AFCEA Bonn e.V.

36. AFCEA Fachausstellung

Informations- und Kommunikationstechnik

10./11. Mai 2023

World Conference Center Bonn

(Künstliche) Intelligenz & Innovationen - Konkrete Nutzungsmöglichkeiten

Industrievorträge FA 2023

Aussteller mit

Inhaltsverzeichnis:

Auf vielfachen Wunsch der Aussteller haben wir bei der AFCEA Fachausstellung 2023 - wie erstmalig auf der AFCEA FA 2022 - zwei Speakercorner für **Industrievorträge** eingerichtet, im SAAL NAIROBI und im SAAL ADDIS ABEBA 3.

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, dahinter die Abstracts.

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 diese Broschüre als pdf-Datei zum download.

Aussteller	Vortrag Nr.	Tag	Zeit	Raum	Stand
Airbus Defence & Space	22	10.05.	16:00	ADDIS A.	F 03
Airbus Defence & Space	25	10.05.	17:30	ADDIS A.	F 03
Bechtle AG	1	10.05.	09:15	NAIROBI	S 18
CAE GmbH	24	10.05.	17:00	ADDIS A.	W 05
CGI	32	11.05.	09:15	ADDIS A.	F 04
Cisco Systems GmbH	23	10.05.	16:30	ADDIS A.	F 08
CONET	6	10.05.	13:15	NAIROBI	S 45

Industrievorträgen

Aussteller	Vortrag Nr.	Tag	Zeit	Raum	Stand
CONET	28	11.05.	11:45	NAIROBI	S 45
dainox GmbH	5	10.05.	12:45	NAIROBI	S 33
Dassault Systemes Deutschland GmbH	15	10.05.	12:30	ADDIS A.	R 11
Dell Technologies	38	11.05.	13:15	ADDIS A.	R 51
ESG Elektroniksystem- und Logistik-GmbH	11	10.05.	14:00	ADDIS A.	F 01
Fujitsu Technology Solutions GmbH	9	10.05.	14:45	NAIROBI	F 13
genua GmbH	19	10.05.	14:30	ADDIS A.	S 25
Hacking-Lab AG	37	11.05.	12:45	ADDIS A.	R 02
HENSOLDT	14	10.05.	12:00	ADDIS A.	W 10
IABG	20	10.05.	15:00	ADDIS A.	W 09
IBM	36	11.05.	12:15	ADDIS A.	F 02
Kommando Luftwaffe	2	10.05.	11:15	NAIROBI	S 65
macmon secure GmbH	3	10.05.	11:45	NAIROBI	R 34
Narda Safety Test GmbH	16	10.05.	13:00	ADDIS A.	S 62
Novachips	21	10.05.	15:30	ADDIS A.	R 03
OPITZ CONSULTING Deutschland GmbH	31	11.05.	13:15	NAIROBI	F 17
Palo Alto Networks (Germany) GmbH	26	11.05.	09:15	NAIROBI	B 09
Pexip	29	11.05.	12:15	NAIROBI	R 04
PLATH Group	38	11.05.	15:00	ADDIS A.	F 19
PLATH Group	39	11.05.	15:30	ADDIS A.	F 19
RHEINMETALL	10	10.05.	09:15	ADDIS A.	W 01
Rittal GmbH & Co. KG	12	10.05.	11:00	ADDIS A.	S 15
Rohde & Schwarz	35	11.05.	11:45	ADDIS A.	F 10
rola Security Solutions GmbH	27	11.05.	11:15	NAIROBI	F 06
RUAG AG	11	10.05.	09:45	ADDIS A.	S 70
Secusmart	7	10.05.	13:45	NAIROBI	S 51
Software AG	34	11.05.	11:15	ADDIS A.	S 20
Somtxt UG (haftungsbeschränkt)	17	10.05.	13:30	ADDIS A.	R 12
ThermoAnalytics GmbH	30	11.05.	12:45	NAIROBI	R 43
Trend Micro Deutschland GmbH	4	10.05.	12:15	NAIROBI	S 36
Trend Micro Deutschland GmbH	8	10.05.	14:15	NAIROBI	S 36
VECTED GmbH	13	10.05.	11:30	ADDIS A.	R 43

Zeitplan

AFCEA Fachausstellung 2023

10.05.2023

	Vortragssaal NAIROBI	Vortragssaal ADDIS ABEBA 3
09:00		
09:15	1 Bechtle AG	10 RHEINMETALL
09:30		
09:45		11 RUAG
10:00	Eröffnung Symposiums-vortrag 1	
10:15		
10:30		
10:45		
11:00 - 11:25		12 Rittal GmbH & Co. KG
11:15 - 11:40	2 Kdo Luftwaffe	
11:30 - 11:55		13 VECTED GmbH
11:45 - 12:10	3 macmon Secure GmbH	
12:00 - 12:25		14 HENSOLDT
12:15 - 12:40	4 Trend Micro Deutschland	
12:30 - 12:55		15 Dassault Systems Germany GmbH
12:45 - 13:10	5 dainox GmbH	
13:00 - 13:25		16 Narda Safety Test Solutions GmbH
13:15 - 13:40	6 CONET	
13:30 - 13:55		17 Somtxt UG
13:45 - 14:10	7 Secusmart	
14:00 - 14:25		18 ESG Elektronik-system- u. Logistik-
14:15 - 14:40	8 Trend Micro Deutschland	
14:30 - 14:55		19 genua GmbH
14:45 - 15:10	9 FuJitsu Services GmbH	
15:00 - 15:25		20 IABG
15:15 - 15:40		
15:30 - 15:55	Die Emerging Leaders AFCEA Bonn (ELA) präsentieren **Startups** in Pitch Sessions	21 Novachips
15:45 - 16:10		
16:00 - 16:25		22 Airbus Defence and Space
16:15 - 16:40		
16:30 - 16:55		23 Cisco Systems
16:45 - 17:10		
17:00 - 17:25		24 CAE GmbH
17:15 - 17:40		
17:30 - 17:55		25 Airbus Defence and Space
17:45 - 17:10		

Industrievorträge

AFCEA Fachausstellung 2023

11.05.2023		Vortragssaal NAIROBI		Vortragssaal ADDIS ABEBA 3
09:00				
09:15	26	Palo Alto Networks (Germany) GmbH	32	CGI
09:30				
09:45				
10:00		Symposium 2 #Digital Defence		
10:15				
10:30				
10:45				
11:00				
11:15 - 11:40	27	rola Security Solutions	33	Software AG
11:45 - 12:10	28	CONET	34	Rohde & Schwarz
12:15 - 12:40	29	Pexip AS	35	IBM
12:45 - 13:10	30	ThermoAnalytics GmbH	36	Hacking-Lab AG
13:15 - 13:40	31	OPITZ CONSULTING	37	Dell Technologies
14:00		Symposiums-vortrag 3		
14:15				
14:30				
14:45				
15:00			38	PLATH Group
15:15				
15:30			39	PLATH Group
15:45				
16:00				
16:15				
16:30				
16:45				

NAIROBI

Speakercorner 1

Nr.	Beginn	Firma/Organisation	Vortragende/r
1	09:15	**Bechtle AG**	Steven Handgrätinger
2	11:15	**Kommando Luftwaffe**	Major Kai Pieters
3	11:45	**macmon secure GmbH**	Andreas Wendt
4	12:15	**Trend Micro Deutschland GmbH**	Björn Glückstadt
5	12:45	**dainox GmbH**	Jochen Brückner Gregor Jehle
6	13:15	**CONET**	Dr. Christian Jürgens
7	13:45	**Secusmart**	Dr. Christoph Erdmann
8	14:15	**Trend Micro Deutschland GmbH**	Robert Wortmann
9	14:45	**Fujitsu Services GmbH**	Tassilo Markert-Mesters

S 1	15:30 17:30	**Aleph Alpha GmbH** **Inhubber GmbH** **KENBUN IT AG** **Motion Miners** **PREVENCY GmbH** **SCALUE GmbH**	

Industrievorträge

Raum NAIROBI

Funktion	Thema
Bereichsvorstand Public Sector der Bechtle AG	Closing the implementation gap: Bechtles Weg zur Nutzung Künstlicher Intelligenz
Leiter NavUstg des Zentrums Simulations- und Navigations-unterstützung Fliegende Waffensys-teme der Bundeswehr	Agile Simulation Support
Key Account Manager	Zero Trust Network Access (ZTNA) – Wie macmon durch autorisierte Zugangskontrolle die Endgerät- und Port-Security in Netzen sichert
Sales Engineer KRITIS	Privat 5G: Revolution des Campus Netzwerks - Ist 5G wirklich „Secure by Design“?
Principal Network Solutions Consultant dainox GmbH Geschäftsführer P3KI GmbH	Menschliches Vertrauen für die digitale Welt - Robuste, dezentrale und offlinefähige Rechtedelegation im Feld
Lead Expert „Sustainability & Green IT“	Green IT – Die Brücke zwischen Nachhaltigkeit und Re-silienz?
Geschäftsführer Secusmart GmbH und SVP BlackBerry Secusmart	Der VS-NfD sichere mobile Arbeitsplatz innerhalb der Bundeswehr und Bundesbehörden
Practice Lead Cyber Defence	Datenzentrische Betrachtung von SOC/CERT Strukturen
Head of Defence Germany	KI für die Streitkräfte - eine Frage der (Trainings)daten und wie sie gewonnen werden

	Pitch Sessions von ausgewählten Startups

ADDIS ABEBA 3

Speakercorner 2

Nr.	Beginn	Firma/Organisation	Vortragende/r
10	09:15	**RHEINMETALL**	Matthias Köhler Sales Manager Mission Systems
11	09:45	**RUAG AG**	Marco Schläppi, B.A.Sc
12	11:00	**Rittal GmbH & Co. KG**	Hartmut Lohrey
13	11:30	**Vected GmbH**	Dr. Andreas de Jonge
14	12:00	**HENSOLDT**	Jan Erbe
15	12:30	**Dassault Systemes Deutsch-land GmbH**	Enrico Scharlock
16	13:00	**Narda Safety Test Solutions GmbH**	Dipl.-Ing. Volker Brands
17	13:30	**Somtxt UG (haftungsbeschränkt)**	Dipl. Päd. Stefan Pforte
18	14:00	**ESG Elektroniksystem- und Logistik-GmbH**	Andreas Schiel
19	14:30	**genua GmbH**	Steffen Ullrich
20	15:00	**IABG**	Patrick Rund Dr. Lukas Höhndorf
21	15:30	**Novachips**	Sejong Yoo
22	16:00	**Airbus Defence & Space**	Andreas Reinecke Robert Sekora
23	16:30	**Cisco Systems GmbH**	Detlef Wallenhorst
24	17:00	**CAE GmbH**	Michael Sauer
25	17:30	**Airbus Defence & Space**	Daniel Kallfass Stefan Nagel

Industrievorträge

Raum ADDIS ABEBA 3	
Funktion	**Thema**
Business Unit Integrated Electronic Systems	Der KI-unterstützte Feuerkampf
ICT Senior System Architect	Sichere Vernetzung im taktischen Netzwerk durch verschlüsselte Übertragung
EMV-Fachreferent	Schutz sicherheitsrelevanter Daten vor elektromagnetischen Beeinflussungen
Head of Artificial Intelligence	Künstliche Intelligenz im Wärmebild
HENSOLDT Optronics Head of Land Solutions	Partnerschaftlicher Ansatz der deutschen Industrie für Sensorfusion
Aerospace & Defense Industry Solution Experience Senior Director	Modellbasiertes Systems of Systems Engineering (MBSE/SoSE) für NGWS
Regional Sales Manager	Funkaufklärung – neu gedacht! Schnelles und genaues Lagebild für Überlegenheit in taktischen Missionen und Bereitstellen wertvoller Informationen für die Kommandoebene
Geschäftsführer, Algorithmen Design KNN	Mit künstlichen neuronalen Netzen orchestrierte Meinungsmanipulation zielgenau aufklären
Director Geschäftsfeld Kampf	Führungsfähigkeit Division 2025 – Energieversorgung
Technology Fellow	Souverän, Resilient, Agil: Warum moderne Verteidigung digitale Nachhaltigkeit braucht
Senior Manager InfoKom Program Manager AI Conformity	Sicherheitsdomäne as a Service & safeAI
General Manager	Novachips CC/CSfC - certified military-grade SSDs
Head of Secure Communications Business Growth Advanced Studies Manager	Breitbandige BLOS Konnektivität für die vernetzte Operationsführung
Geschäftsfeldentwicklung	Digital Mission Agility durch Künstliche Intelligenz, IoT und Edge-Computing
Senior Product Manager Sustainment EMEA - Defence and Security	Einsatzbereitschaft - Gedanken zur Transformation von militärischer Ausbildung und Einsatzvorbereitung
Expert for Operational Analysis & Deputy Head of TEMOA Sen. Expert Mission Ground Syst..	Anwendungsfälle für KI in der Multi-Domain Combat Cloud

