Hardthöhen-KURIER
DAS MAGAZIN FÜR SOLDATEN UND WEHRTECHNIK

FÜR EIN STARKES EUROPA

HHK www.hardthoehenkurier.de AFCEA 2025

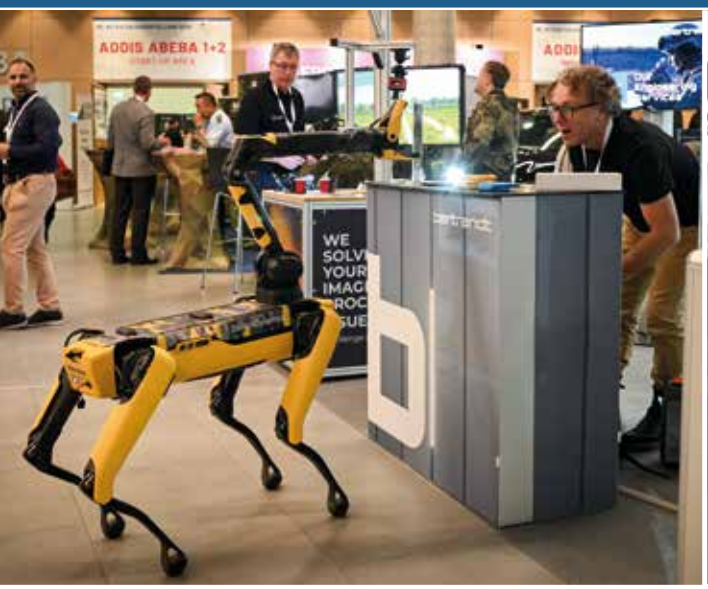
SONDERPUBLIKATION
zur AFCEA Fachausstellung 2025

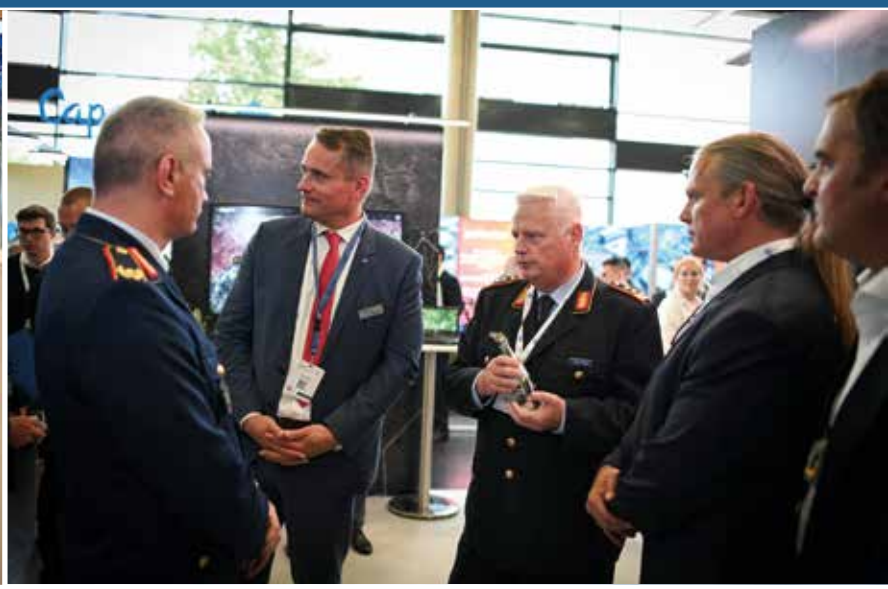
AFCEA Bonn e.V.

38. AFCEA Fachausstellung – 27./28. Mai 2025

AFCEA Bonn e.V.

Was war los auf der AFCEA Fachausstellung?





©MRV/Socrates Tassos (6)

AFCEA Bonn als Enabler und Networking-Instrument

Wir können Digitalisierung! Dies unterstreicht Generalmajor Armin Fleischmann, Vorsitzender AFCEA Bonn e.V. sowie Abteilungsleiter Planung CIR und Digitalisierung der Bundeswehr im Kommando Cyber- und Informationsraum der Bundeswehr, im Interview nach der 38. AFCEA Fachausstellung.

