt der Weg vom Lagebild zur Wirkungskette in der Praxis? Das Panel diskutiert zentrale Voraussetzungen wie Datenhoheit, Datenfusion und wie die notwendige Vernetzung und Orchestrierung zwischen militärischen Akteuren und strategischer Planung. Im Fokus steht die Frage, wie gemeinsames Wirken über Domänen und Teilstreitkräfte hinweg konkret umgesetzt werden kann, wo derzeit die größten Hürden und Anforderungen der modernen Kriegsführung liegen.

Digital Defence Debate

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
30	11:05 Uhr	Plenarsaal

AFCEA BONN E. V.

Emerging Leaders AFCEA Bonn e. V.

Start-up Pitch & Panel Session Innovation mit System – von der Idee zur Fähigkeit

Innovationen entfalten ihren Wert erst dann, wenn Technologie, Organisation und Prozesse wirksam ineinandergreifen. Genau hier setzt die Pitch & Panel Session an: Sie nimmt das Innovationsökosystem der Bundeswehr in den Fokus und zeigt auf, welche Voraussetzungen erforderlich sind, damit neue Technologien den Weg aus der Entwicklung in die praktische Anwendung finden. Im Mittelpunkt steht die Frage, wie aus Ideen konkrete Fähigkeiten entstehen – insbesondere vor dem Hintergrund wachsender sicherheitspolitischer Anforderungen.

Am Beispiel von Drohnenlösungen wird veranschaulicht, wie dynamisch sich Innovationsprozesse aktuell entwickeln und welchen Herausforderungen sie zugleich begegnen. Nach einer kurzen Einführung bietet ein inhaltlicher Impuls einen strukturierten Überblick über die relevanten Akteure, Strukturen und Prozesse im Innovationsökosystem der Bundeswehr. Dabei wird aufgezeigt, über welche Zugangswege und Kooperationsmöglichkeiten junge Unternehmen verfügen – von ersten Kontakten über Erprobung und Pilotierung bis hin zur Skalierung.

Neben diesen strukturellen Rahmenbedingungen werden auch kulturelle, regulatorische und organisatorische Faktoren beleuchtet, die maßgeblich über den Erfolg von Innovationen entscheiden. Gerade in einem sicherheits- und verteidigungsrelevanten Umfeld mit hoher Dynamik kommt diesen Aspekten eine besondere Bedeutung zu.

Im Anschluss präsentieren drei ausgewählte Start-ups ihre Lösungen in kompakten Pitches. Im Fokus stehen dabei nicht nur technologische Ansätze, sondern insbesondere Einsatzreife, Integrationsfähigkeit sowie der konkrete Mehrwert für die Bundeswehr. Die Beiträge werden durch ein Panel aus Vertreterinnen und Vertretern aus Praxis, Technologie und Innovation eingeordnet und diskutiert.

Ein interaktives Publikumsvoting macht unterschiedliche Perspektiven sichtbar, bevor das überzeugendste Start-up ausgezeichnet wird. Die Session schließt mit einem gemeinsamen Ausblick: Welche Rahmenbedingungen braucht es, um Innovation schneller und nachhaltiger in die Anwendung zu bringen?

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
31	12:05 Uhr	Plenarsaal

21strategies

21STRATEGIES GMBH

Dr. Armin Brandstetter

JATOC – Taktikfähigkeiten für agil agierende unbemannte Systeme

In vernetzten, dynamischen Lagen müssen Streitkräfte schnell entscheiden und handeln. Unbemannte Systeme sind dabei integraler Bestandteil dieses Entscheidungs- und Handlungsumfelds. Ihre geringen Produktionskosten ermöglichen wirksame Einsätze auch gegen hochwertige Ziele und haben einen Wettlauf zwischen Einsatz und Abwehr ausgelöst.

Entscheidend ist dabei nicht nur die Wirkung einzelner Systeme, sondern vor allem die Skalierung ihrer Stückzahl bis hin zur Sättigung gegnerischer Abwehr. Ergänzend zur Skalierung müssen Unbemannte Systeme in das Entscheidungs- und Handlungsumfeld integriert und dynamisch sowie taktisch versatil eingesetzt werden. Zu vorhersehbares Verhalten erleichtert ihre Bekämpfung.

