



Bonn e.V.

37. AFCEA Fachausstellung

Informations- und Kommunikationstechnik

26./27. Juni 2024

World Conference Center Bonn

**„Zeitenwende in der nationalen Sicherheit -
Resilienz durch disruptive digitale Lösungen“**

Industrievorträge FA 2024



Inhaltsverzeichnis „Industrievorträge FA 2024“:

Zeitplan/Themen der Industrievorträge	4 - 5
Übersicht der Vortragslots der Aussteller	6 - 7
Themenliste der Vorträge mit Referenten (1 - 31)	8 - 13
Abstracts zu den Vorträgen	16 - 47
Info zu der Startup Pitch und Panel Session	37
Info zum AFCEA Studienpreis 2024	48
Jahresprogramm 2024 von AFCEA Bonn e.V.	49
Notizen zu den Industrievorträgen	50 - 51

Auf vielfachen Wunsch der Aussteller haben wir bei der AFCEA Fachausstellung 2024 - wie auf der AFCEA FA 2022 und FA 2023 - zwei Speakercorner für Industrievorträge eingerichtet, dieses Jahr jedoch im geschichtsträchtigen ehemaligen Plenarsaal des Deutschen Bundestages und im RAUM ADDIS ABEBA 3 auf der RHEINEBENE.

Dort können Aussteller in den Zeiten, in denen keine Vorträge des Symposiums stattfinden, zu einem Thema ihrer Wahl vortragen (Vortrag 20 Min, 5 Min Fragen/ Diskussion).

Auf dieser Seite sehen Sie in alphabetischer Reihenfolge die Aussteller, welche im Rahmen der Industrievorträge vortragen. Auf den folgenden Seiten finden Sie Details zu den Vorträgen im zeitlichen Ablauf.

Mit dem QR-Code kommen Sie zu den Vortragsthemen der Aussteller in zeitlicher Reihenfolge auf unserer AFCEA Homepage und den damit verlinkten vollständigen Abstracts. Sie finden dort auch die Broschüre „Industrievorträge FA 2023 als pdf-Datei zum download.



Speakercorner 2

Speakercorner 1



Industrievorträge

Vortragende Aussteller





Zeitplan der Symposiums- und Industrievorträge

Zeitplan für die Industrievorträge bei der FA 2024

26.06.2024		Speakercorner 1	Speakercorner 2	27.06.2024		Speakercorner 1	Speakercorner 2
		Plenarsaal Bundestag	Vortragssaal ADDIS ABEBA 3			Plenarsaal Bundestag	Vortragssaal ADDIS ABEBA 3
AFCEA Fachausstellung 2024	09:00			AFCEA Fachausstellung 2024	09:00		
	09:30				09:30		
	10:00	Eröffnung Symposiums-vortrag 1			10:00	Symposium 2 #Digital Defence Debate	
	10:30				10:30		
	11:00	Slot Nr:	Slot Nr:		11:00	Slot Nr:	Slot Nr:
	11:15 - 11:40	1 Materna Information & C.	14 Rohde & Schwarz		11:15 - 11:40	22 Genua	27 Telespazio
	11:45 - 12:10	2 CGI	15 RUAG		11:45 - 12:10	23 HENSOLDT	28 Carmenta
	12:15 - 12:40	3 IBM	16 Materna Virtual		12:15 - 12:40	24 Eviden	29 Adva Network Security
	12:45 - 13:10	4 dainox	17 Eviden		12:45 - 13:10	25 AIRBUS	30 NVIDIA
	13:15 - 13:40	5 RHEINMETALL	18 roda Computer		13:15 - 13:40	26 Sophist	31 Best Systeme
	13:45 - 14:10	6 SThree	19 Detecon		14:00	Symposiums-vortrag 3	
	14:15 - 14:40	7 ESG Elektronik	20 Accenture		14:30		
	14:45 - 15:10	8 Conet	21 Thales		15:00		
	15:15 - 15:40	9 rola Security	Ab ca. 15:20 h Die Emerging Leaders AFCEA Bonn (ELA) präsentieren Startups in Pitch Sessions		15:30		
15:45 - 16:10	10 Secusmart		16:00	INDUSTRIE-VORTRÄGE:			
16:15 - 16:40	11 Sophos		16:30				
16:45 - 17:10	12 Constructor						
17:15 - 17:40	13 Bechtle						
18:00	AFCEA Bonn e.V. lädt Aussteller und Besucher ein zum Get-Together (RHEINEBENE)						
19:00							
20:00							
21:00							
bis 22:00							

INDUSTRIEVORTRÄGE:

Auf vielfachen Wunsch der Aussteller richten wir auch bei der AFCEA Fachausstellung 2024 zwei Speakercorner Industrievorträge ein: im ehemaligen Plenarsaal des Deutschen Bundestages und im Vortragssaal ADDIS ABEBA 3. Dort können Aussteller in den Zeiten - in denen keine Vorträge des Symposiums im Plenarsaal stattfinden - zu einem Thema ihre Wahl vortragen (Vortrag 20 Min, 5 Min Fragen/Diskussion).

Auf dieser Seite sehen Sie die Vorträge der Aussteller im zeitlichen Ablauf. Der QR-Code oben rechts bietet den Link zu den Vortragsthemen und den Abstracts sowie zur „Broschüre Industrievorträge 2024“.

Wie bei der FA 2023 haben wir wieder ein **Symposium mit 3 Vorträgen** als Teil der AFCEA Fachausstellung 2024.

SYMPOSIUM:

Industrievorträge

Themen der Industrievorträge

Nr.	Aussteller	Thema des Industrievortrages
1	Materna Information & Communications SE	Verschlusssache to Go - vernetzte und sichere Kommunikation auf ultramobilen Endgeräten
2	CGI Deutschland B.V. & Co. KG	Al Felix – Drei Erkenntnisse für KI-Projekte mit den Streitkräften
3	IBM Deutschland	Bundeswehr: Digital und innovativ
4	dainox GmbH	Software Defined die Zukunft gestalten: Die Symbiose von flexibler Software und robuster Hardware
5	RHEINMETALL	Welche Rolle übernimmt die „alte“ Rüstungsindustrie im digitalen Zeitalter?
6	SThree GmbH	Megatrends managen – und trotz fehlender Fachkräfte den Anschluss nicht verlieren
7	ESG Elektroniksystem- und Logistik-GmbH	Multi-Domain Operations End2End – Vom Sensor über den Shooter bis in die Munition
8	CONET	Mit Lagebildern und technischen Dokumenten sprechen
9	rola Security Solutions GmbH	Tiefenanalyse im Dienst der Sicherheit: Moderne IT-Lösungen für Militäroperationen
10	Secusmart GmbH	SecuSUITE Cross-Plattform – Give Users a Choice
11	Sophos Technology GmbH	Zukunftssichere IT-Sicherheit – und welche Rolle spielen Mensch und KI?
12	Constructor University Bremen gGmbH	Mehr Nutzen aus Geo-Standards für das FMN?
13	Bechtle AG	Skalierbar, standardisiert, agil: beschleunigte Softwareentwicklung über verschiedene Clouds hinweg
14	Rohde & Schwarz	ESSOR – European Secure Software Defined Radio. Mit welchen Schritten wird die Funkinteroperabilität europäischer Streitkräfte endlich konkret ermöglicht?
15	RUAG AG	Krisenkommunikation - und wie kommunizieren Sie und Ihre Organisation in Zukunft?
16	Materna Virtual Solution GmbH	Der sichere ultramobile Arbeitsplatz: Per Smartphone und Tablet auf wichtige Fachanwendungen zugreifen. Schnell. Einfach. VS-NfD-konform.
17	Eviden Germany GmbH	Souveräne Digitalisierung und Ermöglichung von Multi Domain Operations: Erzeugung digitaler Wirkketten und durchgängiger Informationsräume als Element der Multi Domain Combat Cloud
18	roda computer GmbH	Vernetzte Visualisierung
19	Detecon International GmbH	Quantentechnologien und ihr Potenzial, Wirtschaft, Verwaltung und Gesellschaft stark zu verändern
20	Accenture	Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit
21	Thales Deutschland	Möglichkeiten zur Erhöhung von Effizienz und Usability bei der Absicherung von Daten und Sprache im High Security Bereich
22	genua GmbH	Souveräne Cloud: Eine geostrategisch-technische Analyse zu Cybersicherheit
23	HENSOLDT	HENSOLDT FCAS Accelerator – ein Paradigmenwechsel für das Innovationsmanagement in der Verteidigung
24	Telekom	Fokussierung auf Kernaufgaben durch Digitalisierung von Verwaltungsprozessen
25	Airbus Defence and Space	Weltraumgestützte Kommunikation für militärische Anwender
26	SOPHIST GmbH	KI oder Mensch – Wer ist besser im Systems Engineering?
27	Telespazio Germany GmbH	Informationssicherheitskonzepte: Grundlagen und Notwendigkeit
28	Carmenta Germany GmbH	Echtzeit Geodaten als Game-changer auf dem Gefechtsfeld
29	Adva Network Security	Geschützte Glasfasernetze als Fundament einer hochsicheren Kommunikations-Infrastruktur: überwacht, resilient, quantensicher
30	NVIDIA GmbH	Sensorfusion, Metadatenextraktion und Datenreduktion in isolierten Edge-Systemen mit Nvidia Jetson
31	best Systeme GmbH	COTS-Ketten sprengen - Moderne IT für Militärische Anwendungen Oder -> wie kann Ihr Unternehmen durch den Einsatz von MOTs profitieren? Ein Beispiel einer High-Performance-Switch-Modifikation (>100GBs) für die Luftfahrt

Vorträge sortiert nach Ausstellern

Aussteller	Vortrag	Tag	Zeit	Raum	Stand
Accenture	20	26.6.24	14:15	Addis Abeba 3	S 32
Adva Network Security	29	27.6.24	12:15	Addis Abeba 3	N 04
Airbus Defence and Space	25	27.6.24	12:45	Plenarsaal	F 03
Bechtle AG	13	26.6.24	17:15	Plenarsaal	S 18
best Systeme GmbH	31	27.6.24	13:15	Addis Abeba 3	R 48
Carmenta Germany GmbH	28	27.6.24	11:45	Addis Abeba 3	W 11
CGI Deutschland B.V. & Co. KG	2	26.6.24	11:45	Plenarsaal	A 03
CONET	8	26.6.24	14:45	Plenarsaal	S 45
Constructor University Bremen gGmbH	12	26.6.24	16:45	Plenarsaal	R 18
dainox GmbH	4	26.6.24	12:45	Plenarsaal	S 33
Detecon International GmbH	19	26.6.24	13:45	Addis Abeba 3	S 73
Deutsche Telekom Geschäftskunden GmbH	24	27.6.24	12:15	Plenarsaal	A 11
ESG Elektroniksystem- und Logistik-GmbH	7	26.6.24	14:15	Plenarsaal	F 01
Eviden Germany GmbH	17	26.6.24	12:45	Addis Abeba 3	F 31
genua GmbH	22	27.6.24	11:15	Plenarsaal	S 25
HENSOLDT	23	27.6.24	11:45	Plenarsaal	A 07
IBM Deutschland	3	26.6.24	12:15	Plenarsaal	F 02
Materna Information & Communications SE	16	26.6.24	12:15	Addis Abeba 3	S 52
Materna Virtual Solution GmbH	1	26.6.24	11:15	Plenarsaal	S 56
NVIDIA GmbH	30	27.6.24	12:45	Addis Abeba 3	R 48
RHEINMETALL	5	26.6.24	13:15	Plenarsaal	N 01/N 09
roda computer GmbH	18	26.6.24	13:15	Addis Abeba 3	F 05
Rohde & Schwarz	14	26.6.24	11:15	Addis Abeba 3	F 10
rola Security Solutions GmbH	9	26.6.24	15:15	Plenarsaal	F 06 b
RUAG AG	15	26.6.24	11:45	Addis Abeba 3	S 70
Secusmart GmbH	10	26.6.24	15:45	Plenarsaal	S 51
SOPHIST GmbH	26	27.6.24	13:15	Plenarsaal	R 53
Sophos Technology GmbH	11	26.6.24	16:15	Plenarsaal	S 62
SThree GmbH	6	26.6.24	13:45	Plenarsaal	S 52
Telespazio Germany GmbH	27	27.6.24	11:15	Addis Abeba 3	F 09
Thales Deutschland	21	26.6.24	14:45	Addis Abeba 3	S 23