NAIROBI

Speakercorner 1

Nr.	Beginn	Firma/Organisation	Vortragende/r
26	09:15	**Palo Alto Networks (Germany) GmbH**	Horst Kuchelmeister
27	11:15	**rola Security Solutions GmbH**	Robert Schwerdtner
28	11:45	**CONET**	Marcel Tritschler Markus Otterbein
29	12:15	**Pexip**	Dr. Dirk Fischer
30	12:45	**ThermoAnalytics GmbH**	Kethireddy Kameswara Reddy
31	13:15	**OPITZ CONSULTING Deutschland GmbH**	Dr. Roozbeh Faroughi

ADDIS ABEBA 3

Speakercorner 2

Nr.	Beginn	Firma/Organisation	Vortragende/r
32	09:15	**CGI**	Oberst i.G. Klaus Glaab Oberstleutnant Lars Kostka Michael Morton
33	11:15	**SAG Deutschland GmbH**	Dr. Irene Cramer Christoph Reich
34	11:45	**Rohde & Schwarz Vertriebs GmbH**	Dr. Patrick Grames
35	12:15	**IBM**	Carsten Dieterle
36	12:45	**Hacking-Lab AG**	Ivan Bütler
37	13:15	**Dell Technologies**	Laszlo Poór
38	15:00	**PLATH Group**	Dr. rer. nat. Helen Ditz Sven Lüttich (PLATH Group)
39	15:30	**PLATH Group**	Alexander Golding (Airborne Solutions)

Industrievorträge

Raum NAIROBI

Funktion	Thema
Major Account Manager	Kritische Infrastrukturen mit NIST Cybersicherheits Framework (CFS) schützen
Leiter Solution Design	Künstliche Intelligenz: der Gamechanger in der OSINT/OSINF-Lagebewertung?
Junior Consultant Consultant IT-Strategie-management	Prozessdigitalisierung – Wie können Sie sich dem Thema nähern?
Director Public Sector Business DACH, Pexip	Militärische Kommunikation: Umsetzung von Zero Trust in Audio- und Videokonferenzen durch KI
EU Business Develop-ment Manager	Automated synthetic infrared image generation for AI applications
Manager Agile & Innova-tion OPITZ CONSULTING	Schachmatt in 3 Zügen – mit Flexibilität, Schnelligkeit und Innovation zum Gewinner werden: Drei Beispiele aus dem öffentlichen Sektor

Raum ADDIS ABEBA 3

Funktion	Thema
Referatsleiter BMVg und Hauptprozessver-antwortlicher (HPV) Digitale Verwaltungs-arbeit Referent des HPV Engagement Manager DokMBw bei CGI	In „agiler Symbiose“ zum Digitalen Schreibtisch im GB BMVg
Business Development - Integration & APIs Director Defence & Aviation	API-Portale sind Innovationstreiber – nicht nur im Silicon Valley
Vertrieb Taktische Kommunikation	ESSOR - von der Idee der europäischen Interope-rabilität in der Umsetzung
Principle Account Technical Leader - Defense	IT Automation bis in den Einsatz
Gründer und Geschäftsführer	Cyber Range - Attack & Defense Training
Advisory Systems Engineer	"Hilfe, wir wurden gehackt!“ Vor- und Nachsorge mit Dell Technologies
Data Scientist Business Case Manager – Innovations	Künstliche Intelligenz im Bereich der Intelligence Domain
Senior Sales Manager	Drohnen - mehr als fliegende Kameras

Industrievorträge 2023

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
1	10.5.	09:15 - 09:40	Saal NAI-ROBI	Steven Handgrätinger	Bereichsvorstand Public Sector der Bechtle AG

Closing the implementation gap: Bechtles Weg zur Nutzung Künstlicher Intelligenz

KI-Projekte erfolgreich über den Prototypenstatus hinaus zu führen, diese faszinierende Technologie sinnvoll einzusetzen und so nützliche wie nachhaltige Ergebnisse zu erzielen – das ist, was unsere Kunden und Partner mit Bechtle erreichen. Ob Bildanalyse, eine No-Code KI-Entwicklungsplattform oder intelligente Verwaltungsdigitalisierung: Es ist entscheidend, die Entwicklung auf dem IT-Markt zu verstehen und Cutting Edge Technologien voranzutreiben – immer mit dem Ziel einer erfolgreichen Umsetzung. Wir bieten das Fundament dafür: Innovationswille, Kompetenz und ein leistungsfähiges Netzwerk.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
2	10.05.	11:15 - 11:40	Saal NAIROBI	Major Kai Pieters	Leiter NavUstg des Zentrums Simulations- und Navigations-unterstützung Fliegende Waffen-systeme der Bundeswehr

Agile Simulation Support

Der weltweite militärische Flugbetrieb wie auch bodengebundene Kräfte sehen sich im Spektrum möglicher Szenarien heute mit vielen Problemstellung hinsichtlich Komplexität, Bedrohungslage, wenig bekanntem Einsatzraum, Effizienz der Mittel und der kontinuierlichen Verbesserung konfrontiert. Um Soldaten möglichst zielgerichtet gesamtheitlich qualifizieren zu können, finden auch weitere Bereiche den Einstieg in die simulationsgestützte Ausbildung und Einsatzvorbereitung. Mit den voranschreitenden technischen Möglichkeiten und dem militärisch und zivil verfügbaren Produktportfolio wachsen auch die Anforderung an Qualität und Quantität der Simulationsdatenbasen, welche Grundlage für eine möglichst realistische und effiziente Vorbereitung für Übungen und Einsätze sind.

Um insbesondere auch der Anforderung an eine zeitkritische Verfügbarkeit einer neuen Simulationsdatenbasis für ein unvorhergesehenes Krisenszenario Rechnung zu tragen, ist neben verfügbarem Personal für die Umsetzung zukünftig der Schwerpunkt auf prompte technische Realisierungsmöglichkeit zur Beschleunigung zu setzen.

An der Dienststelle Zentrum für Simulations- und Navigationsunterstützung Fliegende Waffensysteme der Bundeswehr wurden hier bereits große Schritte bei den Themenfeldern Virtualisierung der Arbeitsbereiche und Harmonisierung der Datenformate in Richtung Zukunft unternommen. Die Herausforderungen bei der Erstellung neuer Simulationsdatenbasen insbesondere für militärische Flugsimulatoren erfordern bis heute allerdings deutliche Anstrengungen, die von der Quelldatenbeschaffung, Extraktion der nötigen Informationen bis hin zur Modellierung und Bereitstellung der angeforderten Inhalte manuelle Design- und Programmierarbeiten notwendig machen.

Um die zeitkritischen Anforderungen und die technischen Möglichkeiten in Synergie zu bringen, müssen folgende Lösungsmöglichkeiten verfolgt werden: die Nutzung von Angeboten aus Industrie und Open Source, die Einbindung künstlicher Intelligenz bei der Erststellung von Datenbasen und die Ausweitung der Zusammenarbeit mit internationalen Partnern. Damit lässt sich ein wiederverwendbarer, umfangreicher und flexibel einsetzbarer Agile Simulation Support erreichen.

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
3	10.05.	11:45 - 12:10	Saal NAIROBI	Andreas Wendt	Key Account Manager

Zero Trust Network Access (ZTNA) – Wie macmon durch autorisierte Zugangskontrolle die Endgerät- und Port-Security in Netzen sichert.

Die Bundesregierung hat sich das Ziel gesetzt, mehr Sicherheit und einen Rechtsrahmen mit robusten Resilienzmaßnahmen gegen digitale und physische Aspekte gemäß der Strategie für eine Sicherheitsunion zu schaffen. Im Zuge dessen treten zwei wertvolle Richtlinien in Kraft, die die Widerstandsfähigkeit der EU in Bezug auf die kritischen Infrastrukturen (CER) stärken werden. Die CER-Richtlinie ist als ergänzende Gesetzgebung zur ebenfalls überarbeiteten Netz- und Informationssicherheitsrichtlinie (NIS2) konzipiert, die die Anforderungen an die Cybersicherheit kritischer Infrastrukturen neu fasst. Wir wünschen uns die bestmögliche Sicherheit unserer Netzwerke vor externen Angriffen – umso besser, wenn sie einfach und unkompliziert sind. Mit dem IT-SIG 2.0 gehören nun Systeme zur automatisierten Angriffserkennung explizit zu den technisch und organisatorisch notwendigen Sicherheitsvorkehrungen. Der kontrollierte Netzwerkzugang ist die erste Verteidigungslinie vor unberechtigten Zugriffen auf sensible Daten. Jedoch verfügen die Wenigsten über eine vollständige Übersicht und das notwendige Know-how, um zu erkennen, wer und mit welchem Gerät sich unrechtmäßig Zugriff erlangt hat. Erfahren Sie, wie macmon NAC Ihnen dabei hilft, die Anforderungen zu erfüllen und Ihr Netzwerk auf intelligente Weise schützt. Wir stellen Ihnen die Lösung vor, die Ihnen eine permanente Überwachung ihrer gesamten IT-Infrastruktur ermöglicht. Mit macmon NAC wissen Sie jederzeit, welche Geräte sich in Ihrem Netzwerk befinden und wo diese sind. UFOs (unbekannte fremde Objekte) gehören damit der Vergangenheit an, da sämtliche eingesetzten Geräte jederzeit identifiziert, effizient überwacht und vor unbefugten Zugriffen geschützt werden. Mit der Anforderung Cyber Security Maßnahmen umzusetzen, entsteht die Notwendigkeit ganzheitliche und professionelle Systeme zur Gefahrenabwehr einzusetzen. Erfahren Sie wie macmon NAC durch die Integration von Drittanbieterlösungen bei der Umsetzung der organisatorischen Maßnahmen (ISMS, BCMS) und der musterbasierten Angriffserkennung (IDS/IPS, SIEM, SOC, SOAR) unterstützt.

macmon
intelligent einfach

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
4	10.05.	12:15 -12:40	Saal NAIROBI	Björn Glückstadt	Sales Engineer KRITIS

Privat 5G: Revolution des Campus Netzwerks - Ist 5G wirklich „Secure by Design“?

Im Zusammenhang mit Privat 5G wird häufig nicht an Superlativen gespart. Diese Euphorie ist nicht ganz unbegründet. 5G ist ein enormer Sprung nach vorne und wird die Art wie wir in Zukunft Netzwerke bauen und betreiben verändern. Bei aller Euphorie und Tatendrang ob der sich eröffnenden Möglichkeiten darf nicht vergessen werden, dass es sich bei „privat 5G“ um ein Datennetz handelt, das sich genau wie herkömmliche Technologien mit Angriffen von außen und innen beschäftigen muss. Angriffsvektoren wie „Sozial Engineering“ „DoS & DDoS“ „Malware“ oder „Man in the Middle“ sind auch in privaten 5G Netzen möglich. Obwohl 5G sicherer ist als andere drahtlose Kommunikation gibt es doch die selben Herausforderungen. Trend Micro hat dies sehr früh erkannt und sich mit der Lösung dieser Aufgaben befasst. Die Lösung heißt „TMMNS“ Trend Micro Mobile Network Security. TMMNS besteht derzeit aus 2 Hauptkomponenten. TMMNS Endpoint Protection Mit der Endpoint Protection bietet Trend Micro eine eigene SIM Karte und ein SIM Management System. Die SIM Karte kann sowohl als Physikalische SIM in verschiedenen Formfaktoren ausgelegt werden, als auch in Form einer E-SIM. Auf der SIM selbst ist ein Patternbasierter Vierenscanner etabliert. Außerdem wird eine feste Bindung zwischen SIM und Endgerät hergestellt. TMMNS Network Protection Die Network Protection von Trend Micro setzt direkt an den neuralgischen Kommunikationsschnittstellen eines 5G Cores an. Mit der TMMNS Lösung ist Trend Micro in der Lage alle Bereiche eines privaten 5G Netzwerkes abzusichern. Sowohl den Bereich der Endgeräte als auch die Luftschnittstellen und die Core Systeme als solches.