Derzeit wird diese taktische Versatilität überwiegend durch menschliche Bediener – etwa via manuelle Steuerung mit Video-Feedback – sichergestellt. Dieses Bedienkonzept kann der notwendigen Skalierung nicht folgen, da die Zahl verfügbarer Systeme die Zahl einsetzbarer Bediener weit übersteigt. Zukünftig müssen unbemannte Systeme daher befähigt werden, autonom, kooperativ und taktisch versatil zu agieren, um Skalierung und Integration in das Entscheidungs- und Handlungsumfeld gleichermaßen zu ermöglichen.

Der Vortrag stellt die von 21strategies entwickelte edge-fähige Software JATOC (Joint Autonomous Tactical Operations Core) vor: Damit kann man auf Basis von KI-Algorithmen unbemannte Systeme derart automatisieren, dass diese herstellerunabhängig taktisch versatil und kooperativ agieren können. Dabei werden taktische Fähigkeiten in der tactics21-Simulationssoftware entwickelt und dann mittels Sim-To-Real auf Realsysteme portiert. Diese Fähigkeiten konnten im relevanten operationellen Umfeld mit Roboterhunden und UAV bereits erfolgreich demonstriert werden. Im Vortrag adressieren wir die dabei gemachten Erfahrungen, sowie die allgemeinen zu bewältigen Herausforderungen.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
32	12:35 Uhr	Plenarsaal

Hewlett Packard Enterprise

HEWLETT PACKARD ENTERPRISE

Jan-Lukas Wennemar

Datenhoheit im Gefecht der Zukunft: Das souveräne HPE Defense-Ökosystem

Im Gefecht der Zukunft hängt operative Überlegenheit zunehmend davon ab, wie sicher, schnell und souverän Daten genutzt werden können. Sensoren, Plattformen und vernetzte Systeme liefern zahlreiche kritische Informationen, doch erst deren zuverlässige Verarbeitung und geschützte Verteilung ermöglichen fundierte Entscheidungen unter Zeitdruck.

Moderne Streitkräfte stehen dabei vor einem Spannungsfeld: Einerseits wächst der Bedarf an Echtzeitinformationen und KI-gestützter Auswertung, andererseits sind Konnektivität, Bandbreite und Sicherheit im Einsatz nicht jederzeit gewährleistet. Zentrale Architekturen und starre Abhängigkeiten stoßen unter Gefechtsbedingungen schnell an ihre Grenzen. Daten und ihre Nutzung werden damit zu operativen Schlüsselfaktoren.

Das HPE Defense-Ökosystem adressiert diese Anforderungen mit einer modularen, souveränen Architektur, die Edge Computing, AirGap-Systeme für sichere Konnektivität sowie KI-Funktionen integriert. Rechenleistung und Datenverarbeitung werden gezielt in den Einsatzraum verlagert und bei Bedarf in zentrale oder dezentrale Rechenzentren übertragen. So lassen sich Latenzen reduzieren, Abhängigkeiten minimieren und zeitkritische Erkenntnisse schneller nutzbar machen.

Ein besonderer Fokus liegt auf resilienter Konnektivität und sicherer Datenauswertung. Mobile Private-5G-Lösungen von HPE ermöglichen abgeschottete Kommunikationsnetze, die unabhängig von öffentlicher Infrastruktur betrieben und missionsspezifisch angepasst werden können. In Kombination mit verschlüsseltem Datentransport sowie Puffer- und Synchronisationsmechanismen entsteht ein sicherer Informationsfluss vom Einsatzgebiet bis ins Rechenzentrum. Dort werden Daten mithilfe der HPE Private Cloud AI [Disconnected] ausgewertet, um aus komplexen Sachverhalten strategische Erkenntnisse zu gewinnen.

Damit bietet das HPE Defense-Ökosystem Lösungen von der taktischen bis zur strategischen Ebene.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
33	13:05 Uhr	Plenarsaal

]pexip[

PEXIP GERMANY GMBH

Dr. Dirk Fischer (Country Manager DACH)

Kommunikations- und Kollaborationsplattformen in der Verteidigung: Kernanforderungen an Souveränität. Resilienz. Interoperabilität.