Industrievorträgen

Vorträge sortiert nach Vortragsnummern/Reihenfolge

Aussteller	Vortrag	Tag	Zeit	Raum	Stand
Materna Information & Communications SE	1	26.6.24	11:15	Plenarsaal	S 56
CGI Deutschland B.V. & Co. KG	2	26.6.24	11:45	Plenarsaal	A 03
IBM Deutschland	3	26.6.24	12:15	Plenarsaal	F 02
dainox GmbH	4	26.6.24	12:45	Plenarsaal	S 33
RHEINMETALL	5	26.6.24	13:15	Plenarsaal	N 01/N 09
SThree GmbH	6	26.6.24	13:45	Plenarsaal	S 52
ESG Elektroniksystem- undLogistik-GmbH	7	26.6.24	14:15	Plenarsaal	F 01
CONET	8	26.6.24	14:45	Plenarsaal	S 45
rola Security Solutions GmbH	9	26.6.24	15:15	Plenarsaal	F 06 b
Secusmart GmbH	10	26.6.24	15:45	Plenarsaal	S 51
Sophos Technology GmbH	11	26.6.24	16:15	Plenarsaal	S 62
Constructor University Bremen gGmbH	12	26.6.24	16:45	Plenarsaal	R 18
Bechtle AG	13	26.6.24	17:15	Plenarsaal	S 18
Rohde & Schwarz	14	26.6.24	11:15	Addis Abeba 3	F 10
RUAG AG	15	26.6.24	11:45	Addis Abeba 3	S 70
Materna Virtual Solution GmbH	16	26.6.24	12:15	Addis Abeba 3	S 52
Eviden Germany GmbH	17	26.6.24	12:45	Addis Abeba 3	F 31
roda computer GmbH	18	26.6.24	13:15	Addis Abeba 3	F 05
Detecon International GmbH	19	26.6.24	13:45	Addis Abeba 3	S 73
Accenture	20	26.6.24	14:15	Addis Abeba 3	S 32
Thales Deutschland	21	26.6.24	14:45	Addis Abeba 3	S 23
genua GmbH	22	27.6.24	11:15	Plenarsaal	S 25
HENSOLDT	23	27.6.24	11:45	Plenarsaal	A 07
Deutsche Telekom Geschäftskunden GmbH	24	27.6.24	12:15	Plenarsaal	A 11
Airbus Defence and Space	25	27.6.24	12:45	Plenarsaal	F 03
SOPHIST GmbH	26	27.6.24	13:15	Plenarsaal	R 53
Telespazio Germany GmbH	27	27.6.24	11:15	Addis Abeba 3	F 09
Carmenta Germany GmbH	28	27.6.24	11:45	Addis Abeba 3	W 11
Adva Network Security	29	27.6.24	12:15	Addis Abeba 3	N 04
NVIDIA GmbH	30	27.6.24	12:45	Addis Abeba 3	R 48
best Systeme GmbH	31	27.6.24	13:15	Addis Abeba 3	R 48

PLENARSAL

Speakercorner 1			
Nr.	Beginn	Firma/Organisation	Vortragende/r
1	11:15	Materna Information & Communications SE	Johannes Rosenboom Marco Schrader
2	11:45	CGI Deutschland B.V. & Co. KG	Jens Elstermeier Simon Purton
3	12:15	IBM Deutschland	Carsten Dieterle
4	12:45	dainox GmbH	Dipl. Ing. Jochen Brückner
5	13:15	RHEINMETALL	Dr.-Ing. Christian Martens
6	13:45	SThree GmbH	Timo Lehne
7	14:15	ESG Elektroniksystem- und Logistik-GmbH	Andreas Schiel
8	14:45	CONET	Dr. Fabian Reiser Dr. Christine Priplata
9	15:15	rola Security Solutions GmbH	Robert Schwerdtner
10	15:45	Secusmart GmbH	Dr. Christoph Erdmann
11	16:15	Sophos Technology GmbH	Jan Bakatselos
12	16:45	Constructor University Bremen gGmbH	Prof. Dr. Peter Baumann
13	17:15	Bechtle AG	André Alfter

Industrievorträge

ehemaliger Plenarsaal des Bundestages

Funktion	Thema
Senior Vice President Sales, Marketing & Business Development Public Sector, Director Sales, Fregattenkapitän d.R.	Verschlusssache to Go - vernetzte und sichere Kommunikation auf ultramobilen Endgeräten
Head of Business Development & Strategy bei CGI & Section Head (Capability Requirements) Senior Operations Research Analyst, Headquarters Supreme Allied Commander Transformation	AI Felix – Drei Erkenntnisse für KI-Projekte mit den Streitkräften
Technischer Leiter für Bundeswehr, BWI und Wehrtechnische Industrie	Bundeswehr: Digital und innovativ
Principal Network Solutions Consultant	Software Defined die Zukunft gestalten: Die Symbiose von flexibler Software und robuster
Head of BU Integrated Electronic Systems	Welche Rolle übernimmt die „alte“ Rüstungsindustrie im digitalen Zeitalter?
CEO	Megatrends managen – und trotz fehlender Fachkräfte den Anschluss nicht verlieren
Leiter Geschäftsfeld Kampf	Multi-Domain Operations End2End – Vom Sensor über den Shooter bis in die Munition
	Mit Lagebildern und technischen Dokumenten sprechen
Leiter Solution Design	Tiefenanalyse im Dienst der Sicherheit: Moderne IT-Lösungen für Militäroperationen
Managing Director	SecuSUITE Cross-Plattform – Give Users a Choice
Senior Sales Engineer	Zukunftssichere IT-Sicherheit – und welche Rolle spielen Mensch und KI?
Professor Constructor University CEO rassdaman GmbH	Mehr Nutzen aus Geo-Standards für das FMN?
Principal DevSecOps & Platform Engineering	Skalierbar, standardisiert, agil: beschleunigte Softwareentwicklung über verschiedene Clouds

Speakercorner 2

Nr.	Be-	Firma/Organisation	Vortragende/r
14	11:15	Rohde & Schwarz	Dr.-Ing. Patrick Grames
15	11:45	RUAG AG	Marco Schläppi
16	12:15	Materna Virtual Solution GmbH	Marco Schrader
17	12:45	Eviden Germany GmbH	Dr. Thomas Bierhoff
18	13:15	roda computer GmbH	Frau Laura Bertsch
19	13:45	Detecon International GmbH	Sebastian Lueken
20	14:15	Accenture	Stefan Donsa Accenture DACH
21	14:45	Thales Deutschland	Michael Kälber

16:15 - 17:45

Startup Pitch und Panel Session

Marktverfügbare Innovationen für die Zeitenwende

11 ausgewählte Startups präsentieren als Vertreter und Treiber von Innovation im öffentlichen Bereich ihre Lösungen auf der **Sonderausstellungsfläche R 63** einem breiten Publikum.

In unserer Startup Pitch und Panel Session **im Saal Addis Abeba 1 und 2** vertiefen wir den Dialog mit **Key Stakeholdern aus Industrie, Bundeswehr und dem öffentlichen Sektor** und stellen uns die Frage:

„Was ist in der Bundeswehr im Bereich Innovation im letzten Jahr passiert und wie kann Innovation noch zielgerichteter einfließen?“

Die aktuellen Entwicklungen im Bereich Defence Innovation werden reflektiert. Es folgen der BMVg Clusterlogik inhaltlich zugewiesene Startup-Pitches, deren Lösungen durch ein hochrangiges Panel diskutiert werden. Anschließend laden wir alle Teilnehmer herzlich zu einem gemeinsamen **Ausklang mit den Startups** ein.

Industrievorträge

Raum ADDIS ABEBA 3

Funktion	Thema
Special Projects	ESSOR – European Secure Software Defined Radio. Mit welchen Schritten wird die Funkinteroperabilität europäischer Streitkräfte endlich konkret ermöglicht?
ICT Senior System Architect	Krisenkommunikation - und wie kommunizieren Sie und Ihre Organisation in Zukunft?
Senior Account Manager Defense; Fregattenkapitän der Reserve	Der sichere ultramobile Arbeitsplatz: Per Smartphone und Tablet auf wichtige Fachanwendungen zugreifen. Schnell. Einfach. VS-NfD-konform.
CTO PSD&I DEU	Souveräne Digitalisierung und Ermöglichung von Multi Domain Operations: Erzeugung digitaler Wirkketten und durchgängiger Informationsräume als Element der Multi Domain Combat Cloud
Chief Commercial Officer CCO	Vernetzte Visualisierung
Senior Manager Public Sector	Quantentechnologien und ihr Potenzial, Wirtschaft, Verwaltung und Gesellschaft stark zu verändern
	Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit
Senior Manager Solutions	Möglichkeiten zur Erhöhung von Effizienz und Usability bei der Absicherung von Daten und Sprache im High Security Bereich



PLENARSAAL

Speakercorner 1			
Nr.	Beginn	Firma/Organisation	Vortragende/r
22	11:15	genua GmbH	Alexander von Gernler
23	11:45	HENSOLDT	Moritz Pichler
24	12:15	Telekom	Dipl.-Ing.(FH) Uwe Gschwind
25	12:45	Airbus Defence and Space	Markus Gerstl
26	13:15	SOPHIST GmbH	

ADDIS ABABA 3

Speakercorner 2			
Nr.	Beginn	Firma/Organisation	Vortragende/r
27	11:15	Telespazio Germany GmbH	
28	11:45	Carmenta Germany GmbH	Andreas Stiebner
29	12:15	Adva Network Security	Ulrich Kohn
30	12:45	NVIDIA GmbH	Michael Frings
31	13:15	best Systeme GmbH	Dipl.-Ing. (FH) Scharel Clemens

Industrievorträge

ehemaliger Plenarsaal des Bundestages

Funktion	Thema
Abteilungsleiter Research and Innovation	Souveräne Cloud: Eine geostrategisch-technische Analyse zu Cybersicherheit
Head of Ventures	HENSOLDT FCAS Accelerator – ein Paradigmenwechsel für das Innovationsmanagement in der Verteidigung
Digital Enabler, Presales Hyperautomation	Fokussierung auf Kernaufgaben durch Digitalisierung von Verwaltungsprozessen
Head of Sales Region D-A-CH für Space Connectivity	Weltraumgestützte Kommunikation für militärische Anwender
	KI oder Mensch – Wer ist besser im Systems Engineering?

Raum ADDIS ABEBA 3

Funktion	Thema
Head of Training Applications Section	Informationssicherheitskonzepte: Grundlagen und Notwendigkeit
Account Executive	Echtzeit Geodaten als Game-changer auf dem Gefechtsfeld
	Geschützte Glasfasernetze als Fundament einer hochsicheren Kommunikations-Infrastruktur: überwacht, resilient, quantensicher
Federal & Defense Lead	Sensorfusion, Metadatenextraktion und Datenreduktion in isolierten Edge-Systemen mit Nvidia Jetson
Leiter Entwicklung	COTS-Ketten sprengen - Moderne IT für Militärische Anwendungen Oder -> wie kann Ihr Unternehmen durch den Einsatz von MOTS profitieren? Ein Beispiel einer High-Performance-Switch-Modifikation (>100GBs) für die Luftfahrt

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
1	26.06.	11:15	ehem. Plenarsaal Bundestag	Johannes Rosenboom Marco Schrader	Senior Vice President Sales, Marketing & Business Development Public Sector Director Sales, Fregattenkapitän d.R.

Materna Information & Communications SE

Verschlusssache to Go - vernetzte und sichere Kommunikation auf ultramobilen Endgeräten

Ultramobile Geräte wie Smartphones und Tablets haben in Streitkräften sowie Behörden und Organisationen der öffentlichen Verwaltung signifikant an Bedeutung gewonnen. Damit diese Devices nahtlos in alle gängigen Workflows eingebunden werden können, die auch das Arbeiten mit Verschlusssachen beinhalten, bedarf es einer Weiterentwicklung der Sicherheitsarchitektur in Deutschland.