TREND MICRO™

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
5	10.05.	12:45 - 13:10	Saal NAIROBI	Jochen Brückner Gregor Jehle	Principal Network Solutions Consultant dainox GmbH Geschäftsführer P3KI GmbH

Menschliches Vertrauen für die digitale Welt - Robuste, dezentrale und offlinefähige Rechtedelegation im Feld

Im Kern jeder Digitalisierungsbestrebung liegt das Rechtemanagement: Wer darf wann, was, mit welchen Daten anstellen? Wer ist berechtigt Daten einzuspeisen, anzusehen, zu bearbeiten, Befehle zu erteilen? Stand der Technik sind hier komplexe PKI- und Zertifikatsinfrastrukturen. Doch diese skalieren nicht bezüglich der besonderen militärischen Anforderungen wie verschiedene Sicherheitsdomänen, multinationale Interoperabilität, Dezentralität und Offlinefähigkeit. Wir präsentieren ein neuartiges, hochflexibles Berechtigungssystem, welches den Erhalt der Operationsfähigkeit auch unter widrigsten Bedingungen ermöglicht. Betrachtet werden verschiedenste Szenarien wie Kommunikation der Truppe im Feld (Last Mile) sowie der Umgang mit Verlust und Rückeroberung militärischer Infrastruktur unter Nutzung der LoRa WAN Technologie, aber auch Kommunikation zwischen Bündnispartnern oder Dokumentenklassifikation und Zugriffberechtigung jeweils als Ergänzung zu bestehenden X.509 PKI Infrastrukturen. Falls Sie leere Hypeversprechen wie Blockchain erwarten, sind Sie hier falsch. Stattdessen setzt die präsentierte Technologie an den relevanten Stellen auf formale Sicherheitsreduktion und mathematische Beweisbarkeit. In diesem Vortrag erfahren Sie, wie Sie Ihr Berechtigungssystem jetzt strategisch auslegen müssen, um in Zukunft taktisch reagieren zu können. Des weiteren erhalten Sie einen Einblick in den Einsatz und Möglichkeiten der LoRa-WAN Technologie. Für eine persönliche Einführung mit Live-Demo in P3KI und LoRa WAN besuchen Sie uns gerne jederzeit am Stand von dainox (S33/Saal New York/Genf).

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
6	10.05.	13:15 - 13:40	Saal NAIROBI	Dr. Christian Jürgens	Lead Expert „Sustainability & Green IT“

Green IT – Die Brücke zwischen Nachhaltigkeit und Resilienz?

Green IT erfährt in heutigen Zeiten zunehmende Bedeutung, die deutlich über einen Trendbegriff hinausstrahlt.

Die zukunftsfähige Nutzung von Ressourcen erfordert insbesondere vor dem Hintergrund zunehmender Digitalisierung und vernetzter Akteure neue Herangehensweisen.

Als strategisches und datenbasiertes Thema im Bereich des Sustainability-Managements fokussiert Green IT die Umsetzung von intelligenten Lösungen aus den Bereichen effizienterer IT-Infrastrukturen, nachhaltiger Prozesse und nachhaltiger Software von der Beschaffung bis zur Implementierung. Steigende regulatorische Anforderungen, die Verminderung von Abhängigkeiten und die Bemessung im Bereich von Carbon Footprints und Lebenszykluskosten mittels digitaler Lösungen ergänzen bisherige Betrachtungen im Bereich der Wirtschaftlichkeit.

Wo liegen Chancen und bestehende Herausforderungen von Green IT? Was sind aktuelle Trends und Fokusbereiche? Wir geben einen Überblick.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
7	10.05.	13:45 - 14:10	SAAL NAIROBI	Dr. Christoph Erdmann	Geschäftsführer Secusmart und SVP BlackBerry Secusmart

SecuSUITE for Samsung Knox - der VS-NfD sichere mobile Arbeitsplatz

„Der VS-NfD sichere mobile Arbeitsplatz innerhalb der Bundeswehr und Bundesbehörden“ SecuSUITE for Samsung Knox ist mittlerweile als VS-NfD sicherer mobiler Arbeitsplatz innerhalb der Bundeswehr und der Bundesbehörden nicht mehr wegzudenken. Angefangen mit verschlüsselter Telefonie über den sicheren Austausch dienstlicher E-Mails ist die Lösung zum Synonym für sichere Smartphones & Tablets mit BSI-Zulassung bis VS-NfD geworden. Die fortschreitende Digitalisierung erfordert mehr denn je mobile Lösungen zu der Verschlusssachen konformen Verarbeitung von Informationen. Innerhalb der Bundeswehr und Bundesbehörden sind dabei managebare und flexible Lösungen gefragt, die weit über den Austausch dienstlicher Email- und PIM-Daten hinaus gehen und in der Lage sind, weitergehende Nutzeranforderungen zu integrieren. In nur einem Jahr hat die BWI mehr als 25.000 abhörsichere Smartphones und Tablets in der Bundeswehr ausgerollt. Zusätzlich verfügen die Smartphones und Tablets unter anderem über gehärtete Apps und die Secusmart Security Card, die den verschlüsselten Transfer von Daten und Sprache ermöglicht. Die Lösung ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Geheimhaltungsstufe VS-NfD zugelassen. Dazu unterzeichneten BWI und Secusmart bereits in 2019 in Bonn einen Rahmenvertrag, mit dem die beiden Unternehmen ihre langjährige Zusammenarbeit auch künftig unterstreichen. Der Vortrag beinhaltet neben der Bereitstellung, Nutzung und dem Betrieb von mobilen Endgeräten für eine Übertragung von Daten und Sprache bis zu VS-NfD auch deren Integration in das IT-System der Bundeswehr.

BlackBerry® | secusmart®

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
8	10.05	14:15 - 14:40	Saal NAIROBI	Robert Wortmann	Practice Lead Cyber Defence

Datenzentrische Betrachtung von SOC/CERT Strukturen

Durch Security Operations Center (SOC) sollen Security-Incidents überwacht, erkannt, analysiert und behoben werden. Doch oftmals fehlt es den Betriebsteams an ausreichender Visibilität für die erfolgreiche Erbringung dieser Aufgaben. Dies ist unserer Erfahrung nach selten das Problem der zentralen Plattformen wie SIEM oder XDR, sondern liegt daran, dass innerhalb der Anforderungsanalyse die Datenstruktur der Organisation nicht genug betrachtet wurde. Organisationen müssen sich also die Frage stellen, welche Sensoren von Relevanz sind. Hierunter fallen typische Daten wie Endpoint und Netzwerktelemetrie, aber auch immer häufiger Daten aus beispielsweise IoT oder gar 5G Technologien. Wir möchten in diesem Vortrag aufzeigen, wieso nur eine datenzentrische Anforderungsanalyse, gepaart mit einer Threat Intelligence Analyse, zu einer erfolgreichen Umsetzung von zentralen Maßnahmen im SOC führen kann. Wie können Organisationen die richtigen Daten finden und wieso bedarf es in vielen Fällen einen massiven Betriebsaufwand für die Aufbereitung dieser Daten bevor eine relevante Sicherheitsanalyse durch das SOC-Team überhaupt möglich ist? Wir gehen außerdem auf die Frage ein, mit welchen Daten beim SOC Aufbau begonnen werden sollte, so dass Mehrwerte schnell sichtbar und Investitionen durch Messbarkeit dieser möglichst schnell gesichert werden können.

TREND MICRO™

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
9	10.05	14:45 - 15:10	Saal NAIROBI	Tassilo Markert-Mesters	Head of Defence Germany

KI für die Streitkräfte – eine Frage der (Trainings)daten und wie sie gewonnen werden

Der Vortrag wird zunächst die Lösung GlobeRanger vorstellen, diese ist in Zusammenarbeit mit der US-Army entstanden. Wir werden bereits im Einsatz befindliche Lösungsansätze (zivil, mil) präsentieren. Des Weiteren werden die infrastrukturellen Voraussetzungen beleuchtet.

Nach den Anwendungsmöglichkeiten werden Beispiele skizziert, wie diese Auswirkungen auf den Führungsprozess haben können. Schlüsselwörter wie Digital Twin und KI gestützte Entscheidungen werden von abstrakt zu konkret heruntergebrochen.

Fujitsu hat bei NATO Streitkräften jahrelange Erfahrung gesammelt und Prozesse mit neuster Technologie automatisiert. Unsere Edgeware-Lösungen ermöglichen durch Digitalisierung eine präzise Echtzeitüberwachung und sichere Verwaltung der gesamtem militärischen Lieferkette.

FUJITSU

Nr.	Tag	Zeit	Ort
S 1	10.05.2022	15.30 h - 17:30 h	SAAL NAIROBI

Startup Pitch Session

Innovation für eine sichere Digitale Zukunft

Kurzbeschreibung zum Thema:

„Welche Herausforderungen haben innovative Startups in der Bundeswehr?“ Diese Frage stellen wir uns während der Startup Pitch Session und anschließenden Panel-Diskussion im Saal Nairobi. Als Vertreter und Treiber von Innovation im öffentlichen Bereich, werden sich **6 ausgewählte Startups** vorstellen, um ihre Erfolgsgeschichten in der Umsetzung von innovativen Lösungsansätzen zu präsentieren. Gemeinsamen mit **Key-Stakeholdern aus der Bundeswehr** werden wir die identifizierten Herausforderungen diskutieren und Barrieren für Innovation aufzeigen.
Hier im Schwerpunkt: Die Dringlichkeit einer agilen und innovativen Denkweise bei der Zusammenarbeit zwischen Militär und Rüstungsindustrie. Dazu streben wir einen **offenen Austausch mit dem Plenum** an und möchten die Teilnehmer zu einem abschließenden **Ausklang mit den Startups** einladen.

ALEPH ALPHA

Inhubber

KENBUN
Experten für digitale Sprachsysteme und Künstliche Intelligenz

MOTIONMINERS

PREVENCY®
Immersive Simulations

scalue

Ablauf:

15.30 h	16.00 h	16.30 h	17.00 h
Begrüßung	*Pitch*	*Panel*	*Ausklang*

Industrievorträge

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
10	10.05	09:15 - 09:40	Raum ADDIS ABEBA 3	Matthias Köhler	Sales Manager Mission System Business Unit Integrated Electronic Systems

Der KI-unterstützte Feuerkampf

Speziell für zukünftige Generationen von Gefechtsfahrzeugen wird eine stark reduzierte Personalstärke pro Gefechtsfahrzeug gefordert, wodurch die Anforderungen an die Assistenzsysteme drastisch erhöht werden und sich eine gesteigerte Aufgabenkomplexität und ein breiteres Aufgabenspektrum ergibt. Demnach muss die Aufgabenverteilung im Zusammenwirken von Bedienern und Maschine grundlegend angepasst werden, sodass die Fahrzeugbesatzung im Bereich der Beobachtung und Zielerfassung sowie in der Entscheidungsfindung und Wirkung entlastet werden kann.

Ein mögliches Einsatzgebiet eines solchen Assistenzsystems ist die automatisierte Erkennung von (gegnerischen) Fahrzeugen im eigenen Sichtfeld durch die Auswertung von Bild- und Videosignalen. Über diese Assistenz kann die Fahrzeugbesatzung entlastet werden und Fahrzeuge erlangen die Fähigkeit selbstständig aufzuklären, erkannte Objekte zu klassifizieren und in die Bedrohungslage einzuordnen. Die Nutzbarmachung dieser Funktion eröffnet Möglichkeiten zur Reduzierung und Entlastung der Soldaten.

Grundsätzlich lässt sich ein starker Bedarf an Unterstützungsmöglichkeiten mittels Automatisierung von Prozessschritten im gesamten Aufgabenspektrum zukünftiger Generationen von Gefechtsfahrzeugen erkennen. Daher wird KI-Assistenz in der Umgebungswahrnehmung genutzt

Das System ATTAC soll durch gezielte Informationsverarbeitung, Prozesse automatisieren und beschleunigen. Dazu wird bei Gefahrendetektion durch spezifische Sensoren die Kommandantensicht auf den Detektionsbereich zentriert.

Ziel des Systems ATTAC ist die schnelle und akkurate Unterstützung des Kommandanten und Richtschützen im Gefechtsfahrzeug. Das Detektions- und Klassifikationssystem muss daher alle relevanten Objekte mindestens so schnell wie der menschliche Beobachter und mit hinreichender Genauigkeit detektieren, klassifizieren und in den Gefahrenkontext einordnen können.

Die Verwendung von KI in der Feuerleitung und Sensorik:

- schnellere Lagebeurteilung und Feuereröffnung
- zuverlässigere Entscheidungen und Treffleistung
- Entlastung für die Besatzung
- erhöhte Überlebensfähigkeit von mil. Plattformen.

Der Vortrag stellt die aktuelle und seriennahe Verwendung von KI für die Objekterkennung und -klassifizierung in Echtzeit in der Feuerleitung dar. Die Anwendung auf Plattformen für direktes Feuer hat dabei die größte Relevanz. Durch Aufwuchs von Vernetzungspotential sind jedoch auch unmittelbare Implikationen für den Einsatz von indirekten Wirkungen erkennbar.