Echtzeitkommunikation und -kollaboration sind im militärischen Einsatz operative Kernfähigkeiten. Lagebild, Führungsfähigkeit und Wirkungskette werden unmittelbar durch die digitale Souveränität, Cyber-Resilienz und auf Standards basierende Interoperabilität des zugrunde liegenden digitalen Stacks gestützt.

Vor diesem Hintergrund stellt sich die Frage, welche Kernanforderungen ein digitaler Stack erfüllen muss, um souverän, resilient und interoperabel zu sein.

Digitale Souveränität umfasst hierbei nicht nur das Ausmaß der Kontrolle über die Verarbeitung und Speicherung von Daten, sondern auch das Ausmaß der Kontrolle über das Hosting der Lösung einschließlich der Update- und Upgrade-Prozesse. Im Sinne der Software-Souveränität ist zudem das Ausmaß der Anpassungs- und Weiterentwicklungsmöglichkeiten der Software relevant.

Cyber-Resilienz umfasst nicht nur das Ausmaß der Abwehr von Cyber-Angriffen (präventive Komponente), sondern auch das Ausmaß der Wiederherstellungsfähigkeit nach Cyber-Angriffen oder in gestörten Netzen (reaktive Komponente). Zudem ist die Geschäftskontinuität sicherzustellen, das heißt auch das Ausmaß einer robusten Wertschöpfungskette (kommerzielle Komponente) ist Bestandteil der Cyber-Resilienz.

Interoperabilität beschreibt zum einen das Ausmaß, in dem Echtzeitkommunikation und -kollaboration über militärische Standards stattfinden kann. Zum anderen beschreibt sie das Ausmaß, in dem Module eines Stacks über definierte Standards integriert und erweitert werden können. Klar definierte Integrationsstandards sind Voraussetzung, um nationale und multinationale Komponenten in einer kontrollierten Architektur zusammenzuführen.

Der Vortrag gibt Beispiele zur Erfüllung obiger Kernanforderungen und skizziert ein Zielbild europäischer Stacks für Kommunikation und Kollaboration in Echtzeit.

Referent ist Dr. Dirk Fischer, Country Manager DACH beim norwegischen Hersteller Pexip und ehemaliger Dozent an der Universität der Bundeswehr München.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 1
34	13:15 Uhr	Plenarsaal

MOTOROLA SOLUTIONS GERMANY GMBH

Kay Dittloff

Warum die nächste Generation verlegbarer Netze das Gefechtsfeld verstehen muss

Die Digitalisierung der Landstreitkräfte hat die Mobilität durch gehärtete, breitbandige Netze massiv gesteigert. Doch im Szenario 2030+ reicht Konnektivität allein nicht mehr aus: Gegen technologisch ebenbürtige Gegner wird jede Emission zur tödlichen Zielmarke. Klassische Infrastruktur stößt hier an Grenzen. Überlebensfähigkeit im hochintensiven Gefecht erfordert den Wechsel von passiven Systemen hin zu kognitiven Netzen, die den elektromagnetischen Raum aktiv wahrnehmen und sich der Lage anpassen.

Wir brechen mit alten Paradigmen der Fernmeldetruppe und beleuchten das Doppelmandat moderner Überlebensfähigkeit: Signaturmanagement und autonome Regeneration.

Fokus 1: Signaturmanagement als Lebensversicherung
Im modernen Kriegsbild wirken konventionelle Funkstellen wie Leuchtfeuer für die gegnerische Aufklärung. Kognitive Netze müssen ihren elektronischen Fußabdruck dynamisch minimieren. Durch intelligente Architekturen senken wir die Entdeckungswahrscheinlichkeit (LPI), tauchen im Hintergrundrauschen unter und entziehen uns der gegnerischen Zielfindung.

Fokus 2: Resilienz durch Autonomie
Unter massiver elektronischer Störeinwirkung (Jamming) muss das Netz zur Selbstheilung fähig sein. Wir zeigen, wie Spectrum Intelligence und dynamisches Mesh-Routing kritische Datenströme – etwa Video-Lagebilder – ohne Bedienereingriff und Zeitverlust autonom umsteuern.