Das Ziel ist, neben einer vernetzten und sicheren Kommunikation mit verschlüsseltem Datenaustausch in der Bundeswehr und Bundesverwaltung, fachliche Aufgaben digital und mobil erledigen zu können. Auch die Verteidigungsindustrie hat das Potenzial erkannt. Der zunehmende Einsatz mobiler Endgeräte flexibilisiert die Kommunikation und das mobile Arbeiten für Soldaten und zivile Mitarbeiter. Dies ist ein entscheidender Schritt zu wirklich echten Ende-zu-Ende digitalisierten Prozessen zu gehen.

Die beiden führenden Hersteller Apple und Samsung bieten, stand heute, bereits eigene native Sicherheitsfeatures. Die passgenauen Lösungen der Materna-Gruppe erweitern diese gezielt und gewährleisten wichtige Sicherheitsniveaus, bei gleichzeitig hervorragender Nutzerfreundlichkeit.

Der Ansatz von Materna kombiniert die beiden zentralen Aspekte des mobilen Verwaltungsarbeitsplatzes der Zukunft: behördliche Fachlichkeit, geliefert aus der Materna Fachverfahrens-Manufaktur und die BSI-zertifizierte Sicherheit der Materna SecurePIM und TRUST Produkte. So geht digitale Souveränität „Made in Germany“!

MATERNA
Information & Communications

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
2	26.06.	11:45	ehem. Plenarsaal Bundestag	Jens Elstermeier & Simon Purton	Head of Business Development & Strategy bei CGI & Section Head (Capability Requirements) - Senior Operations Research Analyst, Headquarters Supreme Allied Commander Transformation

CGI Deutschland B.V. & Co. KG

AI Felix – Drei Erkenntnisse für KI-Projekte mit den Streitkräften

„Ich erhalte zu viele Informationen.“

„Ich habe keine Zeit, sie zu verarbeiten.“

„Ich kann die benötigten Informationen nicht finden.“

Diese drei Herausforderungen triggerten 2019 das NATO Supreme Allied Command Transformation (SACT) in Norfolk, sich mit dem Einsatz von künstlicher Intelligenz in geschlossenen Netzen – ohne Anbindung an Hyperscaler-Clouds – zu beschäftigen.

SACT ist der Überzeugung, dass die Herausforderungen, denen sich das Bündnis gegenüber sieht, am besten durch Innovation bewältigt werden können. Zur Unterstützung der Innovation hat das SACT eine Agenda zur Verbesserung der Kriegsführung aufgestellt, die auf eine digitale Umgestaltung der Arbeitsweise des Militärs abzielt. Ein Beispiel ist der Einsatz von Tools mit künstlicher Intelligenz, wie dem maschinenlernenden Wissensagenten im geheimen NATO-Netz namens AI FELIX, der sich als Kräfte-Multiplikator bewährt hat und ein greifbares Beispiel für Innovation in der Praxis darstellt.

Mit einem agilen Ansatz und enger Einbeziehung der Nutzer entstanden und entstehen Module, die dem Stab und dem einzelnen Nutzer die tägliche Arbeit vereinfachen und die Datenqualität erhöhen, um damit den Informationszugriff zu verbessern und Informationsüberlegenheit zu erzielen.

Im Laufe des Projektes haben sich drei Erkenntnisse ergeben, die im Vortrag herausgearbeitet werden: Technisch: volle Transparenz mit Zugriff auf den Code, besseres Verständnis der zugrunde liegenden Algorithmen, einfache Anpassung auf Nutzeranforderungen

Fachlich: Nutzbarkeit in der NATO als Ziel, schnelle Mehrwertgenerierung für die Testnutzer, danach Skalierbarkeit und unternehmensweiter Einsatz, immer am Puls der Zeit / Nutzer

Organisatorisch: Sicheres und verantwortliches Experimentieren, Schutz des trainierten Modells, Verantwortung und Transparenz durch Referenzieren und Zugriffsberechtigungen

CGI



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
3	26.6.	12:15	ehem. Plenarsaal Bundestag	Carsten Dieterle	Technischer Leiter für Bundeswehr, BWI und Wehrtechnische Industrie

IBM Deutschland

Bundeswehr: Digital und innovativ

Neuste Technologien und Trends. Digitalisierung braucht Innovation: Herausforderungen, Best Practices und Trends. Informations- und Wirkungsüberlegenheit stärken durch Künstliche Intelligenz und den Einsatz von Generative AI. Automation: Wie Geschäfts- und IT-Betrieb intelligenter, effizienter und Innovationen kräftig beschleunigt werden können.



Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
4	26.6	12:45	ehem. Plenarsaal Bundestag	Dipl. Ing. Jochen Brückner	Principal Network Solutions Consultant

dainox GmbH

Software Defined die Zukunft gestalten: Die Symbiose von flexibler Software und robuster Hardware

In der zivilen Welt ist „Software Defined Anything“ (SDx) in aller Munde. Bei dainox beschäftigen wir uns seit mehr als einer Dekade mit diesem Thema und haben 2019 bereits den Begriff des „Software Defined Mission Network“ (SDMN[®]) geprägt. Mit dem Beginn einer neuen Ära gewinnt „Software Defined Defence“ (SDD) in der gesamten Bundeswehr zunehmend an Bedeutung. Sie steht vor der Herausforderung, ihre Systemlandschaft zu modernisieren und zu flexibilisieren.

Dieser Vortrag beleuchtet die dynamische Beziehung zwischen der aktuellen und zukünftigen Systemlandschaft der Bundeswehr und den innovativen Ansätzen von SDD. Wir erkunden die IT-Architekturen und den serviceorientierten Ansatz der Bundeswehr, insbesondere im Kontext des Federated Mission Networking (FMN), gepaart mit den Erfahrungen aus F&T Studien sowie der Entwicklung und dem Betrieb von Bestandssystemen. Ein kritischer Blick wird auf die Herausforderungen geworfen, die sich im Rahmen der Planung, Dimensionierung, dem Deployment und dem Betrieb der zukünftigen Hardware-Plattformen ergeben. Dadurch wird die Notwendigkeit deutlich, flexible und resiliente Systeme zu entwickeln, die mit dem Software Defined Ansatz Schritt halten können. Besondere Aufmerksamkeit gilt auch den Container-Konzepten, die mit Hardware-Plattformen in verschiedenen Größenordnungen, eine Schlüsselrolle in der Gestaltung zukunftsfähiger Verteidigungssysteme spielen. Wir werden Vorstellungen und Fakten über den „Software Defined“ Ansatz entmystifizieren und einen realistischen Blick auf die Möglichkeiten und Grenzen dieser Technologien werfen.

Ziel ist es, ein umfassendes Verständnis dafür zu schaffen, wie SDD und robuste Hardware zusammenwirken können, um eine effiziente, flexible und zukunftssichere Verteidigungslandschaft zu gestalten. Dieser Vortrag richtet sich an militärisches und ziviles Fachpersonal und Führungskräfte, Entscheidungsträger in der Verteidigungsindustrie, IT- und Cybersecurity-Experten, sowie an Akademiker und Forscher, die an der Schnittstelle von technologischer Innovation und moderner Verteidigungsstrategie arbeiten.



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
5	26.6.	13:15	ehem. Plenarsaal Bundestag	Dr.-Ing. Christian Martens	Head of BU Integrated Electronic Systems

RHEINMETALL

Welche Rolle

übernimmt die „alte“ Rüstungsindustrie im digitalen Zeitalter?

Die Medien berichten aktuell fast täglich von Innovationen und jungen Unternehmen, die im Bereich der Verteidigungsfähigkeit entstehen. Das digitalisierte Gefechtsfeld ist breit und tief. Und es ist komplex, denn auch digitale Produkte und Fähigkeiten sind nicht per se interoperable untereinander, aber sie bieten deutlich mehr Vernetzungsmöglichkeiten, als es in der bisherigen Produkt-Landschaft der Fall war. Durch diese Relationen entstehen kausale Zusammenhänge und dadurch steigt die Komplexität. Rheinmetall hat erkannt, dass es nicht die jungen kleineren Unternehmen sein können, die diese Komplexität beherrschen werden, sondern dass es die Unternehmen sein müssen, die als Systemhäuser breit aufgestellt sind und somit durch das breite Portfolio eine umfassende Bewertungsfähigkeiten haben. Unsere Aufgabe muss und wird es sein, die Komplexität beherrschbar zu machen und Innovationen in die Produkt- besser gesagt in die Kriegstauglichkeit zu bringen. Wir nehmen diese Verantwortung an und haben im Januar diesen Jahres die Entscheidung zur digitalen Transformation unseres Unternehmens angenommen. Mit unserem neuen CDO Dr. Timo Haas entwickeln wir derzeit ein Team auf Corporate-Level, das die Aufgabe hat ein Lösungs-Ökosystem zu bilden mit dem geteilten Wertversprechen des digitalisierten Gefechtsfeldes - Multi-Domain. Zukünftig wird die Aufgabe der Rheinmetall nicht mehr darin bestehen, selbst in allen Bereichen tiefe Wertschöpfung durch eigene Produkte zu erreichen, sondern die richtigen Partner global zu finden, um den militärischen Nutzern die besten technologischen Möglichkeiten anbieten zu können und zwar Schritt für Schritt interoperable by Design. Taking responsibility in a changing world.



RHEINMETALL

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
6	26.6.	13:45	ehem. Plenarsaal Bundestag	Herr Timo Lehne	CEO

SThree GmbH

Megatrends managen – und trotz fehlender Fachkräfte den Anschluss nicht verlieren

Wenn Deutschland als Wirtschaftsstandort in 2024 wettbewerbsfähig bleiben will, sehen sich Unternehmen früher oder später mit den „globalen Megatrends“ konfrontiert. Digitalisierung, New Work, Dekarbonisierung, Research-led Healthcare und der demographische Wandel sind Themen, mit denen sich Unternehmen auseinandersetzen müssen, um nicht langfristig den Anschluss zu verlieren. Die Lösungen dafür sind allesamt technologisch und verlangen nach Fachkräften aus dem MINT-Bereich. Die Digitalisierung stellt Unternehmen auf der ganzen Welt vor große Herausforderungen: Mit dem Aufstieg der Künstlichen Intelligenz (KI) und der durch Corona angetriebenen digitalen Transformation eröffnen sich jedoch zeitgleich auch große Job-Motoren. Arbeitnehmer*innen stehen dieser Entwicklung bislang skeptisch gegenüber: Laut der SThree Studie „How the STEM world evolves“ fürchten 34%, dass sie ihre Jobs durch KI verlieren werden. Gartner hingegen sagt eine überwiegend positive Auswirkung voraus, mit über einer halben Milliarde zusätzlichen Arbeitsplätzen bis 2033. KI kann also durchaus dazu beitragen, den Fachkräftemangel zu minimieren, indem sie Arbeitnehmer*innen bei Routineaufgaben entlastet und somit die Produktivität verbessert. Ob es soweit kommt, liegt jedoch an den Unternehmen selbst und daran, wie schnell und mit welchem Mindset sie sich den Megatrends stellen. Denn Faktoren wie der demografische Wandel tragen Tag für Tag dazu bei, dass der Fachkräftemangel weiter massiv zunimmt. Unternehmen können jetzt schon proaktiv handeln, indem sie beispielsweise ungenutzte Recruiting-Potenziale erschließen und den internationalen Bewerbermarkt nutzen, eine echte Willkommenskultur etablieren und Initiativen zur Begeisterung junger Frauen für MINT-Fächer unterstützen. Offenheit gegenüber Quereinsteiger*innen und der Generation 55+ ist ebenfalls entscheidend. Die Fähigkeiten dieser Gruppen bringen neue Perspektiven und treiben Innovationen voran. Jedes Unternehmen sollte deshalb klar definieren, welches Know-how benötigt wird und wie es durch gezielte Weiterbildung an Quereinsteiger*innen und ältere Berufserfahrene vermittelt werden kann. Zitat Timo Lehne: „Aktuelle Herausforderungen lassen sich nur mit MINT-Expertise, Mut und Innovationsgeist stemmen.“

Kurzvita Timo Lehne: Timo Lehne ist CEO der auf die MINT-Branche spezialisierten Personalberatung SThree. Er verantwortet das Umsetzen der globalen Unternehmensstrategie, das Erreichen der Unternehmensziele und die Leitung eines mehr als 2.900-köpfigen Teams. 2006 begann er seine Karriere bei SThree, 2017 übernahm er als Managing Director die Führung der DACH-Region.