RHEINMETALL

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
11	10.05.	09:45 - 10:10	Raum ADDIS ABEBA 3	Marco Schläppi B.A.Sc.	ICT Senior System Architect, RUAG

Sichere Vernetzung im taktischen Netzwerk durch verschlüsselte Übertragung

Die fortschreitende Digitalisierung im Verteidigungsumfeld stellt laufend höhere Anforderungen an die militärische Kommunikationsinfrastruktur. Die Einbindung unterschiedlichster Fachsysteme bis in die unterste taktische Ebene erhöht die Komplexität des Gesamtsystems und stellt entsprechend erweiterter Anforderungen an die Sicherheit und an die gesamte Netzwerkinfrastruktur. So gewinnen Themen wie Datendurchsatz, Resilienz, Integrität und auch die «Quality of Service» wachsend an Bedeutung.

Im Rahmen der Digitalisierung innerhalb der Schweizer Armee erhielt RUAG den Zuschlag für den Ersatz des Kommunikationsnetzwerkes auf der taktischen Ebene. Das Netzwerk besteht aus unterschiedlichen Knotentypen und bildet das Rückgrat der militärischen Kommunikation. Neben der Übertragung von Sprache ist das System verantwortlich für den gesamten Datenfluss der unterschiedlichen Fachsysteme wie zum Beispiel die Systeme zur Lagebildbeurteilung, Radaraufklärung und weitere. Ein zusätzlicher, wesentlicher Aspekt der Lösung umfasst die Durchgängigkeit von Daten vom Soldaten bis ins Hauptquartier.

Die RUAG Tactical Communication Solution liefert dank einer soft- und hardewarebasierten Lösung das Herzstück der taktisch-militärischen Kommunikation. Der von RUAG entwickelte «Security Core» ermöglicht dabei eine durchgehende, validierbare Rot-Schwarz-Trennung und stellt somit die Authentizität und Integrität der zu übertragenden Daten sicher. Die Fähigkeit der Mandantentrennung erlaubt die Isolierung der verschiedenen Anwendungen und Fachsysteme. Mit dieser taktischen Lösung ist die Interoperabilität und nahtlose Integration in bestehende Kommunikationsinfrastrukturen, sowie bestehende Umsysteme (Legacy) gewährleistet und stellt eine vollkommene Durchgängigkeit von der Führungsebene bis in die mobile Ebene sicher. RUAG ist sich der Wichtigkeit und Tragweite bewusst und bietet eine umfassende, integrierbare, sichere und zukunftsgerichtete Kommunikationslösung an, immer unter Einhaltung der grundlegenden Anforderungen und Bedürfnisse an ein solches System.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
12	10.05.	11:00 - 11:25	Raum ADDIS ABEBA 3	Hartmut Lohrey	EMV-Fachreferent

Schutz sicherheitsrelevanter Daten vor elektromagnetischen Beeinflussungen

Elektromagnetische Felder sind als unvermeidliche Folge von fließenden Strömen und wechselnden Spannungen Ursachen elektromagnetischer Beeinflussungen. Die ausgesendete Energie, meist HF-Strahlung, ist – wenn es sich nicht um Funkanlagen handelt - unerwünscht, bisweilen auch schädlich. Der Einsatz starker Felder kann elektronische Geräte stören oder gar zerstören und ungewollt ausgesendete schwa-che Felder können Informationen für Dritte empfangbar machen. IT-Racks können die eingebaute Hardware vor äußeren Feldern zusätzlich schützen und das Risiko der ungewollten Weitergabe sicherheitsrelevanter Daten vermindern. Damit helfen insbesondere schirmungstechnisch verbesserte Racks den Betrieb und die Zukunfts-fähigkeit der IT-Systemlandschaften zu sichern. Grundlage der Auswahl, ob Serien IT Rack, die verbesserte EMV Variante oder Sonderkonstruktion für höchste Schutzanforderungen zum Einsatz kommen sollen, ist die Orientierung an der vorausgehenden Risikoanalyse. Der Vortrag geht auf die Risiken und Lösungsmöglichkeiten kurz ein und gibt Hinweise zu einer umfassenden Betrachtung der Schutzwirkung schirmender Gehäuse inklusive der Schnittstellen von IT Rack-Anwendungen.

RITTAL

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
13	10.05.	11:30 - 11:55	Raum ADDIS ABEBA 3	Dr. Andreas de Jonge	Head of Artificial Intelligence

Künstliche Intelligenz im Wärmebild

Künstliche Intelligenz (KI) und vor allem künstliche neuronale Netzwerke sind in der Verarbeitung von Bilddaten längst Standard. Beeindruckende Ergebnisse in den Bereichen Klassifizierung, Detektion, Lokalisation und Segmentierung sind für zukünftige Anwendungen in der Wehrtechnik vielversprechend.

Trotz aller Erfolge zeigt sich aber ein Leistungseinbruch, wenn diese Techniken auf Bilddaten angewendet werden, die nicht ganz der Domäne entsprechen, aus der die zum Training der Algorithmen verwendeten Daten entstammen. Gerade der Bildkontrast ist eine große Herausforderung bei der Translation von KI auf Wärmebilder.

Die Beschaffung eines für das Training ausreichend großen und qualitativ hochwertigen Datensatzes stellt seit jeher eine nicht zu vernachlässigende Hürde im Bereich der KI dar. Aufgrund der geringeren Verfügbarkeit von Daten im Wärmebildbereich ist diese Hürde ungleich höher. Wärmebilddaten für den Verteidigungs- und Sicherheitsbereich in das Training einer KI miteinzubeziehen, potenziert hierbei die Komplexität der Anforderungen erheblich.

Mit unserem Vortrag wollen wir unseren Lösungsansatz für eine verlässliche KI im Wärmebildbereich präsentieren. Wir zeigen, dass die Verwendung von künstlich erzeugten Daten erhebliche Kosten- und Trainingsvorteile gegenüber herkömmlich aufgenommenen Daten bietet. Darüber hinaus demonstrieren wir die weitestgehend nahtlose Einsatzbereitschaft einer so trainierten KI in Bezug auf reale Daten. Im Rahmen des Vortrags zeigen wir ebenfalls die Nachvollziehbarkeit der Ergebnisse unserer Algorithmen auf.

Über VECTED

Als Spezialist für Wärmebildtechnologie und Ingenieursdienstleistungen entwickeln und produzieren wir Wärmebildgeräte sowie Elektronikmodule und bieten unseren Kunden individuelle optoelektronische Lösungen. Im Bereich Rüstung sind wir in der Lage, den gesamten Entwicklungs-, Qualifikations- und Produktionsprozess zu leisten. Von der Entwicklung, inkl. Konstruktion sowie Elektronik- und Softwaredesign, über den Prototypenbau und die Qualifikation bis hin zur Produktion kommt bei VECTED alles ITAR-frei aus einer Hand.

Kontakt: Ralph Wilhelm
E-Mail: info@vected.de
Tel: +49 911 960 687 0

VECTED
ENGINEERING. ADVANTAGE

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
14	10.05.	12:00 - 12:25	Raum ADDIS ABEBA 3	Jan Erbe	HENSOLDT Optronics Head of Land Solutions

Partnerschaftlicher Ansatz der deutschen Industrie für Sensorfusion

Der laufende Ukrainekonflikt hat die strategische Bedeutung moderner Führungsfähigkeit und Vernetzung auf dem Gefechtsfeld, eine alte militärische Erkenntnis, erneut prominent vor Augen geführt. Das deutsche Zukunftsvorhaben Digitalisierung landbasierter Operationen (D-LBO) beabsichtigt vor diesem Hintergrund die dringend benötigte Fähigkeitssteigerung im Bereich der Führungsfähigkeit des deutschen Heeres zu realisieren. Diese Mammutaufgabe benötigt das Pooling der besten nationalen Kompetenzen, um gemeinsam mit dem zukünftigen Nutzer in iterativen Entwicklungsschritten das vernetzte Gefechtsfeld der Zukunft aufzubauen.

Die Firma HENSOLDT hat für den Anteil Sensorfusion gemeinsam mit nationalen Partnern eine strategische Roadmap und Lösung mit konkreten, bereits existierenden Demonstratoren entwickelt. Nur gemeinsam, Hand in Hand zwischen Nutzer und Industrie, wird diese massive Anstrengung erfolgreich sein und Informationsüberlegenheit schlussendlich zu Wirkungsüberlegenheit führen können.

HENSOLDT
Detect and Protect.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
15	10.05	12:30 - 12:55	Raum ADDIS ABEBA 3	Enrico Scharlock	Aerospace & Defense Industry Solution Experience Senior Director

Modellbasiertes Systems of Systems Engineering (MBSE/SoSE) für NGWS

Das Future Combat Air System (FCAS) und das Next Generation Weapon System (NGWS) im Speziellen sollen in der Lage sein, Bedrohungen der Zukunft zu beantworten. Dazu zählen neben bekannten Bedrohungsszenarien auch Herausforderungen von heute möglicherweise unbekannten Ausmaßen. Künftige Luftwaffensysteme werden daher nicht nur formulierte Anforderungen erfüllen müssen. Sie müssen auch für künftige Einsatzszenarien anpassungsfähig bleiben, um die Überlegenheit zu wahren. Gleiches gilt für jede andere Dimension, sei es Land, See, Cyber oder Space, besonders in Multi-Domain Operations mit internationalen Bündnispartnern. Um diesen Herausforderungen zu begegnen, setzt die Industrie auf unterschiedliche Methoden und Werkzeuge. Die Entwicklung von komplexen Waffensystemen und Systems of Systems benötigt einen holistischen Ansatz von Konzept, Entwicklung, Fertigung und Wartung. Unterschiedliche Domänen (z.B. Mechatronik, Avionik, Embedded Software usw.) müssen einheitlich entwickelt werden und miteinander kommunizieren. Darüber hinaus wird eine zunehmend engere modelbasierte Zusammenarbeit über den gesamten Lebenszyklus des Systems benötigt. Das gilt sowohl zwischen Herstellern und Streitkräften während der Konzeptphase als auch zwischen den Herstellern und der Zulieferkette in der Entwicklungs- und Fertigungsphase und schließlich den Streitkräften und der gesamten Wertschöpfungskette während der Einsatzphase. Ein zukunftsfähiges Waffensystem bedarf daher einer Produktentwicklung, die den Entwicklungsprozess von der ersten Studie bis zur Außerdienststellung über den gesamten Produktlebenszyklus vollumfänglich abdeckt. Model-based Systems of Systems Engineering hilft nicht nur dabei hochkomplexe Systeme zu entwickeln. Es vermag auch durch ein gemeinsames Systemverständnis bei allen Beteiligten jegliche Anforderung zu erfüllen und flexibel auf neue Anforderungen reagieren zu können, dabei Entwicklungszeiten zu verkürzen und so letztlich einen nachhaltigen Mehrwert darzustellen.

DASSAULT SYSTEMES

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
16	10.05	13:00 - 13:25	Raum ADDIS ABEBA 3	Volker Brands	Regional Sales Manager

Funkaufklärung – neu gedacht! Schnelles und genaues Lagebild für Überlegenheit in taktischen Missionen und Bereitstellen wertvoller Informationen für die Kommandoebene

Viele alte und neue Herausforderungen konkurrieren meist gegeneinander, um oben genannte Ziele zu erreichen - Einrichtungen zur Funkaufklärung sollen idealerweise preisgünstig sein (COTS/MOTS), nicht ausfuhrkontrolliert, einfach skalierbar und integrierbar, schnell verfügbar, SWAP (size, weight and power) optimiert, flexibel, sicher, und sowohl portabel im stand-alone (Stealth mode) als auch als (mini-)System erweitert operabel sein!

Wie ist der Widerspruch zwischen diesen Anforderungen zu lösen? Oder besteht bei diesen offensichtlichen Zielkonflikten auch eine Chance für die Etablierung neuer Lösungen?

Der‚hidden champion' für die Analyse von EMF (electro-magnetic-fields) und EMC (electro-magnetic-compatibility) Narda-STS GmbH in Pfullingen (Baden-Württemberg) hat diese Herausforderungen angenommen. Als Wandel & Goltermann Messgeräte GmbH (später firmiert unter Acterna, dann JDSU, nun VIAVI) vor 100 Jahren gegründet, wurde deren RF-Sparte Ende 1999 an das US-Unternehmen Narda-Miteq (N.Y./US) veräußert. Als Jahrzehnte-langer Marktführer im Bereich EMF Technologie hat die Narda-STS GmbH - später im Konzern L3 / Harris- über ein Jahrzehnt mit ihrer Messtechnik-Erfahrung eine Produktfamilie von tragbaren Empfängern und Peilantennen im Bereich 8 kHz bis 8 GHz entwickelt. Nachdem die ersten Produkte (IDA2, NRA-6000RX) sehr gut vom Markt angenommen wurden (Aufklärung, Geheimdienste, NATO, Bundespolizei, Heer, Innenministerien, Küstenwache, etc.) ist mittlerweile eine neue Produktfamilie entwickelt worden: SignalShark & ADFA2.