Das Ziel: Führungsfähigkeit unter allen Bedingungen
Die Zukunft liegt in einem intelligenten Ökosystem. Erst die Verbindung aus Signaturarmut und automatisierter Resilienz ermöglicht das Unvereinbare: Ein Truppenführer, der mobil und schwer fassbar bleibt, aber permanenten Zugriff auf sein digitales Nervensystem behält.

Diskutieren Sie mit uns, wie europäische Streitkräfte den Informationsvorsprung am Tactical Edge dauerhaft garantieren.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
35	11:05 Uhr	Saal „Addis Abeba 3“

TREND MICRO DEUTSCHLAND GMBH

Robert Wortmann

Digitale Souveränität im Zeitalter globaler Cyberkonflikte – Handlungsfähigkeit trotz Abhängigkeiten

Cyberoperationen sind heute ein fester Bestandteil geopolitischer Machtprojektion. Staaten nutzen Cyberfähigkeiten nicht mehr nur für klassische Spionage, sondern zunehmend zur Vorbereitung hybrider Konflikte, zur strategischen Einflussnahme und zur gezielten Störung kritischer Infrastrukturen. Gleichzeitig beschleunigt Künstliche Intelligenz die Entwicklung neuer Angriffstechniken – von automatisierter Schwachstellensuche bis hin zu KI-gestützter Aufklärung.

Für Staaten, Behörden und sicherheitskritische Organisationen ergibt sich daraus eine zentrale Frage: Wie lässt sich digitale Souveränität erreichen, wenn Cyberverteidigung zwangsläufig von globalen Informationsströmen abhängt?

Threat Intelligence, Vulnerability Research und Threat Research entstehen heute in einem internationalen Ökosystem. Sicherheitslücken werden weltweit entdeckt, Angreifergruppen operieren grenzüberschreitend, und neue Angriffstechniken werden häufig in internationalen Forschungsnetzwerken analysiert. Eine vollständige technologische oder informationelle Isolation ist daher weder realistisch noch sicherheitspolitisch sinnvoll.

Der Vortrag analysiert die aktuelle globale Bedrohungslage anhand aktueller Erkenntnisse aus der TrendAI-Bedrohungsanalyse und zeigt, wie staatliche und sicherheitskritische Organisationen trotz dieser strukturellen Abhängigkeiten strategische Handlungsfähigkeit und Resilienz aufbauen können.

Im Fokus stehen dabei die Auswirkungen geopolitischer Cyberoperationen, die Rolle von Künstlicher Intelligenz für Angreifer und Verteidiger sowie konkrete Ansätze, um Abhängigkeiten transparent zu machen und globale Erkenntnisse in operative Cyberverteidigung zu übersetzen.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
36	11:35 Uhr	Saal „Addis Abeba 3“

THALES
Building a future we can all trust

THALES DEUTSCHLAND

Johannes Loevenich

Algorithms at War: Wie KI und Cyber das vernetzte Gefechtsfeld bis 2030+ transformieren

Das vernetzte Gefechtsfeld bis 2030+ wird nicht mehr primär durch einzelne Plattformen bestimmt, sondern durch die Fähigkeit, Daten, Software, Algorithmen und Wirkungsträger in resilienten, interoperablen Operationsnetzen zusammenzuführen. Aus Sicht von Thales Deutschland markiert Software Defined Defence dabei einen grundlegenden Paradigmenwechsel: Militärische Überlegenheit entsteht künftig nicht allein durch Hardware, sondern durch die schnelle, sichere und missionsorientierte Integration von Software, KI und Cyberfähigkeiten über alle Ebenen und Domänen hinweg.