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
7	26.6.	14:15	ehem. Plenarsaal Bundestag	Andreas Schiel	Leiter Geschäftsfeld Kampf

ESG Elektroniksystem- und Logistik-GmbH

Multi-Domain Operations End2End – Vom Sensor über den Shooter bis in die Munition

Die Integration von Multi-Domain Operations (MDO) in moderne militärische Systeme bringt eine Reihe von Herausforderungen mit sich, die weit über die herkömmlichen Anforderungen an Sensor-to-Shooter-Netzwerke hinausgehen. Durch die Einbindung mehrerer Domänen wird die Wahrscheinlichkeit von Sicherheitsgefällen erhöht, ebenso wie die Notwendigkeit, domänenspezifische Informationsübertragungsmittel wie spezialisierte Funkgeräte zu nutzen. Jedoch reicht der bloße Austausch von Informationen zwischen verschiedenen Domänen nicht aus, um den Anforderungen eines modernen Gefechts im Rahmen von MDO gerecht zu werden. Es bedarf einer umfassenden, von Anfang an integrierten Ende-zu-Ende-Vernetzung. In der gängigen Diskussion um den Sensor-to-Shooter-Ansatz wird oft übersehen, dass der „Shooter“, insbesondere bei der Verwendung moderner intelligenter Munition, lediglich ein Zwischenelement darstellt. Eine echte Ende-zu-Ende-Vernetzung erfordert, dass Informationen von einem Sensor direkt in die Munition übertragen werden. Der Vortrag wird sich nicht nur mit diesen Überlegungen beschäftigen, sondern auch auf die spezifischen Herausforderungen bei der Umsetzung eingehen. Es wird argumentiert, dass allgemeine Konzepte wie „Cloud Computing“ nicht ausreichen, um diese Herausforderungen zu bewältigen. Vielmehr müssen die technischen Herausforderungen konkret benannt und angegangen werden, um effektive Lösungen zu finden. Abschließend wird ein optimistischer Ausblick geboten, in dem aufgezeigt wird, wo innerhalb der Bundeswehr bereits wesentliche Bestandteile für Multi-Domain Operations erfolgreich implementiert wurden. Dies bietet eine Grundlage für weitere Entwicklungen und Verbesserungen in diesem schnell fortschreitenden Bereich der Militärtechnologie. Die ESG ist herstellerunabhängiger Systemintegrator und der nationale Technologie- und Innovationspartner für Verteidigung und öffentliche Sicherheit. Wir treiben mit unseren Lösungen und Services die sichere Digitalisierung und Vernetzung in allen Dimensionen voran. Dabei übernehmen wir die Entwicklung, Realisierung, Betreuung und den Betrieb einzelner Plattformen und komplexer Gesamtsysteme.

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
8	26.6.	14:45	ehem. Plenarsaal Bundestag	Dr. Fabian Reiser, Dr. Christine Priplata, Dr. Colin Stahlke	

CONET

Mit Lagebildern und technischen Dokumenten sprechen

„Als Erster wissen, was passiert; schnell und präzise eine Lage verstehen und Entscheidungen fällen. Mit der Flut an multimedialen Daten, Sensorsystemen und neuen technologischen Möglichkeiten werden diese Herausforderungen immer größer. Lagebilder sind dabei der zentrale Anlaufpunkt für Datenströme. Sie dienen als Informationsquelle und bilden die Grundlage der Entscheidungsfindung. Generative Künstliche Intelligenz (KI) bietet neuartige Möglichkeiten, Texte, Bilder und beispielsweise Geodaten wesentlich leichter zu verstehen, automatisiert Themen und Zusammenhänge zu erkennen sowie Anweisungen präzise zu befolgen. Dabei können große Sprachmodelle (Large Language Models / LLMs) direkt auf umfangreiche interne Datenbestände oder das Weltwissen zugreifen. Indem diese Daten direkt befragt werden können, werden Informationen verfügbarer. Diese direkte Interaktion und intelligente Unterstützung vereinfacht die Auswertung von hochkomplexen Situationen. Gleichzeitig erhöht sich die Qualität der Automatisierung deutlich. Bisher verborgene Informationen sind in Echtzeit zugänglich und durch geeignete Visualisierung begreifbar. Dieser Zuwachs an Fähigkeiten und die bessere Beherrschung der Lage stärken die Resilienz, auch im Hinblick auf neue Bedrohungsszenarien aus den Bereichen Cyber-Kriminalität und Desinformation sowie im Umgang mit Krisen. Wir geben anschauliche Einblicke in das zukünftige Lagebild sowie die KI-gestützte smarte Assistenz zur Kommunikation mit komplexen Dokumenten, zum Beispiel mit technischen Handbüchern. Zudem sehen wir uns mögliche Angriffe auf LLMs an. Die grundlegenden Einsichten und praktischen Beispiele zeigen die Möglichkeiten für ein ganz neues Level an Assistenz, eröffnet durch die Zusammenführung unterschiedlicher Technologien und Intelligence-Disziplinen.“





Nr.	Tag	Zeit	Ort	Vortragender	Funktion
9	26.6.	15:15	ehem. Plenarsaal Bundestag	Robert Schwerdtner	Leiter Solution Design

rola Security Solutions GmbH

Tiefenanalyse im Dienst der Sicherheit: Moderne IT-Lösungen für Militäroperationen

Entscheidungen auf operativer, taktischer und strategischer Ebene erfordern stets ein aktuelles Lagebild. Die Handlungsfähigkeit in militärischen Operationen hängt dabei entscheidend von der Geschwindigkeit bei der Zusammenführung relevanter Informationen und deren Verarbeitung ab. Wer als Erster die Informationen zusammenführt, relevante Daten extrahiert, versteht und in ein Lagebild überführt, hat in kritischen Situationen den entscheidenden zeitlichen Vorteil. Leistungsstarke Softwarelösungen tragen dazu bei, das verfügbare Wissen effektiv zu nutzen und in nachvollziehbare Lagebilder zu übersetzen.

Erfahren Sie in diesem Vortrag, wie moderne Technologien die Bundeswehr dabei unterstützen, hochrelevante, offene Informationskanäle für eine Tiefenanalyse zu nutzen. Die KI-gestützte Auswertung von Bild- und Videosignalen mithilfe individueller militärischer Klassifizierer, OCR-Texterkennung, Transkription und Übersetzungsmöglichkeiten trägt dazu bei, den entscheidenden Zeitvorteil bei der Auswertung und Analyse zu gewinnen. Die Erkenntnisse werden in gesicherten Netzwerken (on-premises) konsolidiert, um die Integration weiterer Informationsquellen zu ermöglichen. Die nahtlose Datenfusionierung liefert so ein belastbares und nachvollziehbares Grundlagenwissen. Ein strukturierter Intelligence Knowledge Graph und die quellenbasierte Erfassung relevanter Daten unterstützt zudem die kollaborative Analyse, ein nahtloses Reporting und wird den hohen Sicherheitsanforderungen gerecht.

Wir freuen uns darauf, Ihr Interesse an KI-basierten Lösungen zu vertiefen und mit Ihnen in den Austausch zu treten. Für weiterführende Informationen und persönliche Gespräche stehen wir Ihnen gerne zur Verfügung. Besuchen Sie uns auch am Stand F06 im Foyer.

rola.

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
10	26.6.	15:45	ehem. Plenarsaal Bundestag	Dr. Christoph Erdmann	Managing Director

Secusmart GmbH

SecuSUITE Cross-Platform – Give Users a Choice

„Ab sofort haben Sie die Wahl:

Die digitale Verwaltung steht vor der Herausforderung, neue Arbeitsweisen anzunehmen, um effizienter und sicherer zu arbeiten. Die Attraktivität eines digitalen Arbeitsplatzes wird immer wichtiger, sowohl für Organisationen als auch für Mitarbeiter. Dabei ist es entscheidend, das passende Gerät für den jeweiligen Anwendungsfall zu wählen und Flexibilität, Anpassungsfähigkeit und Resilienz zu gewährleisten. Secusmart, als Marktführer für Mobilprodukte im Segment VS-NfD, bietet essentielle Applikationen für die digitale Verwaltung auf iOS iNDIGO und Samsung Knox an. Nach erfolgreicher Evaluierung durch das BSI wurden iPhones und iPads in einer sicheren Konfiguration für die Verarbeitung von VS-NfD-Daten freigegeben. Secusmarts neue SecuSUITE for iOS (SS4iOS) ergänzt Apple iNDIGO ideal, indem sie den Funktionsumfang für den produktiven behördlichen Einsatz erweitert. SS4iOS konzentriert sich auf die Kernbedürfnisse der Anwender bei der Kommunikation, dem Zugriff auf Informationen sowie deren Verarbeitung über Smartphones und Tablets. Die langjährige Erfahrung von Secusmart mit den Anforderungen der Bundesverwaltung spiegelt sich auch in den Apps der SecuSUITE for iOS wider. Die wichtige App SecuVOICE ist wichtiger denn je und Bestandteil beider Lösungen. Welche Plattform für Sie und Ihre Einrichtung wichtig ist, erläutert Ihnen Dr. Christoph Erdmann in seinem Vortrag.“

 **BlackBerry**[®]

secusmart[®]



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
11	26.6.	16:15	ehem. Plenarsaal Bundestag	Jan Bakatselos	Senior Sales Engineer

Sophos Technology GmbH

Zukunftssichere IT-Sicherheit – und welche Rolle spielen Mensch und KI?

- Wie stelle ich meine IT-Sicherheit langfristig zukunftssicher und resilient auf?
- Welche Rollen spielen dabei Technologie inklusive KI und menschliche Experten?
- Wie hilft mir Sophos Managed Detection and Response dabei, Investitionen zu sichern und Kosten zu sparen?

Cyberangriffe mit Ransomware, Datendiebstahl und Betriebsunterbrechung sind heute die Existenzbedrohung Nr. 1 für Behörden und Unternehmen. Um Hacker frühzeitig erkennen und stoppen zu können, benötigen Organisationen mehrere Voraussetzungen. Neben modernen Werkzeugen inklusive KI-Unterstützung zum Schutz und zur Erkennung von Cyberangriffen werden Experten benötigt, die diese Werkzeuge rund um die Uhr bedienen und wissen, wie im Falle eines Angriffs vorzugehen ist.

Sophos MDR bietet einen 24/7 Managed SOC Service mit Spezialisten im Bereich Bedrohungserkennung, Analyse und Incident Response – und nutzt dazu neben Sophos Werkzeugen auch bereits vorhandene Werkzeuge von Drittherstellern in den Bereichen Endpoint, Firewall, NDR, Email, IAM und Cloud Security.

SOPHOS

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
12	26.6.	16:45	ehem. Plenarsaal Bundestag	Prof. Dr. Peter Baumann	Professor Constructor University CEO, rassdaman GmbH

Constructor University Bremen gGmbH

Mehr Nutzen aus Geo-Standards für das FMN?

Die Gewinnung, Aufbereitung und Verknüpfung sowie die empfängergerechte Bereitstellung der benötigten Information trotz aller Heterogenität von Daten und Akteuren sind zentrale Herausforderungen für Interoperabilität im Federated Mission Network (FMN) der NATO.