Dank eines kostengünstigen und trotzdem hoch-performantem Konzept konnten viele der oben genannten und gewünschten Eigenschaften realisiert werden, nämlich ein offenes (Schnittstellen-) Konzept, MOSA (modular open system architecture) bezüglich der eingesetzten Hardware (HW) & Software (SW). Des Weiteren bietet die Plattform Geräte für den Außeneinsatz (leicht & tragbar oder für die Mastmontage) oder Einbau (cabinet / vehicle), HW & SW (auch 3rd party) erweiterbar, autonom oder im Verbund betreibbar!

Wir laden Sie gerne auf
unseren Stand Nr. S62
zu Ihrer persönlichen
Live-Präsentation ein!

narda
Safety Test Solutions

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
17	10.05	13:30 - 13:55	Raum ADDIS ABEBA 3	Dipl. Päd. Stefan Pforte	Geschäftsführer, Algorithmen Design KNN

Mit künstlichen neuronalen Netzen orchestrierte Meinungsmanipulation zielgenau aufklären

Die Somtxt UG ist eine Analysefirma in Rostock, die auf die Verarbeitung und Mustererkennung in großen Textdatenbeständen spezialisiert ist. Wir arbeiten dazu mit künstlichen-neuronalen Netzen und weiteren statistischen Verfahren. Mit dem von der Somtxt UG entwickelten Algorithmus Textrapic und der Plattform Kalevi bietet die Somtxt UG eine Lösung, die Advanced Persistent Manipulator (APM) Teams identifiziert, die über soziale Medien und digitale Plattformen Meinungsmanipulation betreiben. Die Somtxt UG kann insbesondere unter der Einbindung zweier sehr populärer sozialer Netzwerke mehrere tausend Web-Seiten innerhalb weniger Tage identifizieren, auf denen Verschwörungserzählungen, Propaganda oder Falschnachrichten kultiviert und von APM Teams verbreitet und in manipulativer Absicht künstlich verstärkt werden, wahlweise in russischer, englischer, spanischer, französischer und weiteren Sprachen. Neben autokratischen Regimen wirken auch in den Mitgliedsländern der Europäischen Union angesiedelte Unterstützer-Organisationen durch APM Teams strukturiert und planvoll mit Cyber-Einflussoperationen auf die hiesige Bevölkerung. Auch diese Organisationen verwenden Methoden und Taktiken, die mit Somtxt UG Technologie aufgeklärt werden können. In unserem Industrievortrag zeigen wir den Datenverarbeitungsprozess und die Mustererkennung mit künstlichen neuronalen Netzen in der Kalevi-Plattform, sowie die Binnenstruktur fremdstaatlich gesteuerter Meinungsmanipulation exemplarisch auf. An verschiedenen Beispielen erfolgreicher Mustererkennung geben wir dem Fachpublikum einen tiefen Einblick in die Wirkmechanismen und grundlegenden Eigenschaften manipulativer Kampagnenarchitekturen, um zu verdeutlichen, in welcher Qualität und vor allem Quantität sich die wachsende Herausforderung der Meinungsmanipulation darstellt.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
18	10.05.	14:00 - 14:25	Raum ADDIS ABEBA 3	Andreas Schiel	Director Geschäftsfeld Kampf

Führungsfähigkeit Division 2025 – Energieversorgung

Eine leistungsfähige und verlässliche Energieversorgung ist auf dem Gefechtsfeld von entscheidender Bedeutung: Moderne, hochgradig digitalisierte Kriegswaffen, Führungssysteme, Funkgeräte und IT-Komponenten benötigen Strom, um erfolgreich eingesetzt werden zu können. Daher ist es unerlässlich, dass die Energieversorgung jederzeit robust, zuverlässig und sicher gewährleistet ist. In der Vergangenheit wurden für die Energieversorgung auf dem Gefechtsfeld hauptsächlich mobile Stromgeneratoren mit hohen Betriebsstoffbedarfen eingesetzt. Eine neue, richtungsweisende Lösung in diesem Bereich ist die „New Prime Power Unit" (NPPU) des Counter Battery Radar (COBRA), die sich unter anderem durch einen signifikant niedrigeren Betriebsstoffbedarf auszeichnet und dadurch vergleichsweise leichter versorgen lässt.

Das der NPPU zugrunde liegende innovative Konzept baut auf die Vorteile von hybrid variablen Stromgeneratoren mit dynamischer Drehzahl in Kombination mich hochleistungsfähigen Batteriepuffern („Supercaps"). Diese Generatoren passen den Strombedarf automatisch an die Last an, so dass der Kraftstoffverbrauch bei gleichzeitig hoher Performanz und Zuverlässigkeit optimiert wird.

Dieser mit dieser Lösung realisierbare Effizienzgewinn ist insbesondere für Einsatzszenarien in abgelegenen Gebieten ohne eine verlässlich verfügbare Energie-Infrastruktur von enormem Einsatzwert. Zudem wirken sich die vergleichsweise höhere Zuverlässigkeit und leichtere Versorg- und Wartbarkeit positiv hinsichtlich der Betriebskosten aus.

Die Technologie der New Prime Power Unit bietet den eingesetzten Kräften eine robuste und zuverlässige Energiequelle, die sie nachhaltig bei der erfolgreichen Erfüllung ihres Auftrags auf dem Gefechtsfeld unterstützt.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
19	10.05	14:30 - 14:55	Raum ADDIS ABEBA 3	Steffen Ullrich genua GmbH	Technology Fellow

Souverän, Resilient, Agil: Warum moderne Verteidigung digitale Nachhaltigkeit braucht

Die zunehmende Digitalisierung ist auch im Verteidigungssektor eine Mammutaufgabe. Sie erfordert Flexibilität, Agilität und Öffnung von IT-Infrastruktur. Digitale Ökosysteme und Wertschöpfungsketten sorgen für steigende Komplexität und bringen neue Abhängigkeiten. Hinzu kommt die hohe Geschwindigkeit technologischer Entwicklungen wie Quantencomputer und KI, welche sowohl Chancen sein können als auch neuartige Risiken produzieren.

Nachhaltigkeit im Kontext der Digitalisierung geht weit über ökologischen Aspekte hinaus und zielt darauf ab, sowohl in der aktuellen als auch zukünftigen digitalisierten Gesellschaft souverän handeln und gestalten zu können. Digitale Nachhaltigkeit ist daher eine wesentliche Voraussetzung dafür, die digitale Transformation mit ihre Risiken für Staat und Gesellschaft zu beherrschen und eine stabile, vertrauenswürdige und zukunftsfähige digitale Infrastruktur zu schaffen. Das Paradigma der Digitalen Nachhaltigkeit lässt sich in fünf Dimensionen beschreiben: Beherrschbarkeit, Robustheit, Sicherheit und Zukunftsfähigkeit der eingesetzten Technologien sowie, als Fundament, die technologische Souveränität.

Ein aktuelles Beispiel für nachhaltig gedachte Digitalisierung ist der neue europäische Cyber Resilience Act (CRA). Er zielt darauf ab, die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen festzulegen und unter anderem „Security by Design“ vorzugeben. Es ist heutzutage weitgehend akzeptiert, dass eine solide Sicherheit tief in dem Design von Produkten und Infrastrukturen verankert sein muss. Eine nachträgliche Härtung komplexer Systeme ist sowohl kostspielig als auch unzureichend.

In seinem Vortrag erklärt Technology Fellow Steffen Ullrich, welche Herausforderungen und Lösungsansätze sich hinter den fünf Dimensionen Digitaler Nachhaltigkeit verbergen, und wie diese im Sinne einer nachhaltigen Cybersicherheitsstrategie zusammenspielen. In seinem „Security by Design Deep Dive“ zeigt er außerdem beispielhaft, wie zentrale Designprinzipien von minimalen Privilegien und mehrstufiger Sicherheit in Produkten am Beispiel der Highly Resistance Firewall genugate umgesetzt

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
20	10.05.	15:00 - 15:25	Raum ADDIS ABEBA 3	Patrick Rund	Senior Manager InfoKom

Sicherheitsdomäne as a Service & safeAI

Geleitet vom modularen Baukastenprinzip, entwickeln IABG, Infodas und Kernkonzept eine modulare Cloud-Lösung (als Private-Cloud), die mit unterschiedlichen Sicherheitsdomänen „as a Service“ die Cloud als echte elastische Ressource für VS-IT erschließt: verschieden eingestufte Sicherheitsdomänen können mit ein- und derselben Hardware betrieben werden. Erstmals schaffen wir die Übertragung von Skalierungseffekten und Effizienzgewinnen der typischen Cloud-Technologien auf die VS-IT über Einstufungsgrenzen hinweg. Zudem wird die Bereitstellung von IT-Services über unterschiedliche Sicherheitsdomänen im „Zero-Touch Prinzip“ möglich sein. Auf diesem Wege werden entscheidende Vorteile in der Verarbeitung von eingestuften Daten möglich. Beispielsweise können Aufklärungsdaten schnell sowie mit entsprechenden Cloud-Technologien ausgewertet werden und so militärische Operationen mit Informationsüberlegenheit zum Erfolg führen.

Unsere modulare Cloud-Lösung berücksichtigt die Vorgaben der VSA und DSGVO, stellt digitale Souveränität sicher und berücksichtigt die strategischen Vorgaben des Bundes bzgl. Cloud-Computing. Durch einen kontrollierten Informationsaustausch zwischen den verschiedenen Sicherheitsdomänen stellen wir Ende-zu-Ende digitalisierte Prozesse über Einstufungsgrenzen hinaus und innerhalb der Cloud sicher, einschließlich Erstellen von NATO STANAG 4774/4778 konformen und hochsicheren Security Labeln für Daten.

safeAI:

KI-basierte Systeme gewinnen nicht nur im militärischen Kontext stark an Bedeutung. Sie werden in der Regel in Cloud-Umgebungen entwickelt, gespeichert und genutzt. Das safeAI-Team der IABG entwickelt Lösungen für die Bewertung der Sicherheit und Robustheit von KI in Produktivumgebungen. Wir kombinieren die langjährige Erfahrung der IABG auf den Gebieten Test-, Analyse- und Zertifizierungsprozesse mit neuesten Erkenntnissen aus KI-Normungsgremien auf nationaler, Europäischer und internationaler Ebene, die wir aktiv mitgestalten.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
21	10.05.	15:30 - 15:55	Raum ADDIS ABEBA 3	Herr Sejong Yoo	General Manager

Novachips CC/CSfC-certified military-grade SSDs

Cybersecurity is becoming a top priority, and self-encrypting SSDs (Solid-State Drives) are necessary to prevent the recovery of collected mission data by adversaries. Furthermore, new types of autonomous vehicles and machines are required to process and record a larger amount of mission data within a smaller footprint size, so it requires a higher density of data storage with requiring a higher level of operating reliability and security.

NSA-approved CSfC (Commercial Solution for Classified) DARCP (Data-At-Rest Capability Package) can help to achieve those goals by adopting double layers of encryption from two independent vendors. Novachips is listed as one of CSfC approved component vendors of HWFDE (hardware full disk encryption), and its SCALAR and EXPRESS P-series SSD can be a good candidate to consist of the various types of HF, HS, or HH solutions with combining with software encryption layer for building the trusted computing system.

In the case of using SSD as the primary OS disk, the system is required to perform pre-boot authentication even before booting up the main OS. For this purpose, Novachips is providing the bundle PBA image which is can be cloned into the Shadow disk area of CSfC SSD. Only after acquiring authorization by authenticating the user password or other authentication factors, the full-capacity User disk will appear automatically.

Especially for defense and military application, Novachips P-series SSDs are designed and tested for the extreme condition where the temperature cycling range from -40 ~ +85°C, the vibration/shock peaks up to 40G, and the radiation level is 500 times higher than zero altitudes. SSD can also service the commands of immediate zeroization or sanitization method per NIS800-80 compliant Purge or Clear methods. And those security erase functions can be triggered via hardware signal or host command without any 3rd party host production or additional hardware elements.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
22	10.05.	16:00 - 16:25	Raum ADDIS ABEBA 3	Andreas Reinecke Robert Sekora	Head of Secure Communications Business Growth Advanced Studies Manager

Breitbandige BLOS Konnektivität für die vernetzte Operationsführung

Seit dem Start des ersten Nachrichtensatelliten hat der Bedarf an sogenannter „Beyond Line of Sight (BLOS)" Kommunikation, also Funkverbindungen über die Sichtweite hinaus, dramatisch zugenommen. Während diese Art der Kommunikation anfangs weitgehend auf stationäre Teilnehmer über feste Bodenstationen beschränkt war, wurde diese seit Beginn dieses Jahrtausend verstärkt auf (teil-) mobile Anwendungen für Land-, See- und Luftstreitkräfte erweitert. Aus der zivilen und militärischen Welt ist diese Technik nicht mehr wegzudenken. Gerade durch neue Trends, Märkte und Technologien hat die satellitengestützte Breitbandkommunikation einen weiteren Schub erhalten und eröffnet damit bisher nicht bekannte Möglichkeiten für eine vernetze Operationsführung.