Der Vortrag beleuchtet, wie KI, Cyber und Informationssicherheit das zukünftige Operationsbild verändern. Generative KI, insbesondere Large Language Models, entwickelt sich vom Assistenzwerkzeug zum operativen Enabler: für die Auswertung heterogener Lageinformationen, die Verdichtung komplexer Meldungen, die Unterstützung militärischer Führungsprozesse und die Automatisierung von Datenanalysen. In Verbindung mit Reinforcement Learning entstehen agentische Systeme, die in dynamischen Umgebungen Handlungsoptionen bewerten, priorisieren und adaptiv an Missionsbedingungen anpassen können. Perspektivisch eröffnen World Models zusätzliche Potenziale für vorausschauende, modellbasierte Entscheidungsunterstützung.

Gleichzeitig werden zentrale Fähigkeitslücken sichtbar, die prioritär geschlossen werden müssen: eine belastbare digitale Datenbasis, sichere, standardisierte Schnittstellen, schnelle Entwicklungs- und Ausbringungszyklen, vertrauenswürdige KI sowie der Schutz KI-gestützter Systeme und Modelle gegen Manipulation, Täuschung und Ausnutzung. Software Defined Defence erfordert deshalb, “AI for Cyber Security“ und „Cyber Security for AI“ konsequent zusammenzudenken.

Der Vortrag beleuchtet, welche technologischen Weichen heute gestellt werden müssen, damit Streitkräfte im Jahr 2030+ in einem von Software getriebenen und umkämpften Informationsraum handlungsfähig, resilient und überlegen bleiben.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
37	12:05 Uhr	Saal „Addis Abeba 3“

AIRBUS DEFENCE AND SPACE

Daniel Kallfass

MissionAI-Bw - Der souveräne taktische KI-Assistent für den digitalen Gefechtsstand

Generative KI-Systeme eröffnen der Bundeswehr erhebliche Potenziale zur Unterstützung militärischer Operationen - von der schnellen Erstellung von Berichten, E-Mails und Briefings bis hin zu fundierter Entscheidungsunterstützung im Führungsprozess. Sie ermöglichen eine verbesserte Lageerfassung, erleichtern die Interaktion mit unbemannten Systemen und tragen zur Optimierung der Gefechtsstandsarbeit bei. Um dieses Potenzial gezielt zu untersuchen, führt das Unterstützungskommando die Studienreihe „KI für Taktik Chat in Simulationssystemen“ (KITCH) durch.

Ziel ist es, den Mehrwert generativer KI-Systeme für die taktische Ausbildung und die Einsatzplanung zu bewerten, insbesondere im Kontext komplexer Führungsprozesse. Die im Rahmen der KITCH Studie entwickelte MissionAIBw Plattform basiert auf umfangreichen militärischen Regelwerken, NATO-Doktrinen und taktischen Ausbildungsmaterialien und ist darauf ausgelegt, kontextgenaue, verlässliche Antworten zu liefern. Ein zentraler Fokus liegt dabei auf der Minimierung von Halluzinationen - ein kritisches Thema bei der Nutzung von KI in sicherheitsrelevanten Umgebungen. Um dies zu gewährleisten, werden KI-Agenten und Pipelines entwickelt, die nicht nur Vorschläge erstellen, sondern diese auch qualitätsprüfen, sodass zum Beispiel Antworten auf aktuellen, autorisierten Quellen basieren und diese entsprechend referenzieren.

Darüber hinaus wird MissionAIBw mit Sitaware HQ über Model Context Protocol (MCP) gekoppelt, um auch aktuelle Gefechtssituationen zuzugreifen. Zudem ist MissionAIBw mit der militärischen Gefechtssimulation ReLeGSim gekoppelt, um die KI in realistischen Gefechtsszenarien zu testen und ihre Fähigkeit zur lagebezogenen Entscheidungsunterstützung praktisch zu erproben. Diese Integration ermöglicht nicht nur die Beantwortung taktischer Fragen, sondern auch die Analyse dynamischer Lagen und die Bewertung von Handlungsoptionen unter realitätsnahen Bedingungen.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
38	12:35 Uhr	Saal „Addis Abeba 3“

HAT.TEC

Dr. Fabian Schmitt | Leonard Wessendorff

Komplexität, KI, Kooperation: Über integrierte Lagebilder in Multi-Domain-Missionen

Vielfältige bemannte wie unbemannte Systeme und Plattformen in europäischen Armeen. Eine nie dagewesene Anzahl an Sensoren, die Parameter in Land, Wasser, Luft und Weltall erfassen (von Radar- über Hochfrequenz- und akustischen bis hin zu Photodetektor- und Infrarot-Signalen). Noch nie standen in Verteidigung und Sicherheit mehr Daten zur Verfügung. Gleichzeitig war die Komplexität noch nie so groß. Und sie muss von immer weniger Operatoren bewältigt werden.