Insbesondere pixel-orientierte Sensoren an Land, über oder unter Wasser, in der Luft und im Weltraum liefern „Big Data“ Ströme mit all ihren Problemen. Im zivilen Bereich arbeitet das Open Geospatial Consortium (OGC) mit ISO zusammen, um Interoperabilität in vernetzten Datenströmen und Diensten zu erreichen; über die OGC Defence and Intelligence Working Group (D&I.DWG) besteht auch eine Verbindung in den militärischen Bereich und die Standardisierung von STANAG etc. Speziell für raum-zeitliche Daten existiert das Konzept der „Coverages“, welches insbesondere Rasterdaten und Datenwürfel modelliert. In OGC/ISO werden dazu Daten- und Prozessierungsmodelle bereitgestellt, welche u.a. auch von INSPIRE, der europäischen vereinheitlichten Geo-Dateninfrastruktur, übernommen sind. Werkzeuge auf Basis dieser Coverage-Standards sind in Industrie, Forschung und Behörden im aktiven Einsatz.

Im Vortrag wird der aktuelle Stand der Standardisierung vorgestellt, inklusive der Planungen. Anhand exemplarischer Implementierungen auf Basis der Referenzimplementierung rassdaman wird Interoperabilität in Live-Demos illustriert. Besonderes Augenmerk wird den Anforderungen von FMN gewidmet. Die Präsentation fußt auf 17 Jahren aktiver Beteiligung in der Standardisierung als Editor, Projektleiter und Chair mehrerer Arbeitsgruppen.

rassdaman
raster data manager



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
13	26.6.	17:15	ehem. Plenarsaal Bundestag	André Alfter	Principal DevSecOps & Platform Engineering

Bechtle AG

Skalierbar, standardisiert, agil: beschleunigte Softwareentwicklung über verschiedene Clouds hinweg

Ob bei der Digitalisierung von Lagebildern und Landoperationen, der Krisenfrüherkennung oder bei Multi Domain Operations - Cloud gehört zu den wichtigsten Technologien für die Bundeswehr. Doch die am Markt vorhandenen Cloud-Anwendungen der verschiedenen Anbieter können nicht alle 1:1 von der Bundeswehr genutzt werden.

Insbesondere die Sicherheitsanforderungen erfordern individuelle Maßnahmen und maßgeschneiderte Lösungen. Hier kommt die neue Entwicklerplattform „Internal Developer Platform“ (IDP) von Bechtle ins Spiel. Die Plattform gewährleistet eine standardisierte Developer Experience über verschiedene Clouds hinweg, einschließlich Azure und der isolierten privaten Cloud von Bechtle. Die IDP ermöglicht es, eine Code-basierte Abstraktionsschicht einzusetzen. Diese wiederum ermöglicht eine Open-Source-Workload-Spezifikation und bietet letztlich den Vorteil, dass Entwickler kein spezifisches Cloud-Wissen mehr benötigen.

Sich daraus weiterhin ergebende Vorteile liegen auf der Hand: Durch Standardisierung entfallen infrastrukturbezogene Herausforderungen, der Fokus kann auf die eigentlichen Entwicklungsaufgaben konzentriert werden. Und das bedeutet Effizienzgewinn und höhere Produktivität. In Summe ein wichtiger Beitrag zur digitalen Souveränität.

Im Vortrag wird anhand eines Air-Gapped-Szenarios aus der Praxis die Funktionsweise sowie Vorteile der Internal Developer Platform aufgezeigt.



Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
14	26.6.	11:15	Addis Abeba 3	Dr.-Ing. Patrick Grames	Special Projects

Rohde & Schwarz

ESSOR – European Secure Software Defined Radio.

Mit welchen Schritten wird die Funkinteroperabilität europäischer Streitkräfte endlich konkret ermöglicht?

Verbindung halten und führen können, sind wesentliche Eckpfeiler der vernetzten, militärischen Operationsführung. Nationale Streitkräfte benötigen daher über deren Teilstreitkräfte hinweg unbedingt sichere, verschlüsselte und national interoperable Funkkommunikationslösungen.

Im Bereich der deutschen Landstreitkräfte ist die Basis hierfür durch die Vergabe der Elemente für D-LBO Basic geschaffen worden. Darauf aufbauend besteht Bedarf für die Interoperabilität für die verschiedenen Streitkräfte der multinationalen Bündnispartner untereinander. Basierend auf jeweiliger nationaler Führungsfähigkeit müssen sie sich via Sprach- und Datenfunk gegenseitig und medienbruchfrei vernetzen können. Die multinationale Sicherung der europäischen Ostflanke, die auch durch den Aufbau einer deutschen Brigade in Litauen gelingen wird, ist nur ein Beleg dafür, dass europäische Interoperabilität in der militärischen Kommunikation bereits heute keine Theorie mehr sein kann.

Vereint durch die Leitidee von ESSOR und unter dem Management der OCCAR arbeiten Spanien, Italien, Frankreich, Finnland, Polen und Deutschland gemeinsam für dieses Ziel. Auf den nationalen vertrauenswürdigen Funkgerätefamilien der jeweiligen nationalen Champions, die nach dem Software Defined Radio-Prinzip funktionieren, wird eine gemeinsame Wellenformfamilie entstehen.

Dieser Beitrag beleuchtet, welche konkreten Vorhaben in den nächsten Monaten und Jahren die Interoperabilität und damit Verteidigungsbereitschaft und Kampfkraft der europäischen Partner verbessern werden. Ausgehend von den Wellenformen, die im Rahmen des European Defense Investment Program (EDIDP) entstehen, wird die direkte Einwirkung in Zukunftsprogramme wie D-LBO, FCAS (Future Combat Air System) und MGCS (Main Ground Combat System) dargestellt.



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
15	26.6.	11:45	Raum Addis Abeba 3	Marco Schläppi	ICT Senior System Architect

RUAG AG

Krisenkommunikation - und wie kommunizieren Sie und Ihre Organisation in Zukunft?

Krisensituationen sind ein Fakt und stellen uns laufend vor neue Herausforderungen. Wo die zivilen Einsatzkräfte an ihre Kapazitätsgrenzen stossen, können die Armeen einen wesentlichen Unterstützungsbeitrag leisten.

Für die Kommunikation ist es das A und O, dass die Armee mit den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) zusammenarbeiten. Das bedeutet, dass die Kommunikationsmittel bereichsübergreifend miteinander funktionieren müssen, damit alle Dienststellen gemeinsam kommunizieren können.

Vernetzung alleine genügt dabei schon lange nicht mehr. Eine Plattform oder Kommunikationssysteme, die nur durch einen Akteur genutzt werden können, ist dabei nicht mehr ausreichend. Erst die Interoperabilität aller Kommunikationssysteme und Lagebildprogrammen ermöglichen die Führungsfähigkeit in allen Lagen und besonders auch in Krisensituationen.

RUAG hat sich dazu entschieden, das Zusammenführen all dieser Elemente zu einer Priorität zu machen. Dabei strebt RUAG eine organisationsübergreifende und mobile Kommunikationsplattform an. Unter dem Arbeitstitel «House of Guardian» könnte somit die Grundlage geschaffen werden, dass sowohl die Armee als auch die BOS unterbruchfrei kommunizieren können. Dabei wird ein Hauptaugenmerk auf die Integrität und Vertraulichkeit gelegt.

Es soll eine Komplettlösung entstehen, welche Smartphone Endgeräte über sichere Applikationen, die Nutzung von Mission Critical Netzwerken bis hin zur Nutzung von SciON beinhaltet. Damit kommt RUAG den wachsenden Bedürfnissen nach, schneller und effizienter in allen Lagen zu kommunizieren.

RUAG



Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
16	26.6.	12:15	Raum Addis Abeba 3	Marco Schrader	Senior Account Manager Defense Fregattenkapitän d.R.

Materna Virtual Solution GmbH

**Der sichere ultramobile Arbeitsplatz:
Per Smartphone und Tablet auf wichtige Fachanwendungen zugreifen.
Schnell. Einfach. VS-NfD-konform.**

Nicht nur die Einsatz- und Streitkräfte sondern auch die Verwaltung in der Bundeswehr stehen vor ganz speziellen Herausforderungen: Sie müssen schneller und mobiler werden. Ohne digitale Lösungen wird das nicht gehen. Dabei spielt die ultramobile Kommunikation und Kollaboration per Tablet und Smartphone eine wichtige Rolle. Dafür werden hochsichere Anwendungen benötigt, die den besonderen Sicherheitsanforderungen der Truppe gerecht werden.

In ihrem Vortrag beleuchten Marco Schrader, Senior Account Manager Defense bei Materna Virtual Solution und Fregattenkapitän der Reserve, sowie Herr Gert Stiewi, Geschäftsführer bei SMS System-Management Stiewi, dessen Travel-Managementsystem im Verteidigungsumfeld vielerorts Anwendung findet, anhand konkreter Beispiele, wie ein ultramobiler Arbeitsplatz im Bundeswehr-Umfeld aussehen kann. Im Vordergrund stehen dabei die Sicherheitsmechanismen und Vorteile containerbasierter, verschlüsselter Lösungen. Sie ermöglichen den sicheren Zugriff auf interne Informationen und webbasierte Fachanwendungen per Smartphone und Tablet. Daten und Applikationen sind dabei jederzeit so geschützt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine VS-NfD-Zulassung für iOS, eine Einsatzerlaubnis für Android sowie eine Einsatzerlaubnis für NATO RESTRICTED erteilt hat. Neben wichtige Office-Funktionen, sorgt ein sicherer Intranet-Browser für den ultramobilen Zugriff auf spezifische Fachanwendungen, sodass auch von unterwegs aus, wichtigste Aufgaben und Prozesse mobil abgebildet und erledigt werden können, selbst, wenn es um sensible Informationen des Geheimhaltungsgrades „VS-NfD“ geht. So wird es beispielsweise möglich, mobil auf ein hochsicheres Travel-Management zuzugreifen. Von der Antragstellung über Genehmigung und Buchung bis zur Auszahlung können diese Vorgänge sicher per Smartphone oder Tablet abgewickelt werden.

MATERNA
Virtual Solution

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
17	26.6.	12:45	Raum Addis Abeba 3	Dr. Thomas Bierhoff	CTO PSD&I DEU

Eviden Germany GmbH

Souveräne Digitalisierung und Ermöglichung von Multi Domain Operations: Erzeugung digitaler Wirkketten und durchgängiger Informationsräume als Element der Multi Domain Combat Cloud

Im Zuge der fortschreitenden Digitalisierung setzt die Bundeswehr und deren Partner zunehmend auf Software-definierte Funktionalität in militärischen Systemen und Verfahren (Software Defined Defence). D.h. sowohl neue Funktionalität wird mittels Software digital zur Verfügung gestellt als auch die digitale Automation etablierter Arbeitsabläufe ermöglicht. Einsatztaugliche Ausprägung der Technologien, einfache Bedienbarkeit und Betrieb sowie die Fähigkeit zur sicheren, systemübergreifenden Vernetzung verschiedener Technologien sind essenziell. Hierzu ist der Paradigmenwechsel hin zur Datenzentrierung unerlässlich, um von vornherein die weitere Verwertung in anderen Services sowie eine agile Nutzung und Weiterentwicklung zu ermöglichen. Bedingt durch begrenzte Ressourcen und dynamischere Szenarien ist die Erzielung zeitnaher praktischer Fortschritte unerlässlich. Hierzu sind die einsatztaugliche Ausprägung der Technologien und einfache Nutz- und Betriebsfähigkeit, die Etablierung und Aufrechterhaltung digitaler Souveränität sowie die Fähigkeit zur sicheren übergreifenden Vernetzung verschiedener Technologien und die Fähigkeit zur flexiblen Weiterentwicklung essenziell. Der Vortrag erläutert anhand eines anschaulichen Beispiels mit konkreten marktverfügbaren Lösungsbausteinen die praktische Vernetzung relevanter Sensoren und Effektoren, um einen Zeitvorteil in der Kette Sensor-to-Shooter zu erlangen. Dies leistet einen Beitrag zur Erlangung der Fähigkeit der Bundeswehr ihre Gegner aus verschiedenen Dimensionen heraus gleichzeitig bedrohen zu können. Die Umsetzung erfolgt auf Grundlage zur Multi Domain Combat Cloud als einer virtuellen Service Plattform. Jene stellt die erweiterte, missionspezifische Vernetzung der multiplen IT-Elemente der Dimensionen sowie weiterer relevanter Services und relevanter Netzwerke zur Daten- und Informationsübertragung stationärer, verlegefähiger und mobiler Ebene zum gemeinsamen Informationsraum zur Verfügung. Hierbei stehen nicht einzelne (System-)Plattformen oder Applikationen, sondern die datenzentrische Vernetzung aller Services im Vordergrund.