Das bedeutet aber auch, dass diese Art von Breitbandkommunikation mit bestehend Kommunikationsmitteln und Netzwerken interagieren kann. In der Praxis müssen daher eine Vielzahl an Teilnehmern eingebunden werden, Besonders wichtig ist dabei eine stabile Verbindung, und dass die Informationen sicher und zuverlässig den entsprechenden Empfänger erreichen. Dies wird heute zwar schon mit komplexen Nachrichtensystemen erfüllt. Aber bedingt durch den steigenden Informationsbedarf, werden diese Systeme an Ihre Grenzen stoßen. Daher muss auch hier Zug um Zug der Mehrwert von AI basierten Technologien und Verfahren entwickelt und genutzt werden. Damit wird ein signifikanter Beitrag zur Beschleunigung der entsprechenden Entscheidungsprozesse im militärischen Umfeld geleistet.

Wie AI in Verbindung mit BLOS Breitbandkommunikation als Wegbereiter in der vernetzten Operationsführung genutzt werden kann und welche Technologien, Architekturen und Dienstleistungen daraus für den militärischen Nutzer zukünftig denkbar sind, soll dieser Fachvortrag im Detail vorstellen, erklären und zur weiteren Diskussion stellen.

AIRBUS

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
23	10.05.	16:30 - 16:55	Raum ADDIS ABEBA 3	Detlef Wallenhorst	Geschäftsentwicklung

Digital Mission Agility durch Künstliche Intelligenz, IoT und Edge-Computing

Daten schnell und intelligent nutzen zu können ist einer der wesentlichen Erfolgsfaktoren unserer digitalisierten Zeit – dies gilt nicht zuletzt im Verteidigungssektor. Mit künstlicher Intelligenz, dem Internet der Dinge und dem sogenannten Edge-Computing stehen Mittel zur Verfügung, dies zu verwirklichen, um so die digitale Missions-Agilität zu optimieren und das Fundament für eine Multi Domain Operation zu legen. Die Umsetzung eines solchen Vorhabens ist gleichwohl komplex und von Spannungsfeldern geprägt, die sich in der Regel zwischen Anforderungen nach Sicherheit, Datenschutz und Souveränität auf der einen Seite sowie nach Agilität, Innovation und Kooperation auf der anderen Seite ergeben. Um die Komplexität beherrschbar zu machen und die Spannungsfelder zu managen bedarf es mithin geeigneter Strukturen, Prozesse und Architekturen. Im Rahmen dieses Vortrages wird zunächst aufgezeigt, wie solche Strukturen, Prozesse und Architekturen zu gestalten sind, um dies anschliessend am Beispiel eines Use Cases aus dem Bereich des Internet of Military Things zu konkretisieren.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
24	10.05.	17:00 - 17:25	Raum ADDIS ABEBA 3	Michael Sauer, MBA	Senior Manager Product Sustainment EMEA, CAE GmbH

Einsatzbereitschaft - Gedanken zur Transformation von militärischer Ausbildung und Einsatzvorbereitung

Streitkräfte stehen an einem Wendepunkt. Eine Welt in der sich neue globale Bedrohungen und Herausforderungen entwickeln, zwingt Streitkräfte zur Weiterentwicklung und Anpassung an diese neuen Lagen. Dabei spielt die Zeit die unsere Streitkräfte bis zur vollen Einsatzbereitschaft benötigen eine entscheidende Rolle. Der völkerrechtswidrige Angriffskrieg Russlands auf die Ukraine macht mehr als deutlich, dass wir uns Qualitätseinbußen und Verzögerungen in der Ausbildung und Einsatzvorbereitung unserer Soldaten und Soldatinnen nicht leisten können. Neue Technologien, gepaart mit aktuellen Erkenntnissen aus den Wissenschaften, erlauben uns herkömmliche Konzepte und Lösungen für die Ausbildung und Einsatzvorbereitung zu überdenken und in zeitgemäße Ansätze zu überführen. Diese neuen Ansätze haben das Potential schneller, kostengünstiger und mit höherer Qualität als bisher möglich, Ausbildung, Training und Einsatzvorbereitung zu gewährleisten.

Fortschritte in der künstlichen Intelligenz und im maschinellen Lernen verbessern die Fähigkeit Daten zu nutzen, um wertvolle Informationen und Erkenntnisse über individuelle Leistungen, aber auch die Leistungsfähigkeit von Schulungseinrichtungen und Curricula zu gewinnen. Adaptive Lernansätze, kompetenzbasierte Trainingsrahmen und kontinuierliche Verbesserungsprozesse erhöhen die Kapazität und Leistung von Trainingssystemen in großem Maßstab. Leistungsfähige virtuelle Umgebungen sowie hochauflösende Sichtsysteme (Augmented Reality, Virtual Reality und Mixed Reality) erlauben eine nie dagewesene Immersion der Auszubildenden.

Schließlich ermöglichen moderne Technologien Einsatzausbildung und -vorbereitung mit einer bisher nicht möglichen Realitätsnähe. In der Simulation lässt sich z.B. ein Landes- und Bündnisverteidigungsszenario über alle Domänen, voll integriert und vernetzt abbilden und trainieren, das in seiner Komplexität im realen Luftraum, auf Truppenübungsplätzen oder zur See nicht annähernd vorgefunden werden kann.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
25	10.05.	17:30 - 17:55	Raum ADDIS ABEBA 3	Daniel Kallfass Stefan Nagel	Expert for Operational Analysis & Deputy Head of TEMOA, Senior Expert Mission Ground Systems

Anwendungsfälle für KI in der Multi-Domain Combat Cloud

Die moderne Gefechtsführung steht mit einem digitalen Operationsumfeld vor einem disruptiven Umbruch. Zukünftige militärische Operationen erfordern hohe Flexibilität und Mobilität sowie effiziente entscheidungsunterstützende Services. Dabei wird das zukünftige Gefechtsfeld ergänzt um bemannte und unbemannte Waffensysteme und Sensoren in übergreifender Zusammenarbeit über die Teilstreitkräfte, Organisationsbereiche und Bündnispartner hinweg.

Das Erlangen von Informationsüberlegenheit gegenüber dem Gegner, sowie die Fähigkeit, diese Überlegenheit weitgehend automatisiert zu nutzen und Führungsüberlegenheit zu erlangen, sowie Informationen in einer komplexen Systemumgebung zur richtigen Zeit am richtigen Ort bereitzustellen ist ausschlaggebend für den Erfolg des Gefechts und die Wirkungsüberlegenheit: hier spielt Künstliche Intelligenz die zentrale Rolle.

Dazu bedarf es einer Ende-zu-Ende gesicherten Kommunikationsinfrastruktur, begleitet von Multi-Layer Cyber Security Maßnahmen, der Fähigkeit Massendaten zeit- und inhaltsgenau auszuwerten sowie Informationen den vielfältigen angeschlossenen Waffensystemen. Hier wird künstliche Intelligenz eine wesentliche Rolle spielen, insbesondere auf der letzten Meile, punktgenau bereitzustellen und mit Hilfe von künstlicher Intelligenz die Soldaten in ihrer Tätigkeit zu unterstützen als auch in der Cloud, in der die fusionierte Lageinformation durch eine KI ausgewertet und den militärischen Führer in der Lageauswertung und Operationsplanung unterstützen kann.

Mit der Multi-Domain Combat Cloud ermöglicht Airbus die Integration und Kombination von Zukunftsanwendungen und Bestandssystemen zu einem zukunftsfähigen Systemverbund mit einem gemeinsamen Informationsraum. Die Verwendung von standardisierten offenen Schnittstellen ermöglicht dabei die Integration Hersteller-unabhängiger Services und Einzellösungen. Die Airbus Multi-Domain Combat Cloud unterstützt in allen Phasen des Führungsprozesses und ermöglicht so schnellere Entscheidungszyklen und wird dadurch die Effizienz in Operationen deutlich verbessern. Um dieses zu ermöglichen bietet Airbus einen cloud- und servicebasierten Informationsraum (Shared Information Space) für alle beteiligten Systeme und und Anwendungen in den Dimensionen Cyber- und Informationsraum, Land, Luft, See und Weltraum.

AIRBUS

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
26	11.05.	09:15 - 09:40	Saal NAIROBI	Horst Kuchelmeister	Major Account Manager

Kritische Infrastrukturen mit NIST Cybersicherheits Framework (CFS) schützen

Die nationale und wirtschaftliche Sicherheit eines Landes hängt zunehmend von cyber abhängigen, kritischen Infrastrukturen ab. Im Jahr 2013 gab der Präsident des amerikanischen National Institute of Standards and Technology (NIST) die Anweisung, ein Cybersicherheit Framework (CSF) zu entwickeln. Seit der Veröffentlichung von CSF v1.0 im Februar 2014 haben Organisationen weltweit das Framework implementiert, es dient dabei Cyber-Risiken besser zu verstehen und zu bewältigen. Damit man mit den stetig wachsenden Bedrohungen auf dem Laufenden bleibt, wurde im April 2018 das CSF weiterentwickelt. Das Update auf CSF 1.1 bietet zusätzliche Anleitungen zur Authentifizierung, Identität, Selbsteinschätzung des Cyber-Sicherheitsrisikos und Umgang mit der Offenlegung von Schwachstellen. Das CSF definiert 5 wichtige Gruppen, 1. Identifizieren, 2. Schützen, 3. Erkennen, 4. Reagieren und 5. Wiederherstellen. "Identifizieren" beschäftigt sich mit Themen wie, was muss geschützt werden, wie hoch ist das Risiko, gesetzliche Vorgaben etc. Themen wie Access Control, Security Awareness Training, Datensicherheit werden in "Schützen" definiert. Die 3. Gruppe "Erkennen" beschäftigt sich mit Sicherheitsmonitoring, Prozesse zum Erkennen von Bedrohungen und Anomalien. Um Anomalien zu erkennen, wird hauptsächlich künstliche Intelligenz (KI) und maschinelles Lernen (ML) eingesetzt. Im Bereich "Reagieren" wird definiert, wie auf Bedrohungen reagiert wird, wie Angriffe schnell eingedämmt werden und wie kommuniziert wird. Die letzte Gruppe "Wiederherstellung" befasst sich damit, wie Systeme, Daten etc. nach einem Angriff wiederhergestellt werden. Ein maximaler Schutz kritischer Infrastrukturen ist nur dann zu erreichen, wenn alle 5 Gruppen vom CSF sauber definiert und implementiert sind.

paloalto® NETWORKS

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
27	11.05.	11:15 - 11:40	Saal NAIROBI	Robert Schwerdtner	Leiter Solution Design

Künstliche Intelligenz: der Gamechanger in der OSINT/OSINF-Lagebewertung?

Nicht erst seit Beginn des Ukrainekrieges besteht auch im militärischen Kontext der gesteigerte Bedarf, Meta- und Contentinformationen aus gängigen Social Media Kanälen zu erheben und die visuellen Inhalte der Streams analysier- und teilinterpretierbar zu machen. Doch wie lässt sich KI-basierte Objekterkennung in Verbindung mit OSINF/OSINT-Monitoring einsetzen? Und wie kann diese Kombination einen echten Mehrwert für die Lagebewertung darstellen? Wir skizzieren das optimale Zusammenspiel geeigneter Tools bis hin zur Weiterverwendung der Lageinformationen in angeschlossenen Intelligence-Applikationen. Darüber hinaus gehen wir auf die Wichtigkeit eines offenen und transparenten Datenhandlings ein, das mit der Bereitstellung von Lageinformationen in Form eines Datenlayers zur Verwendung in einer Geodateninfrastruktur einhergeht.

rola.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
28	11.05.	11:45 - 12:10	Saal NAI-ROBI	Marcel Tritschler Markus Otterbein	Junior Consultant Consulant IT-Strategie-management

Prozessdigitalisierung – Wie können Sie sich dem Thema nähern?

Das Thema „Digitale Prozesse" oder synonym „Prozessdigitalisierung" ist mehr als ein Modewort und vor allem ist es eins nicht: ein Projekt. Die Umstellung auf „digital" ist ein fortwährender Prozess, der niemals endet.