Die zunehmende Menge an Daten droht, Einsatzkräfte zu überfluten. Dabei steht mit den Weiterentwicklungen der Künstlichen Intelligenz (KI) ein Werkzeug zur Verfügung, das genau hier seine größten Stärken hat: in der Verarbeitung großer Datenmengen zu verwertbaren Informationen. Doch solange die Daten von untereinander nicht kompatiblen Systemen erfasst werden und nur heterogen und isoliert zur Verfügung stehen, bleibt diese Stärke ungenutzt.

Hier müssen wir ansetzen – und zwar sofort, nicht erst mit der nächsten Generation an Systemen und Plattformen. Wir müssen das Bestehende integrieren, Interoperabilität sicherstellen und unsere Daten optimal nutzen – über eine durchgängige Kette vom Sensor bis zur Wirkung. Dafür braucht es nicht nur Integration, sondern die gezielte Orchestrierung von Sensoren und Systemen sowie deren nahtlose Einbindung in die Missionsführung über den gesamten OODA-Loop hinweg.

Voraussetzung dafür ist ein vollständiges Lagebild. Mit einer plattform- und herstellerunabhängigen Lösung können wir die verfügbaren Sensoren integrieren, Daten zusammenführen und in Echtzeit auswerten. Neben bestmöglichem Situationsbewusstsein können wir darüber hinaus die Möglichkeiten von KI nutzen, um automatisierte Unterstützung entlang des gesamten Entscheidungsprozesses zu bieten. Das alles entlastet die menschlichen Operatoren, die sich so auf ihre wichtigsten Aufgaben konzentrieren können: Das Treffen kritischer Abwägungen und Entscheidungen sowie die Erfüllung des Missionsziels.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
39	13:05 Uhr	Saal „Addis Abeba 3“

MATERNA Virtual Solution

MATERNA VIRTUAL SOLUTION GMBH

Marco Schrader (Sales Director) | Prehm David (Geschäftsführer & Executive Architect)

Von der Smartcard zur mobilen PKI-Wallet: Souveräne digitale Identitäten im sicherheitskritischen Bereich

Nicht nur Streitkräfte, sondern auch Behörden und Organisationen mit Sicherheitsaufgaben stehen vor der Herausforderung, Identitäten und Zugriffe zunehmend mobil abzubilden. Klassische Smartcards bilden seit Jahren das Rückgrat sicherer digitaler Identitäten, stoßen jedoch insbesondere im mobilen Einsatz an operative Grenzen.

SecureID adressiert diesen Bedarf mit einer mobilen PKI-Wallet für sicherheitskritische Umgebungen. Die Lösung überführt das bewährte Sicherheitsmodell der Smartcard kontrolliert auf das Smartphone und vereint Ausweis, Zertifikate und Berechtigungen in einer hochsicheren mobilen Identität. Das mobile Endgerät wird damit zum persönlichen Identitäts- und Zugangsträger für digitale und physische Prozesse.

Im Mittelpunkt stehen dabei starke PKI-basierte Authentifizierung für IT-Systeme wie Festplattenverschlüsselung, VDI und VPN, rechtssichere digitale Signaturen, verschlüsselte Kommunikation (S/MIME) sowie physische Zutritts- und Berechtigungsszenarien per NFC. Identität, Gerät und Anwendung bleiben dabei klar getrennt und folgen etablierten Sicherheits- und Compliance-Vorgaben.

In ihrem gemeinsamen Vortrag zeigen SaltRock, Materna Virtual Solution und Nexus (IN Groupe) anhand praxisnaher Szenarien, wie die SecureID PKI-Wallet bestehende Smartcard-, PKI- und IAM-Infrastrukturen ergänzt statt ersetzt und so eine evolutionäre Migration hin zu mobilen Identitäten ermöglicht. Die Lösung ist auf den Einsatz bis zur Schutzklasse VS-NfD ausgelegt; eine entsprechende Einsatzerlaubnis gemäß den Vorgaben des BSI wird angestrebt.