EVIDEN

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
18	26.6.	13:15	Raum Addis Abeba 3	Frau Laura Bertsch	Chief Commercial Officer CCO

roda computer GmbH

Vernetzte Visualisierung

Die vernetzte Visualisierung ist ein multidisziplinärer Ansatz, der Datenvisualisierung mit modernen Technologien und Kommunikationskonzepten sowie IT Sicherheit verbindet. Sie ermöglicht es, komplexe Informationen und Daten in Echtzeit zu erfassen, rollen- oder zuschauerspezifisch konfiguriert darzustellen und zu analysieren. Nationale und internationale Operationszentren sind ein zunehmend integraler Bestandteil vieler militärischer Strukturen und Missionen, in denen ein ständiger Zugriff auf mehrere Informationsströme in unterschiedlichen Sicherheitsdomänen, die in Echtzeit visualisiert werden und sichtbar gemacht werden, unabdingbar ist. Moderne Operationszentren verfügen in der Regel über eine große Videowand für den gemeinsamen Zugriff und die Visualisierung von Daten und Gruppenanalysen sowie über Einzelarbeitsplätze. Diese Arbeitsstationen haben Zugriff auf dieselben Daten wie die große Videowand sowie auf zusätzliche Informationen, so dass spezialisierte Bediener, die für ihre spezifischen Stabsaufgaben erforderlichen Zusatzinformationen abrufen können. In diesen Bereichen sind die Befehlsgeber auf eindeutige und ununterbrochene visuelle Informationen angewiesen, um Einsatzlagen zu überwachen, eigene Kräfte zu führen und die Einsätze der Teams zu koordinieren. Vor allem aber sind die Informationen in Operationszentralen die maßgebende Grundlage für taktische Operationen und die Bewertung von Bedrohungen. Für einen möglichst effizienten Betrieb müssen die Bediener in den Kontrollräumen über aktuelle, genaue und vollständige Informationen verfügen. Diese Daten müssen ihnen auf nachvollziehbare und logische Weise präsentiert werden, und zwar in einem Layout, das bei Bedarf schnell angepasst werden kann, damit sie schnell auf veränderte Situationen und Notfälle reagieren können. Die hoch sensiblen Daten sind durch ein IT-Sicherheitskonzept geschützt, damit keine vertraulichen bzw. eingestufteten Information ungeschützt nach außen dringen können. Durch die Kombination von marktführenden Display-Technologie mit extrem leistungsstarken sowie zuverlässigen Videowand-Verarbeitungslösungen inklusive der gesamten Netzwerkarchitektur bietet roda schlüsselfertige Lösungen für bestehende und zukünftige Kontrollräume und Operationszentralen. Dabei bieten die Großbildwände mit Bildverbesserungstechnologie optimierte Bilder und sorgen für hohe Sichtbarkeit im 24/7 Betrieb. Der modularer Systemaufbau ermöglicht kundenspezifische Displayformate, zugeschnitten auf die jeweilige Videowände. Dabei bietet roda aus einer Hand das vollständige Konzept, den Aufbau mit Installation bis hin zur Serviceleistung während der Nutzung.

roda
RUGGED IT & ELECTRONICS

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
19	26.6.	13:45	Raum Addis Abeba 3	Sebastian Lueken	Senior Manager Public Sector

Detecon International GmbH

Quantentechnologien und ihr Potenzial, Wirtschaft, Verwaltung und Gesellschaft stark zu verändern

Quantentechnologien sind eine Zukunftstechnologie mit disruptivem Potenzial. Auch wenn sie sich derzeit noch in einem vergleichsweise frühen Entwicklungsstadium befinden, zeichnen sich bereits umfangreiche und vielversprechende Anwendungsperspektiven ab, die deutlichen Einfluss auf die Leistungserstellung in Wirtschaft und Verwaltung haben werden. Für Verteidigung, Innere Sicherheit und öffentliche Verwaltung relevante Beispiele sind die Quantenkommunikation und Quantenkryptografie, die die Sicherheit von Daten und Kommunikation erhöhen, indem sie abhörsichere Kommunikationskanäle bereitstellen. Ein weiterer Anwendungsfall ist Quantencomputing, das komplexe Berechnungen erlaubt, die die Datenanalyse verbessern und somit die Effizienz von Verwaltungsprozessen steigern. Quantensimulation macht es möglich, komplexe Systeme genauer vorherzusagen und durch Routenoptimierung die Effizienz von Logistik- und Transportprozessen zu optimieren. Äußerst relevant sind darüber hinaus die Quantum Enabling Technologies. Diese stellen eine kritische Komponente für die Wertschöpfung dar und sind damit ein wichtiger Bestandteil zum Erhalt der technologischen Souveränität. Insbesondere in zukunftsgerichteten Technologiefeldern ist die digitale Souveränität Deutschlands und Europas von elementarer Bedeutung. Dies wird nicht nur bei den erwarteten Leistungen der Quantentechnologie im Bereich von Datenverschlüsselung, aber auch der Datenentschlüsselung als Angriffsfläche für die Sicherheit deutlich. Derzeit hat Deutschland in den genannten Technologiefeldern gute Chancen, eine stabile Position einzunehmen. Wir zeigen, was es bedarf, um diese Position im internationalen Vergleich zu halten und auszubauen: ein ganzheitliches Ökosystem, das geeignete Strukturen zur Verfügung stellt, die enge Kooperation von Industrie und Wissenschaft sowie die frühe Einbindung der Anwender in den weiteren Entwicklungsprozess.

DETECON

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
20	26.6.	14:15	Raum Addis Abeba 3	Stefan Donsa Accenture DACH	

Accenture

Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit

Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit Der Vortrag „Adoption, Anpassung und Risiko: Generative KI und nationale Sicherheit“ beleuchtet die zentrale Herausforderung, vor der sowohl militärische als auch zivile Sicherheitsorganisationen stehen: Die Integration der bahnbrechenden Technologie der generativen KI in nationale Sicherheitsstrategien. Die weltweite Verbreitung dieser Technologie führt zu einem Paradoxon, das in der komplexen Abwägung von Chancen und Bedenken sowie im zunehmend exponentiellen Risiko bei Nicht- oder Langsamadoption liegt. Die geopolitische Dringlichkeit ist unübersehbar, da nicht eingeschränkte staatliche und kriminelle Akteure vermehrt kritische Infrastrukturen, politische Systeme, die nationale Sicherheit und das öffentliche Vertrauen ins Visier nehmen. In diesem Kontext wird der Vortrag das besagte Paradox eingehend erörtern und dabei die vielschichtigen Möglichkeiten und Risiken der generativen KI in der nationalen Sicherheit beleuchten. Generative KI eröffnet enorme Chancen, um auf die sich rasch ändernde Geschwindigkeit, den Umfang und die Art der Bedrohungen für die nationale Sicherheit in einer zunehmend volatilen Umgebung zu reagieren. Dabei steht die zentrale Frage im Raum, wie Sicherheitsbehörden diese Gelegenheit nutzen können, um Bedrohungen verantwortungsbewusst, sicher und koordiniert zu begegnen und gleichzeitig strategische, operative und taktische Elemente zu schützen. Ein Fokus des Vortrags liegt auf der Identifikation entscheidender Aspekte für die erfolgreiche Integration generativer KI in nationale Sicherheitsstrukturen. Hierbei werden bewährte Praktiken und Erfahrungen aus erfolgreichen Implementierungen von KI-Lösungen in anderen Bereichen betrachtet und auf die spezifischen Anforderungen der nationalen Sicherheit adaptiert. Abschließend gibt der Vortrag einen Ausblick auf zukünftige Entwicklungen und Potenziale generativer KI in der nationalen Sicherheit. Dabei werden Empfehlungen für die Weiterentwicklung von Strategien und Policies präsentiert, um Akteure der inneren und äußeren Sicherheit dabei zu unterstützen, die Chancen dieser disruptiven Technologie zu nutzen und gleichzeitig Risiken zu minimieren.

**>
accenture**

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
21	26.6.	14:45	Raum Addis Abeba 3	Michael Kälber	Senior Manager Solutions

Thales Deutschland

Möglichkeiten zur Erhöhung von Effizienz und Usability bei der Absicherung von Daten und Sprache im High Security Bereich

Die Krypto-Modernisierung der Bundeswehr stellt im Kontext Cyber Security einen zentralen Schritt zur Bereitstellung erforderlicher Fähigkeiten für die Zukunft dar. Die Modernisierung bezieht sich hierbei auf die Anwendungssysteme und die Management-Infrastruktur zur Bereitstellung und Verwaltung von Kryptomitteln. Bestehendes wird hierbei oftmals durch Neues ersetzt. In einigen Fällen ist jedoch auch ein Parallelbetrieb bestehender und neuer Verfahren und Standards zu erwarten. In Bezug auf die Modernisierungsmaßnahmen exemplarisch zu nennen sind große Anwendungsgebiete wie z. B. fortschreitende Digitalisierung der Systeme mit dem relevanten Teilbereich Authentisierung zur digitalisierten Autorisierung sicherheitskritischer Prozesse, Nutzung moderner Protokolle und Verfahren im Zuge der Einführung neuer Standards sowie insbesondere Maßnahmen zur Begegnung der Quantencomputer-Bedrohung. Die stetige Weiterentwicklung im Sektor Quantencomputing stellt ein steigendes Risiko für die Sicherheit kryptografischer Verfahren und damit für die sie nutzenden Systeme dar. Einhergehen muss diese technologische Modernisierung mit einer Weiterentwicklung nutzerorientierter, ergonomischer Bedienabläufe über die gesamte Systemlandschaft hinweg. Die Modernisierungsinitiativen stehen im Einklang mit der zunehmenden Betonung der Cybersicherheit seitens der Bundeswehr. Über die Einführung modernisierter Technologien und Systeme hinaus besteht die Notwendigkeit, die Anwenderschaft – von Nutzer, Administratoren bis zu den Kryptoverwaltern – im Zuge von Integration und Training an Einsatz und Handhabung dieser neuen Technologien heranzuführen. Thales Deutschland ist seit Jahrzehnten verlässlicher Partner der Bundeswehr für wehrtechnisches Material insbesondere für Krypto Systeme und Technologien mit Handlungsschwerpunkt im Kontext Krypto-Management. Thales beschäftigt sich intensiv mit der Weiterentwicklung des Krypto Portfolios unter Berücksichtigungen der neuen Herausforderungen im Kontext Kryptographie sowie den mit Weiterentwicklung und Modernisierung verbundenen Konzeptionen und Technologien. Der Vortrag beinhaltet eine Einschätzung zu sinnvollen Handlungslinien für die Bundeswehr sowie zu Realisierungschancen und -herausforderungen.

Industrievorträge

Nr.	Tag	Zeit	Ort
S 1	26.06.2024	16:15 - 17:45 h	SAAL Addis Abeba 1 - 2

Startup Pitch und Panel Session

Marktverfügbare Innovationen für die Zeitenwende

Kurzbeschreibung zum Thema:

Bestätigt durch den Erfolg der vergangenen Jahre wird es auch 2024 einen „Innovationsbereich für Startups“ (R 63) auf der AFCEA-Fachausstellung geben. Initiiert von den AFCEA Emerging Leaders erwarten Sie **11 ausgewählte Startups** als Vertreter und Treiber von Innovation im öffentlichen Bereich, die ihre Lösungen auf der Ausstellungsfläche einem breiten Publikum präsentieren.