Gerade wer erst anfängt sich mit diesem Thema auseinander zu setzen und somit im digitalen Reifegrad ganz am Anfang steht, hat Unmengen an Fragen und sieht den berühmten Wald vor lauter Bäumen nicht. Damit in Konsequenz keine Schockstarre eintritt, werden mit dem Vortrag praxisbezogene, gut umsetzbare Ansatzpunkte und Lösungsvorschläge gegeben, damit die ersten Schritte in die Prozess-digitalisierung leichtfallen.

Dabei wollen wir Ihnen Einblicke in unsere Praxiserfahrung geben, damit der Einstieg in das Thema „Prozessdigitalisierung" gelingt.

Anschließend freuen wir uns auf Ihre Fragen und gehen gerne vertiefend auf einzelne Aspekte ein.

CONET

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
29	11.05.	12:15 - 12:40	Saal NAIROBI	Dr. Dirk Fischer	Director Public Sector Business DACH, Pexip

Militärische Kommunikation: Umsetzung von Zero Trust in Audio- und Videokonferenzen durch KI

Die Bedrohung durch Cyberangriffe hat sich laut BSI durch die jüngsten Kriegsereignisse weiter verschärft. In diesem Zusammenhang stellt das Militär im transatlantischen Bündnis ein zunehmendes Hochwertziel für Akteure im Cyber- und Informationsraum (CIR) dar. Um diesen adäquat zu begegnen, müssen Organisationen für Sicherheit und Verteidigung ihre Kommunikations- und Informationstechnologie entsprechend schützen.

Ein zentraler Bereich der militärischen Kommunikationstechnik sind hierbei Audio- und Videokonferenzen.

Erfahren Sie im Vortrag, wie softwaredefinierte Meeting-Sicherheit die Prinzipien von Zero Trust und künstlicher Intelligenz nutzen kann, um autorisierte Teilnehmer zu identifizieren und damit die operative Sicherheit bei missionskritischer Kommunikation in Echtzeit signifikant erhöhen kann:

Eine Confidence Engine mit Designer wird dabei mit Anwendungs- und Policy-Stacks integriert, um vordefinierte Akzeptanz-Baselines (=IST-Daten) zu erfassen und mit Autorisierungsprofilen (= SOLL-Daten) abzugleichen, unter Berücksichtigung von biometrischen Daten, Verhaltensdaten, sowie gerätebezogenen Daten.

Bei festgestellten Anomalien im Meeting oder Bedarf weiterer Klassifizierung des Gesprächs, werden die operativen Risikoprofile automatisch angepasst und alle nicht berechtigten oder nicht vertrauenswürdigen Teilnehmer automatisch ausgeschlossen. Mit zunehmender Meetingzahl wird die Confidence Engine trainiert, das heißt die Kernvariablen zur Identifizierung autorisierter Teilnehmer werden gehärtet (agile Cybersicherheit).

Dr. Dirk Fischer, Director Public Sector Business DACH von Pexip, Experte für Videokommunikation und ehemaliger Dozent der Bundeswehr-Univiersität München führt Sie durch einen praxisnahen und gleichzeitig inspirierenden Vortrag über das Konzept und die Anwendung softwaredefinierter Meeting-Sicherheit von Pexip. trainiert, das heißt die Kernvariablen zur Identifizierung autorisierter Teilnehmer werden gehärtet (agile Cybersicherheit).

Dr. Dirk Fischer, Director Public Sector Business DACH von Pexip, Experte für Videokommunikation und ehemaliger Dozent der Bundeswehr-Univiersität München führt Sie durch einen praxisnahen und gleichzeitig inspirierenden Vortrag über das Konzept und die Anwendung softwaredefinierter Meeting-Sicherheit von Pexip.

] pexip [

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
30	11.05.	12:45 -13:10	Raum NAIROBI	Kethireddy Kameswara Reddy	EU Business Development Manager

Automated synthetic infrared image generation for AI applications

AI-powered systems have demonstrated state-of-the-art target recognition performance, however, they require large training sets of images to ensure decent accuracy.

In the case of electro-optical infrared (EO/IR) remote sensing, acquiring sufficient measured imagery can be difficult, in particular for confidential and high-value targets. Highly accurate EO/IR scene simulation is a great alternative to the testing which is expensive and, in most cases, impossible & confidential. In this presentation, we are proposing an automated process to generate such highly accurate IR images through our physics-based simulation software, MuSES, and Process flow Software, Cotherm. The MuSES inputs include environmental factors, global location, date and time, vehicle engine state, target perspective, sensor resolution, waveband, etc. The output of this process is a MuSES-generated EO/IR sensor radiance image dataset with the necessary variety to be suitable for algorithm development and training. This process enables users to build imagery of any target under any condition.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
31	11.05.	13:15 - 13:40	Saal NAIROBI	Dr. Roozbeh Faroughi	Manager Agile & Innovation OPITZ CONSULTING

Schachmatt in 3 Zügen – mit Flexibilität, Schnelligkeit und Innovation zum Gewinner werden: Drei Beispiele aus dem öffentlichen Sektor

Anhand von drei unterschiedlichen Beispielen aus dem öffentlichen Sektor zeigen wir Ihnen in diesem Best-Practice-Dialog, wie die Erfolgsfaktoren Flexibilität, Schnelligkeit und Innovation jeweils in einem einzelnen Projekt zum Erfolg geführt haben und wie sie als gemeinsamer Lösungsansatz noch mehr Wirkung in der digitalen Transformation entfalten können. Erschwerte Bedingungen durch hohen Modernisierungsdruck und gleichzeitig noch Innovationserwartungen: Unser Moderator begleitet Sie durch diese drei konkreten Ausgangslagen und diskutiert mit Experten aus den Projekten die jeweils verfolgten Lösungsansätze

OPITZ CONSULTING

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
32	11.05.	09:15 - 09:40	Raum ADDIS ABEBA 3	Oberst i.G. Klaus Glaab OTL Lars Kostka Michael Morton	Referatsleiter BMVg und Hauptprozessverantwortlicher (HPV) Digitale Verwaltungsarbeit Referent des HPV Engagement Manager DokMBw bei CGI

In „agiler Symbiose“ zum Digitalen Schreibtisch im Geschäftsbereich BMVg

Moderne agile IT-Anwendungen gestalten das Verwaltungshandeln einer Digitalen Bundeswehr (Von DokMBw, über Groupware Bw, zum „Digitalen Schreibtisch“)

Die ersten 35.000 Bundeswehrangehörigen nutzen seit dem 5. Oktober 2021 verpflichtend unser DokMBw 1. Ausbaustufe (1.AS) für ihre Verwaltungsarbeit und die elektronische Veraktung. Damit kommt die Bundeswehr und das BMVg nicht nur den gesetzlichen Forderungen des E-Governmentgesetzes nach, sondern haben einen ersten wesentlichen Beitrag für die Digitalisierung der Verwaltungsarbeit in ihrem Ressort gelegt. Parallel zur formalen Verwaltungsarbeit führt die Bundeswehr bis zum Jahresende 2024 die neue moderne IT-Plattform Groupware Bw mit diversen kollaborativen Tools für die Mailkommunikation, Chat-Funktionalitäten sowie Online-Videokonferenzen für 190.000 Nutzende ein. Diese IT-Plattform bildet die Grundlage für alle neuen IT-Lösungen im Bereich der Verwaltung – und damit auch für die neue 2. Ausbaustufe (2.AS) von DokMBw. Doch digitale Verwaltung bedeutet mehr als die Einführung einer Software: Sie ist vor allem auch eine (ablauf-)organisatorische Veränderung. Das BMVg hat daher zeitgleich den neuen Hauptprozess „Digitale Verwaltungsarbeit“ (HP DiV) etabliert, der die Verwaltungsabläufe analysiert, optimiert und für die digitale Zukunft modelliert. Auf dieser Grundlage basieren alle nötigen Veränderungen im gesamten IT-System als auch Änderungen von Vorschriften und Regelungen für den Geschäftsbereich. Dank „agiler Symbiose“ mit dem Kunden entwickeln wir in enger Zusammenarbeit mit dem neuen HP DiV die neue 2. AS von DokMBw in Scrum-Schritten und mit allen Funktionalitäten für die zukünftige digitale Verwaltungsarbeit in der Bundeswehr. Auch wird der neue „Digitale Schreibtisch“ als zentrales (web-basiertes) Übersichts- und Management-Tool aller Groupware Bw- IT-Anwendungen (einschl. DokMBw 2. AS) vollumfänglich unterstützt / eingebunden.

Erfahren Sie mehr: Gemeinsam mit dem BMVg informieren wir über gewonnene Erkenntnisse wie auch über das Potenzial von agiler Softwareentwicklung und geben einen Ausblick auf DokMBw 2. AS und den „Digitalen Schreibtisch“.

CGI

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
33	11.05.	11:15 - 11:40	Raum ADDIS ABEBA 3	Dr. Irene Cramer Christoph Reich	Business development - Integration & APIs Director Defence & Aviation

API-Portale sind Innovationstreiber – nicht nur im Silicon Valley

Innovation braucht Kaffeehaus-Kultur (übrigens nicht nur in der NATO-Pause), beschreibt es Steven Johnson in seinem berühmten TED-Talk „Wo gute Ideen herkommen". Während Kaffeehäuser den Austausch und die Weiterentwicklung von Gedanken aller Art fördern, fördern API-Portale den Austausch, die Weiterentwicklung und -verwendung von Daten bzw. Funktionen und somit Software-Innovation. API-Portale implementieren, im übertragenen Sinn, einige der innovationsfördernden Aspekte von Kaffeehäusern auf technischer Ebene. Was heißt das nun konkret?

Um mit einem Smartphone eine Zugverbindung zu buchen, nutzen wir eine Applikation. Auch Applikationen nutzen (andere) Applikationen, Ihre Smartphone-App weiß nämlich selbst nicht, welche Verbindungen Ihnen zur Verfügung stehen, sondern muss diese Information wiederum bei einer anderen Applikation anfragen. APIs (Application Programming Interfaces) sind Schnittstellen, die für die Zusammenarbeit von zwei oder mehr Applikationen gedacht sind; also genau die Zusammenarbeit, die Ihre Smartphone App mit anderen Apps im angegebenen Beispiel durchführen muss.

Ein API-Portal wiederum ist eine Art Online-Marktplatz, auf dem Software-Entwickler APIs (d.h. wiederverwendbare Daten & Funktionen) finden und buchen können, die von anderen Entwicklern bzw. Organisationen angeboten werden. API-Portale dokumentieren zudem, wie und wofür die verfügbaren APIs verwendet werden. Dadurch können Entwickler einfach auf Vorhandenes aufsetzen und entsprechend schneller neue Software entwerfen, bauen und testen.

In diesem Vortrag erklären wir anhand einfacher Beispiele die Grundgedanken von APIs und API-Portalen und warum sie in diesem Kontext besonders innovationsfördernd wirken können.

Wir freuen uns Sie an unserem Stand S 20 im Saal New York/ Genf persönlich zu treffen!

software AG

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
34	11.05.	11:45 - 12:10	Raum ADDIS ABEBA 3	Dr. Patrick Grames	Rohde & Schwarz Vertriebs GmbH

ESSOR – von der Idee der europäischen Interoperabilität in die Umsetzung

Sich verstehen und aktiv untereinander austauschen – dieser Idealzustand ist in militärischen Operationen im Bündnis bis heute nicht erreicht. Unter dem Dach von ESSOR (European Secure Software Defined Radio) und dem Management der OCCAR haben sich Spanien, Italien, Frankreich, Finnland, Polen und seit 2020 auch Deutschland vorgenommen, dieses Ziel zu erreichen. Auf jeweils nationalen vertrauenswürdigen Funkgerätefamilien der jeweiligen nationalen Champions, die nach dem Software Defined Radio-Prinzip funktionieren, wird eine gemeinsame Wellenformfamilie entstehen, die parallel zur nationalen Führung erstmals wahre europäische Interoperabilität ermöglicht.

Neben einer Führung durch die Entstehungsgeschichte und der Vorstellung des zum heutigen Stand Erreichten mit der Wellenform OC1 wird ein Ausblick auf die weiteren Wellenformen im Rahmen des European Defense Investment Program (EDIDP) gegeben und die Brücke zu den großen Zukunftsprogrammen für Deutschland geschlagen: D-LBO, FCAS (Future Combat Air System) und MGCS (Main Ground Combat System).