Mittwoch, 13. Mai 2026

Slot-Nr.	Beginn	Speakercorner 2
40	13:35 Uhr	Saal „Addis Abeba 3“

rasdaman
raster data manager

RASDAMAN GMBH

Prof. Dr. Peter Baumann

KI-gestützte Föderation für Multi-Domain GEOINT: Was geht, Stand heute?

Die Digitale Transformation ist in vollem Gang. Spätestens die Abschaltung von Starlink für die russischen Streitkräfte hat verdeutlicht, welch zentrale Bedeutung einer durchgängig vernetzten digitalen Gefechtsführung zukommt. Für die verbündeten Nationen der NATO ist zusätzlich die Interoperabilität unabhängig entstandener Technologien essenziell. Modular Open Systems Architecture (MOSA) ist ein wichtiger Trend, um selektiv „best of breed“ Komponenten statt monolithischen „take it or leave it“ Systemen beschaffen zu können. Weiterhin spielt der Einsatz von KI eine immer wichtigere Rolle mit einer Reihe von potenziellen Vorteilen.

All dies ist klar erkannt, entsprechende Strategien sind von ACT und anderen formuliert, und die Hersteller haben mit Entwicklungen begonnen. Doch was ist, angesichts der engen Zeitschienen, die aktuelle Verfügbarkeit solcher Prinzipien und Produkte, Stand heute? In unserem Vortrag stellen wir praxiserprobte, heute einsatzfähige Fähigkeiten (TRL 9) für C2/C4ISR vor, insbesondere für GEOINT und FMN:

> Intelligente, semantikbasierte Dienste

> Zero-Coding Datenanalyse

> Verteiltes Management und Analyse von raum-zeitlichen „Big Data“ und KI-Modellen

> Orts-transparente Föderation von autonomen Datenanbietern

> Multi-Domänen-fähige Cloud/Edge-Integration (Satellit, Drohne, Schiff, etc.)

> Volle Interoperabilität (u.a. mit NATO Core-GIS) durch offene Standards (Referenz-Implementierung)

> Integration beliebiger KI-Modelle

In den AI-Cubes von rasdaman sind diese Fähigkeiten implementiert und in TRL 9 in USA, Europa und Asien operativ im Einsatz. Im Vortrag illustrieren wir die Technologie an Hand von Live-Demos und stellen in den Kontext aktueller Standardisierung.

AFCEA Bonn e.V.

World Conference Center Bonn | 12./13. Mai 2026

RECRUITING
Saal „Berlin“

Ihre Chance auf den Einstieg und die Karriere in die IT- und Verteidigungsbranche!

12.05.2026
11:00–12:00 Uhr
14:30–15:30 Uhr

Die **Nachfrage nach qualifizierten Fachkräften** in der IT- und Verteidigungsbranche wächst stetig.

13.05.2026
12:30–13:30 Uhr

Nutzen Sie die Gelegenheit, beim **Recruitingevent der AFCEA Fachausstellung 2026** auf potenzielle Arbeitgeber zu treffen, sich direkt mit führenden Unternehmen auszutauschen und Karrierechancen in spannenden und zukunftsorientierten Bereichen zu entdecken.

AFCEA Bonn e. V.
Borsigallee 2 · 53125 Bonn
Telefon: +49 228 925 82 52
E-Mail: buero@afcea.de
www.afcea.de

Alle Informationen in der:

AFCEA APP

https://event.afcea.de

- Standpläne
- Programm
- Aussteller
- Informationen
- Favoriten

und mehr ...

Scan me

Entdecken Sie die Fachausstellung über unsere **Web-App** mit nur einem Fingertipp.

*Discover the trade exhibition via our **web app** with just one tap.*

Mit der Event-Web-App auf Ihrem Homescreen haben Sie **alle Informationen** jederzeit griffbereit.

*With the event web app on your home screen, you have **all the details** right at your fingertips.*

Powered by Capgemini