In unserer Startup Pitch und Panel Session im Saal Addis Abeba 1 und 2 vertiefen wir den Dialog mit **Key Stakeholdern aus Industrie, Bundeswehr und dem öffentlichen Sektor** und stellen uns die Frage:

„Was ist in der Bundeswehr im Bereich Innovation im letzten Jahr passiert und wie kann Innovation noch zielgerichteter einfließen?“

Die aktuellen Entwicklungen im Bereich Defence Innovation werden reflektiert. Es folgen der BMVg Clusterlogik inhaltlich zugewiesene Startup-Pitches, deren Lösungen durch ein hochrangiges Panel diskutiert werden. Anschließend laden wir alle Teilnehmer herzlich zu einem gemeinsamen **Ausklang mit den Startups** ein.

 **TENZIR**

langlauf
SECURITY AUTOMATION

AIUI 


pwc

 **PREVENCY®**

 **SECURITY FOR THINGS**

RIVADA
SPACE NETWORKS

 **traversals**

eleQtron

 **LocateRisk**
MAPS • COMPARE • OPTIMIZE • SECURE


**cyber
innovation
hub**

 **KENBUN**

 **GOV RADAR**

 **Possible**

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
22	27.6.	11:15	ehem. Plenarsaal Bundestag	Alexander von Gernler	Abteilungsleiter Research and Innovation

genua GmbH

Souveräne Cloud:

Eine geostrategisch-technische Analyse zu Cybersicherheit

IT-Sicherheit mag früher ein Nischenthema gewesen sein. Heute ist sie eine Frage digitaler Souveränität und damit der nationalen Sicherheit. Nicht zuletzt im Ukrainekrieg und an den vorangegangenen Hackerangriffen auf zivile Infrastrukturen wird deutlich, dass eine empfindliche Störung kritischer Informationsinfrastruktur militärisch von hohem Interesse ist. Angriffe zu militärischen Zwecken können unbeabsichtigt und schnell auf zivile Strukturen übergreifen. Gleichzeitig bietet der Operationsraum der Cyberdomäne Möglichkeiten der Manipulation und Beeinträchtigung von Infrastrukturen, die unter der Schwelle zum bewaffneten Konflikt liegen. Somit ist das Risiko einer Eskalation für staatliche Akteure geringer als in anderen Bereichen der Auseinandersetzung. Sie sind damit ein bevorzugtes Mittel der Wahl. In den letzten Jahren beobachten IT-Sicherheitsexperten nun nicht nur die steigende Relevanz von Zero Trust für eine souveräne Informationsverarbeitung, sondern auch den Wunsch, behördliche Informationsverarbeitung mittels Cloudtechnologien zu konsolidieren, wie es die Wirtschaft seit Längerem tut. Wie können wir aber Vertrauen in die Sicherheit kritischer digitaler Infrastrukturen und souveräner Clouds entwickeln? Und wodurch kann dieses Vertrauen letztendlich gerechtfertigt sein? Der Vortrag bietet eine geostrategisch-technische Analyse zur Cybersicherheit in der Cloud-Ära.

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
23	27.6.	11:45	ehem. Plenarsaal Bundestag	Moritz Pichler	Head of Ventures

HENSOLDT

HENSOLDT FCAS Accelerator –

ein Paradigmenwechsel für das Innovationsmanagement in der Verteidi-

Kurz nach der Beauftragung der nationalen Ergänzungsstudien zum Future Combat Air System (FCAS) haben die Teams aus den verschiedenen Divisionen und dem Engineering bei HENSOLDT Sensors GmbH die Arbeit aufgenommen. Die nationalen Forschungs- und Technologievorhaben (F&T) zum Next Generation Weapon System (NGWS) sollen Technologieentwicklungen ermöglichen, die im multinationalen FCAS-Projekt nicht oder nicht ausreichend berücksichtigt sind, aber aus nationaler Sicht für ein NGWS in einem FCAS-Systemverbund notwendig sind. Die deutsche Beschaffungsbehörde BAAINBw hat Ende Oktober mit dem FAM Konsortium die Champions der deutschen militärischen Luftfahrtindustrie für diese nationale Ergänzungsstudie unter Vertrag genommen. Das Konsortium besteht aus Airbus, MBDA und der FCMS GbR mit den Firmen Diehl, ESG, Rohde & Schwarz und HENSOLDT. Die F&T-Studie umfasst acht Vorhaben, von denen zwei - das Vorhaben „Sensor-Datenfusion/Sensorressourcenmanagement“ und das zum „Elektronischen Kampf“ - direkt von HENSOLDT als Einzelvorhabenskoordinator geführt werden. Um das Ökosystem für Innovationen und Dual Use Produkte in Europa anzukurbeln sowie Hidden Champions für eine Zusammenarbeit im FCAs Programm zu identifizieren, hat HENSOLDT den FCAS Accelerator auf die Beine gestellt. Dieses Programm bot europäischen Top-Innovatoren aus der Dual-Use-Industrie am FCAS-Programm teilzunehmen. Nach intensivem Scouting von mehr als 300 Start-ups in den Bereichen disruptive Sensoren, Befähigung von AI, 3D gedruckte Elektronik, elektronische Materialien & Komponenten und innovative RF Technologien, hatten 10 ausgewählte Start-ups 13 Wochen Zeit an ihren Ideen zu feilen, ihr proof-of-concept zu erarbeiten, mit Entscheidungsträgern und Stakeholdern zu netzwerken und an Workshops teilzunehmen. Das Programm trug nicht nur dazu bei, das eigene Portfolio der HENSOLDT mit innovativen Lösungen zu ergänzen und durch neue disruptive Technologien in die Zukunft zu investieren, sondern auch ein dynamisches Ökosystem für Innovation und Zusammenarbeit zwischen Industrie und Start-ups zu fördern. Der FCAS Accelerator stellt einen Paradigmenwechsel für das Innovationsmanagement in der Verteidigung dar.



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
24	27.6.	12:15	ehem. Plenarsaal Bundestag	Dipl.-Ing.(FH) Uwe Gschwind	Digital Enabler, Presales Hyperautomation

Deutsche Telekom Geschäftskunden GmbH

Fokussierung auf Kernaufgaben durch Digitalisierung von Verwaltungsprozessen

Die Unterstützung der Zeitenwende durch disruptive KI-basierten Automatisierungslösungen in Verwaltungs- und Beschaffungsprozessen lässt sich nicht mehr aufhalten. Automatisierung, künstliche Intelligenz (KI) und die Entwicklung mit No-/Low Code Lösungsansätzen werden den Alltag, auch der Bundeswehrverwaltungen, zukünftig prägen. KI-basierte Automatisierungslösungen ermöglichen dabei eine schnellere und effektivere Bereitstellung von resilienten Prozessautomatisierungen. Durch den Einsatz von KI können wiederkehrende Aufgaben automatisiert und somit die Effizienz gesteigert werden. KI-basierte Algorithmen lernen, wie Prozesse ausgeführt werden sollen, und führen diese eigenständig aus. Dies führt zu einer Reduktion von menschlichen Fehlern, steigert die Qualität, Geschwindigkeit und die Effizienz. Das vorhandene Personal kann sich somit den Kernaufgaben der Bundeswehr widmen. Im Fokus steht die Automatisierung von Prozessen und Anwendungen. No-/Low Code ermöglicht mit einfachen Mitteln, teilweise vollständig ohne Programmierung, Mitarbeiter in der Bundeswehrverwaltung die notwendigen Prozesse selbstständig zu automatisieren und kontinuierlich zu optimieren. So kann auch entscheidend dem Fachkräftemangel entgegen gewirkt und die Mitarbeiterbindung gefördert werden. Darüber hinaus müssen Automatisierungslösungen die nationale Datensouveränität stärken, die verantwortungsvolle Datennutzung und den Datenschutz optimal unterstützen. Die Einsatzmöglichkeiten und die Fähigkeiten heutiger Automatisierungsplattformen zeigen wir an konkreten, markterprobten Beispielen und Referenzen. Neben Automatisierungslösungen wie der Verarbeitung von Handschrifterkennung auf Formularen und der weiteren Verarbeitung in nachgelagerten IT-Systemen, werden auch Automatisierungslösungen aus dem Bereich Personalwesen gezeigt. Im Bereich Personalwesen setzt unserer Unternehmen selbst eine Automatisierungslösung zur Abbildung von über 700 HR-Prozessen für ca. 200.000 Mitarbeiter in verschiedensten Organisationseinheiten ein. Mehr erfahren Sie in unserem Vortrag, wir freuen uns auf Ihren Besuch.



Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
25	27.6.	12:45	ehem. Plenarsaal Bundestag	Markus Gerstl	Head of Sales Region D-A-CH für Space Connectivity

Airbus Defence and Space

Weltraumgestützte Kommunikation für militärische Anwender

„Satellitenkommunikation durch Multi-Orbit Anbindung. Anwendungen und Umsetzung“
Dieser Vortrag beleuchtet wegweisende Fortschritte in der Satellitenkommunikation. Dabei werden insbesondere die funktionalen und wirtschaftlichen Vorteile von Low Earth Orbit (LEO) Konstellationen für den Einsatz der Streitkräfte herausgestellt. Anhand verschiedener Anwendungsbeispiele wird dargestellt, welche zusätzlichen operationellen Möglichkeiten sich mit dem Einsatz von LEO Satelliten Konstellationen zu Land, zu Luft und zu See eröffnen. Ein Vergleich mit bestehenden militärischen Satellitenkonstellationen (z.B. SATCOMBw) und das Aufzeigen möglicher Grenzen werden den Vortrag abrunden.“

AIRBUS

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
26	27.6.	13:15	ehem. Plenarsaal Bundestag		

SOPHIST GmbH

KI oder Mensch – Wer ist besser im Systems Engineering?

Seit gut einem Jahr erobern unterschiedliche Künstliche Intelligenzen (KI), speziell Generative pre-trained Transformer (GPT) wie ChatGPT4.0 oder Google Gemini, immer mehr Branchen und Einsatzgebiete mit überzeugenden Ergebnissen. Seien es die Generierung von Websites, Marketingtexten, Stellenausschreibung oder auch kompliziertere Aufgaben wie die Erstellung von Trainingskonzepten zur Vermittlung von Wissen oder lippensynchrone Übersetzung von Videos. Doch was ist mit der Entwicklung von technischen Systemen? Als SOPHIST GmbH experimentieren wir seit geraumer Zeit, mit generativen KIs und deren Einsatzmöglichkeiten in diesem Gebiet. Die Ergebnisse sind zum Teil so beeindruckend, dass wir uns die Frage stellen, ob uns KI in absehbarer Zeit als Systems Engineers ersetzen wird. In diesem Vortrag lernen Sie anhand unterschiedlicher Einsatzszenarien und Erfahrungsberichte, wie Ihre Systementwicklung von KI profitieren kann und wo derzeit die Grenzen liegen.



Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
27	27.6.	11:15	Raum Addis Abeba 3		Head of Training Applications Section

Telespazio Germany

Informationssicherheitskonzepte: Grundlagen und Notwendigkeit

„Satellitenkommunikation durch Multi-Orbit Anbindung. Anwendungen und Umsetzung“
Dieser Vortrag beleuchtet wegweisende Fortschritte in der Satellitenkommunikation. Dabei werden insbesondere die funktionalen und wirtschaftlichen Vorteile von Low Earth Orbit (LEO) Konstellationen für den Einsatz der Streitkräfte herausgestellt. Anhand verschiedener Anwendungsbeispiele wird dargestellt, welche zusätzlichen operationellen Möglichkeiten sich mit dem Einsatz von LEO Satelliten Konstellationen zu Land, zu Luft und zu See eröffnen. Ein Vergleich mit bestehenden militärischen Satellitenkonstellationen (z.B. SATCOMBw) und das Aufzeigen möglicher Grenzen werden den Vortrag abrunden.“

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
28	27.6.	11:45	Raum Addis Abeba 3	Andreas Stiebner	Account Executive

Carmenta Germany GmbH

KI oder Mensch – Wer ist besser im Systems Engineering?