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
35	11.05.	12:15 - 12:40	Raum ADDIS ABEBA 3	Carsten Dieterle	Principle Account Technical Leader - Defense

IT Automation bis in den Einsatz

In seinem Vortrag stellt Carsten Dieterle, technischer Experte bei der IBM für die Bundeswehr, eine durchgehende und domänenübergreifende Automationsstrategie für IT-Systeme bis in den Einsatz vor. Mit dieser wird die Bundeswehr zukünftig in der Lage sein, nicht nur die BWI IT-Systeme, sondern auch die bei militärischen IT-Programmen und -Projekten, wie z.B. German Mission Network oder D-LBO, ausgebrachten IT-Equipments und IT-Services voll automatisiert zu führen. Weitere Vorteile der Strategie sind: • eine einheitliche, domänenübergreifende und durchgängige Steuerung und Management • Betriebsbereitschaft auf Knopfdruck • die Möglichkeit bedarfsgerecht zu skalieren und für mobile Anteile schnell und kontrolliert bereitzustellen (DC, Fog und Edge) Die Lösung besteht aus Steuerungs-, Überwachungs-, Rollout-, und Deploymentanteilen die mit entsprechenden KI-Funktionalitäten ausgestattet sind.

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
36	11.05.	12:45 - 13:10	Raum ADDIS ABEBA 3	Ivan Bütler	Gründer und Geschäftsführer

Cyber Range - Attack & Defense Training

Eine Cyber Range ist eine virtuelle Umgebung, die es ermöglicht, sicherheitstechnische Szenarien zu simulieren und zu trainieren. Sie wird häufig verwendet, um Mitarbeitende im Umgang mit Bedrohungen und Sicherheitsvorfällen zu schulen und ihre Fähigkeiten zu verbessern. Cyber Ranges können verschiedene Formen haben, von einfachen simulativen Umgebungen bis hin zu realitätsnahen Szenarien mit täuschend echt wirkenden Netzwerken und Systemen. Sie werden häufig von Regierungsbehörden, Unternehmen und Bildungseinrichtungen genutzt, um ihre Cybersecurity-Fähigkeiten zu verbessern und ihre Mitarbeitenden auf mögliche Bedrohungen vorzubereiten. In einer Cyber Range können die Teilnehmenden in verschiedenen Rollen agieren, z.B. als Angreifer/in oder Verteidiger/in. Sie haben die Möglichkeit, verschiedene Technologien und Werkzeuge zu nutzen, um sich mit Sicherheitsbedrohungen auseinanderzusetzen und zu lernen, wie man sie bekämpft. Die Simulationen in einer Cyber Range können auch dazu genutzt werden, um neue Sicherheitsmaßnahmen und -verfahren zu testen und zu verbessern. Dieser Talk stellt die Cyber Range von Hacking-Lab AG vor.

HACKING-LAB

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
37	11.05.	13:15 - 13:40	Raum ADDIS ABEBA 3	Laszlo Poór	Advisory Systems Engineer

„Hilfe, wir wurden gehackt! Vor- und Nachsorge mit Dell Technologies“

Die Anzahl der Cyberangriffe auf Unternehmen, egal welcher Branche und Größe, steigt stetig.

Die Art und Weise, wie Unternehmen angegriffen werden, ist sehr vielseitig. Meist wird nur ein Ziel verfolgt: Unternehmensdaten zu verschlüsseln, den Geschäftsbetrieb lahm zu legen und den Geschädigten zu zwingen, Geld gegen die Herausgabe des Decodierungs-Schlüssels zu bezahlen.

Ein Angriff dauert oft nur wenige Minuten und findet oft nachts statt. Das Resultat ist im schlimmsten Fall die **Verschlüsselung aller Daten** im Unternehmen, vom Applikationsserver, über den Storage bis hin zum Backup. In einem etwaigen Ausweich-Rechenzentrum sind die Daten ebenso korrumpiert. Ein Zurückspielen der Backupdaten, der Snapshots oder der gespiegelten Daten ist nicht mehr möglich. Der Geschäftsbetrieb steht. Um dennoch wieder schnellstmöglich den Geschäftsbetrieb aufnehmen zu können, müssen „saubere“ (nicht korrumpierte) Daten vorhanden sein. Diese können in die Produktivumgebung zurückgespielt werden.

Die **Dell PowerProtect Cyber Recovery (CR)** ist in der Lage, Daten zu isolieren und im Falle eines erfolgten Cyber Angriffs, „saubere“ Daten zur Verfügung zu stellen. Mit PowerProtect Cyber Recovery können Unternehmen ihren Geschäftsbetrieb nach einem Cyberangriff schneller wiederaufnehmen.

Die CR Lösung ist wie jede IT-Security Lösung nicht nur ein Stück Hard- oder Software, sondern besteht additiv aus Prozessen und Workflows.

- Voraussetzung für die Implementierung einer CR Lösung ist das Vorhandensein einer Data Domain (PowerProtect DD Appliance), welche die produktiven Backupdaten speichert.
- Im Cyber Vault Bereich kommt ebenfalls eine Data Domain zum Einsatz, der sogenannte Vault Storage. Der Vault Storage dient als Replikationsziel ausgewählter kritischer Daten.
- Das **Air Gap isoliert** das Cyber Vault komplett. Der Cyber Vault ist weder über das Internet noch über das Unternehmensnetzwerk erreichbar.
- Mit der Analyse Software **CyberSense** (optional erhältlich) werden die Golden Copies in der Landing Zone auf ihre Integrität überprüft. Die isolierten Daten im sicheren Cyber Vault-Bereich werden mit CyberSense-Analysen und Machine Learning überwacht und deren Datenintegrität überprüft. CyberSense überprüft die Integrität der Daten, so dass im Falle eines Cyberangriffs nur saubere Daten sicher im Cyber Vault gespeichert werden.

DELL Technologies

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
38	11.05.	15:00 - 15:25	Raum ADDIS ABEBA 3	Dr. rer. nat. Helen Ditz Sven Lüttich (PLATH Group)	Data Scientist Business Case Manager - Innovations

Künstliche Intelligenz im Bereich der Intelligence Domain

Das Konzept der ganzheitlichen Vernetzung von Teilsystemen und der Einsatz von künstlicher Intelligenz (KI) in Bereich der Intelligence Domain gewinnt im heutigen Informationszeitalter rasch an Bedeutung. Angesichts der zunehmenden Menge, Vielfalt und Geschwindigkeit der Daten besteht ein wachsender Bedarf, die Effizienz und Effektivität der Erfassung, Verarbeitung und Analyse von Informationen zu verbessern. In diesem Beitrag werden die potenziellen Vorteile der ganzheitlichen Vernetzung dieser Systeme und der Einsatz von KI im Intelligence Cycle untersucht, wobei beispielhaft auf die Datenfusion und -analyse eingegangen wird.

Ganzheitliche Vernetzung bedeutet die Integration verschiedener Subsysteme wie Sensoren, Kommunikationsgeräte und Verarbeitungseinheiten in ein einheitliches Netzwerk, das Daten in Echtzeit erfassen und verarbeiten kann. Mit Hilfe dieses Netzwerks können Informationen aus verschiedenen Quellen wie COMINT, ELINT, CNM, Satellitenbildern, sozialen Medien und anderen OSINT Quellen gesammelt werden, um ein umfassendes Bild der Lage zu erhalten.

KI kann die Datenfusion und -analyse unterstützen, indem sie den Prozess der Erkennung von Mustern und Anomalien in großen Datensätzen automatisiert. Algorithmen für maschinelles Lernen können so trainiert werden, dass sie verschiedene Datentypen wie Bilder, Text und Audio erkennen und klassifizieren und daraus relevante Informationen extrahieren und fusionieren. Dies kann dazu beitragen, die Arbeitsbelastung menschlicher Analysten zu verringern und den Prozess der Informationsgewinnung zu beschleunigen.

Neben der Datenfusion und -analyse kann KI auch in anderen Bereichen des Aufklärungszyklus helfen, etwa bei der Identifizierung von bedeutenden Signalen, der Bewertung von Bedrohungen und der Entscheidungsfindung. So kann KI beispielsweise zur Analyse von Sprache oder Bildern genutzt werden.

Dabei muss jedoch das Bewusstsein geschaffen werden, dass KI mit Bedacht in diesem wichtigen Bereich eingesetzt werden muss, da es auch diverse Herausforderungen mit sich bringen kann und dass somit der Einsatz mit Einschränkungen und Risiken verbunden ist. So können KI-Algorithmen beispielsweise anfällig für Verzerrungen, Fehler und gegnerische Angriffe sein, rechtliche und ethischen Bedenken sind ebenfalls relevant. Insbesondere wenn Entscheidungskompetenzen in der Prozesskette (Sensor to Shooter) abgetreten werden würden.

Zusammenfassend lässt sich sagen, dass sich der Einsatz eines Intelligence Netzwerkes und künstlicher Intelligenz im Intelligence Bereich das Potenzial hat, die Geschwindigkeit, Genauigkeit und Wirksamkeit der Sammlung, Verarbeitung und Analyse von Informationen zu verbessern. Es ist jedoch wichtig, einen vorsichtigen und verantwortungsvollen Ansatz für den Einsatz von KI zu wählen und sicherzustellen, dass menschliches Urteilsvermögen und Fachwissen im Mittelpunkt aller Prozesses bleiben.

PLATH Group

Nr.	Tag	Zeit	Ort	Vortragender	Funktion
39	11.05.	15:30 - 15:55	Saal NAIROBI	Alexander Golding	Senior Sales Manager

„Drohnen - mehr als fliegende Kameras“

Drohnen sind mehr als nur fliegende Kameras. Sie haben viele Anwendungsbereiche und können mit einer Vielzahl von Sensoren und Geräten ausgestattet werden, um eine breite Palette von Aufgaben zu erledigen.

Unbemannte Luftfahrzeuge (UAV) sind ein hochflexibles Mittel zur Abdeckung großer Gebiete. Heutige UAVs sind in der Regel mit hochleistungsfähigen optischen Systemen ausgestattet, die es den Betreibern ermöglichen, den Überblick zu behalten und sich auf bestimmte Orte von Interesse zu konzentrieren.

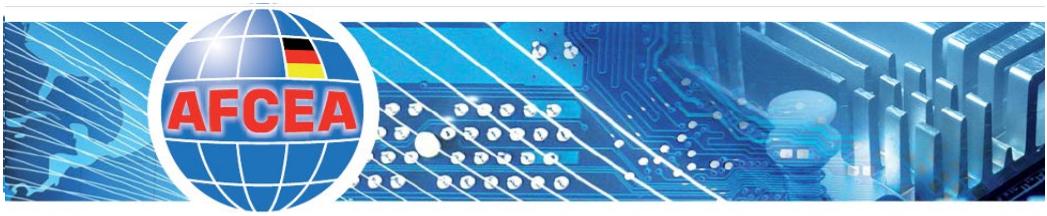
Die Lokalisierung von spezifischen Zielen oder die Identifizierung von Signals of Interest (SOI) im Einsatzgebiet ist oft mit der Notwendigkeit verbunden, Bodentruppen in der Nähe des Ziels einzusetzen. Dies führt zu einem höheren Risiko, entdeckt zu werden und weniger Flexibilität und Mobilität.

Zur effizienten Erkennung von Signalen von Interesse sind verschiedene Sensoren, die auf bestimmte Signale (z.B. GSM, Funk oder SatCom) für die so genannte Communication Intelligence (COMINT) für verschiedene Dienste. Damit ist es möglich, die Bodeneinsatzkräfte mit einem Situationsüberblick zu unterstützen und übergeordnete Stellen in die Lage zu versetzen, die Bewegungen der verschiedenen Einheiten zu koordinieren. Bislang wurden solche Sensoren selten in UAVs integriert. Dieser Vortrag dient als Ausblick auf mögliche technische Lösungen einschließlich der Anwendungsfälle, um den Nutzen der Kombination die Vorteile von UAVs mit COMINT-Sensoren zu kombinieren.

Industrievorträge

Ihre Notizen zu den Industrievorträgen:

Jahresprogramm 2023



AFCEA Bonn e.V.

Studien PREIS 2023

Das Bonner Chapter des internationalen Anwenderforums für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) verleiht jährlich einen **Studienpreis**, der mit insgesamt **20.000 €** dotiert ist. Der Verein fördert damit junge Wissenschaftler/innen, die hervorragende **Masterarbeiten** oder **Magisterarbeiten** auf den Gebieten

- **Angewandte Informatik**
- **Nachrichtentechnik**
- **Automatisierungstechnik**

erstellt haben. Auch **Bachelorarbeiten** sind zugelassen, jedoch werden an alle Arbeiten dieselben Maßstäbe angelegt.

Professoren/innen 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 dazu ihre besten Absolventen/innen 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-2023**.
Die Preisverleihung findet am **14-September-2023** 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

Industrievorträge 2023

AFCEA Fachausstellung 2023

10./11. Mai 2023