Seit gut einem Jahr erobern unterschiedliche Künstliche Intelligenzen (KI), speziell Generative pre-trained Transformer (GPT) wie ChatGPT4.0 oder Google Gemini, immer mehr Branchen und Einsatzgebiete mit überzeugenden Ergebnissen. Seien es die Generierung von Websites, Marketingtexten, Stellenausschreibung oder auch kompliziertere Aufgaben wie die Erstellung von Trainingskonzepten zur Vermittlung von Wissen oder lippensynchrone Übersetzung von Videos. Doch was ist mit der Entwicklung von technischen Systemen? Als SOPHIST GmbH experimentieren wir seit geraumer Zeit, mit generativen KIs und deren Einsatzmöglichkeiten in diesem Gebiet. Die Ergebnisse sind zum Teil so beeindruckend, dass wir uns die Frage stellen, ob uns KI in absehbarer Zeit als Systems Engineers ersetzen wird. In diesem Vortrag lernen Sie anhand unterschiedlicher Einsatzszenarien und Erfahrungsberichte, wie Ihre Systementwicklung von KI profitieren kann und wo derzeit die Grenzen liegen.



carmenta

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
29	27.6.	12:15	Raum Addis Abeba 3	Ulrich Kohn	

Adva Network Security

Geschützte Glasfasernetze als Fundament einer hochsicheren Kommunikations-Infrastruktur: überwacht, resilient, quantensicher

Optische Netze bilden die Grundlage von Kommunikationsnetzen in vielen kritischen Einrichtungen. Die hohe strategische Bedeutung von Glasfasernetzen impliziert eine hohe Schutzwürdigkeit. Dies gilt besonders wegen einer zunehmenden Bedrohungslage durch geopolitische Verwerfungen oder Naturkatastrophen. In diesem Vortrag wird systematisch die Risikosituation analysiert und die technischen Möglichkeiten des Schutzes zur Sicherstellung eines robusten und zuverlässigen Betriebs erläutert. Fasermonitoring zur Störungsanalyse in Echtzeit Betreiber von Glasfaserinfrastrukturen müssen in der Lage sein, feindliche Aktionen an jedem Punkt ihres großflächigen Netzes schnell zu detektieren, zu identifizieren und zu lokalisieren. Faser-Monitoring liefert mittels OTDR-Technik in Echtzeit Informationen, um Unterbrechungen zu lokalisieren aber auch andere Störungen zu erkennen. Ersatzschaltung und Wiederherstellung Faserunterbrechungen sind eine häufige Ursache schwerwiegender Ausfälle eines Kommunikationsnetzes. Für die schnelle Wiederherstellung der Verbindungen müssen bei Planung und Installation des Netzes zusätzlich Ressourcen zur Ersatzschaltung vorgehalten werden. Die Wiederherstellung der gestörten Strecken auf dem optischen Layer schützt eine hohe Anzahl von Verbindungen auf höheren Layern und stellt einen wesentlichen Beitrag zur Resilienz eines Netzes dar. Schutz durch quantensichere Verschlüsselung Sensible Daten, die mit Glasfasern über große Entfernungen übertragen werden, bieten viele Ansatzpunkte für Lauschangriffe oder Störungen. Dies stellt ein erhebliches Risiko für die Sicherheit der Kommunikation dar. Eine robuste Verschlüsselung in Kombination mit einer starken Authentifizierung sind eine bewährte Methode, um Daten auf der Übertragungsstrecke vor Diebstahl, Missbrauch und Manipulation zu schützen. Für eine langfristige, kompromisslose Sicherheit ist der Einsatz eines quantensicheren Schlüsselaustauschs mit PQC oder QKD unerlässlich.



Nr.	Tag	Zeit	Ort	Vortragender	Funktion
30	27.06.	12:45	Raum Addis Abeba 3	Michael Frings	Federal & Defense Lead

NVIDIA GmbH

Sensorfusion, Metadatenextraktion und Datenreduktion in isolierten Edge-Systemen mit Nvidia Jetson

Isolierte Edge-Computing-Systeme, die autonom Sensordaten verarbeiten, Metadaten extrahieren und Daten reduzieren, erfordern spezielle Hardwarelösungen, die sowohl leistungsstark als auch energieeffizient sind. Die Nvidia Jetson Produktfamilie ist eine solche Lösung, die sich für diese Aufgaben besonders gut eignet. Die Leistungsfähigkeit des Jetson Moduls ist entscheidend, da diese Systeme oft eine große Menge an Sensordaten in Echtzeit verarbeiten müssen. Mit einem leistungsstarken ARM-Prozessor und einer dedizierten GPU bietet der Jetson Orin die erforderliche Rechenleistung für komplexe Datenverarbeitungsaufgaben. Energieeffizienz ist in isolierten Umgebungen von großer Bedeutung, in denen Ressourcen begrenzt sein können. Jetson Orin wurde entwickelt, um einen geringen Energieverbrauch zu gewährleisten und damit die Betriebskosten zu minimieren. Für die Metadatenextraktion und Datenreduktion spielt die Unterstützung für KI-Beschleunigung eine entscheidende Rolle. Jetson Orin verfügt über eingebaute KI-Kerne, die die Ausführung von KI-Algorithmen beschleunigen und somit die Effizienz dieser Prozesse steigern. Die Robustheit des Jetson Orin ermöglicht den Einsatz in rauen Umgebungen, in denen die Systeme widrigen Bedingungen ausgesetzt sein können. Die Konstruktion ist darauf ausgelegt, diesen Herausforderungen standzuhalten und gleichzeitig zuverlässig zu funktionieren. Die Integration von Sensor-Schnittstellen erleichtert die nahtlose Erfassung von Sensordaten und Weiterverarbeitung. Dies ist entscheidend für den Erfolg von Edge-Systemen in isolierten Umgebungen, da sie oft eine Vielzahl von Sensoren verwenden. Die Flexibilität und Anpassbarkeit der Jetson-Plattform ermöglicht Entwicklern die Erstellung maßgeschneiderter Softwarelösungen, die den spezifischen Anforderungen dieser Systeme gerecht werden. Dies ist von entscheidender Bedeutung, da isolierte Edge-Systeme oft herausfordernde Anforderungen haben.



nVIDIA®

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
31	27.06.	13:15	Raum Addis Abeba 3	Dipl.-Ing (FH) Scharel Clemens	Leiter Entwicklung

best Systeme GmbH

COTS-Ketten sprengen - Moderne IT für Militärische Anwendungen

Oder -> wie kann Ihr Unternehmen durch den Einsatz von MOTS profitieren?

Ein Beispiel einer High-Performance-Switch-Modifikation (>100GBs) für die Luftfahrt

COTS-Komponenten sind bekanntermaßen beliebt und kostengünstig. Sie sind bereits für ihren vorgesehenen Einsatzzweck entwickelt und ersparen Ihnen die teure Eigenentwicklung sowie aufwendige Qualifizierung. Durch den Einsatz von COTS-Komponenten können Sie auf die Fachkenntnisse spezialisierter Hersteller zurückgreifen und sich zugleich die langfristige Lieferbarkeit der Produkte sichern. Diese vorgefertigten Lösungen ermöglichen erhebliche Einsparungen bei der Realisierung von Gesamtprojekten. Jedoch stoßen Sie als Systemarchitekten ambitionierter Projekte zunehmend auf Herausforderungen: Die stetig wachsenden Datenmengen sensorgestützter Systeme erfordern deutlich höhere Übertragungsraten als von herkömmlichen COTS-Komponenten bereitgestellt werden können. Zudem machen die Komplexität der Anforderungen und die rasante technologische Entwicklung eine maßgeschneiderte Entwicklung von Grund auf beinahe unmöglich. Die best Systeme GmbH packt es an und bringt modernste IT-Systeme in die Luft:

- Durch unsere 30-jährige Erfahrung auf dem Markt haben wir die zuverlässigsten Hersteller von COTS-Komponenten identifiziert, darunter NVIDIA Networking (ehemals Mellanox).
- Unsere Partner liefern Ihnen die schnellsten und zuverlässigsten Netzwerkkomponenten auf dem Markt.

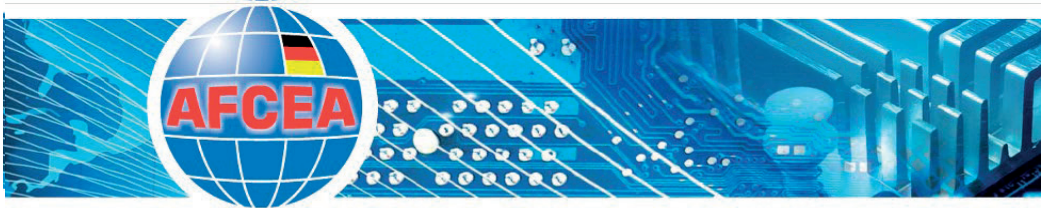
Dabei sind die Systeme offen gestaltet, um Anpassungen sowohl auf Hardware- als auch auf Softwareebene zu ermöglichen. Unsere Lösungen, insbesondere die Ethernet-Switches der Spectrum-Reihe, bieten Ihnen somit die ideale Basis für die Datenübertragung auch unter anspruchsvollen Bedingungen. - Entdecken Sie, wie eine kluge Auswahl von COTS-Komponenten und Fachwissen Ihnen einen Technologievorsprung verschaffen kann.

- Erfahren Sie, wie der Übergang von COTS zu MOTS Ihre Projekte effizienter und zukunftssicherer macht.





Bonn e.V.



AFCEA Bonn e.V.

Studien PREIS 2024

Das Bonner Chapter des internationalen Anwenderforums für Fernmelde-technik, Computer, Elektronik und Automatisierung (AFCEA) verleiht jährlich einen **Studienpreis**, der mit insgesamt **20.000 €** dotiert ist.

Der Verein fördert damit junge Wissenschaftlerinnen und Wissenschaftler, die hervorragende **Masterarbeiten** auf den Gebieten der **Angewandten Informatik** und der **Nachrichtentechnik** erstellt haben. Auch **Bachelorarbeiten** sind zugelassen, jedoch werden an alle Arbeiten dieselben Maßstäbe angelegt.

Professorinnen und Professoren der Universitäten und Fachhochschulen aus der Wissenschaftsregion **Aachen-Bonn-Koblenz**, dem Wirkungskreis des Stifters, sowie der **Universitäten der Bundeswehr** in Hamburg und München, die dem thematischen Fokus Verteidigung und Sicherheit entsprechen, schlagen ihre besten Absolventinnen und Absolventen für den Studienpreis vor.

Die Entscheidung über die auszuzeichnenden Arbeiten obliegt einer unabhängigen Jury.

Die Frist für die Abgabe der Vorschläge endet am **30. April 2024**.

Die Preisverleihung findet am **24. Oktober 2024** im Rahmen der Koblenzer IT-Tagung statt.

Details sowie die Bewerbungsunterlagen finden Sie unter

<https://www.afcea.de/studienpreis>

Brigadegeneral Armin Fleischmann
Vorsitzender AFCEA Bonn e.V.

Dr. Hans-Peter Quadt
Vorsitzender der Jury



AFCEA Bonn e.V.

*Anwenderforum für Fernmeldetechnik,
Computer, Elektronik und Automatisierung*

AFCEA Jahresprogramm 2024



Mehr Wissen teilen

*AFCEA Bonn e. V. hat sich der Zielsetzung verschrieben
ein Spezialforum moderner Informations- und
Kommunikationstechnologie für Öffentliche Verwaltung,
Sicherheit und Verteidigung zu bieten.*

*AFCEA Bonn e.V. besteht seit 1983 und umfasst über
1.000 persönliche und mehr als 100 Firmenmitglieder.*

*Zu den Firmenmitgliedern gehören neben den Großen der
IT- und Kommunikationsbranche eine Vielzahl
mittelständischer und kleinerer Unternehmen
vornehmlich aus der Region Bonn-Köln-Koblenz.*

*Nähre Informationen unter: www.afcea.de
buero@afcea.de · twitter.com/AFCEA Bonn · www.facebook.com/AFCEABonneV*

AFCEA Bonn e.V. · Borsigallee 2 · 53125 Bonn



Bonn e.V.

Aussteller

Unsere Aussteller bei der AFCEA



Logo - Collage

EA Fachausstellung 2024





Bonn e.V.

Industrievorträge 2024



AFCEA Fachausstellung 2025

27./28. Mai 2025