Sehr geehrter Herr General, die AFCEA Fachausstellung 2025 ist beendet. Wie lautet Ihr Fazit?
Es war unsere bisher größte Veranstaltung. Wir hatten so viele Teilnehmerinnen und Teilnehmer wie noch nie. Schon am ersten Tag waren es rund 4.800, so viel wie sonst an beiden Tagen. Und noch einmal rund 3.000 am zweiten Tag. Das hat man auch an den Einlasskontrollen gemerkt, die wir ja durchführen mussten. Die werden wir nächstes Jahr mit Sicherheit noch mal deutlich optimieren.
Das Echo war überwältigend, sowohl von den Ausstellern als auch den Besuchern. Durch die Bank eine positive Resonanz, ein tolles Feedback. Vor allem wird unsere Bandbreite geschätzt. Denn wir haben ja wirklich von Großunternehmen bis zu Start-ups, von kleinen Innovatoren bis zu den ganzen Behörden alle mit dabei. Das gibt es nirgendwo anders. Ich habe viele Leute gesprochen, die mir gesagt haben, ihre Füße tun ihnen schon weh. So vieles haben sie sich angeschaut. Das sagt alles!

Zur AFCEA Bonn e.V.: Wie ist der Verein in eine internationale Organisationsstruktur eingebunden?
AFCEA Bonn e. V. ist und war schon immer ein gemeinnütziger Verein nach deutschem Recht. Wir gehören allerdings zu einer internationalen Community, der AFCEA International, mit Sitz in Fairfax. Das ist westlich von Washington, D.C. – dort war ich kürzlich zu einem Besuch. Die komplette AFCEA-Community ist in drei Regionen aufgeteilt: in die Vereinigten Staaten von Amerika, Europa und den südostpazifischen Raum.
Europa ist der zweitgrößte Bereich nach den USA. Wir sind in sogenannten Chaptern organisiert, wobei AFCEA Bonn e. V. eins von fünf Chaptern in der Bundesrepublik Deutschland ist. Es gibt hier drei amerikanische und zwei deutsche, letztere in Bonn und München. Bonn ist mit Abstand das größte Chapter in Europa. Wir haben fast so viele Mitglieder und Firmen, die zu uns gehören und die wir als Teil in diese Community einbringen, wie der Rest in Europa zusammen. Darum können wir auch solche Fachausstellungen durchführen.
Wir sind, wie gesagt, ein Verein nach deutschem Recht und betreuen natürlich im Kern den Köln-Bonn-Koblenzer-Raum. Das machen wir seit vielen Jahren sehr erfolgreich. Wir sind auch in Berlin tätig. Allerdings haben wir als gemeinnütziger Verein nicht die Mittel, um auch in der Hauptstadt ein Büro aufzubauen. Das liegt auch ein bisschen an der Historie.

©MRV/Socrates Tassos

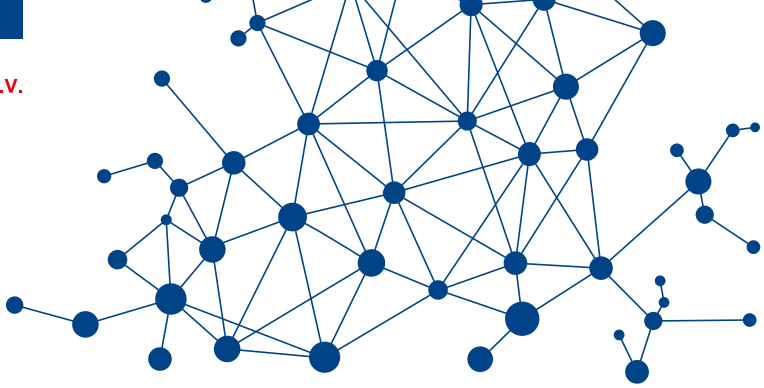
Auf dem Stand des Mittler Report Verlages stellte sich der Vorsitzende von AFCEA Bonn, Generalmajor Armin Fleischmann, den Fragen von Burghard Lindhorst.

Inwieweit können Sie jetzt schon einen Ausblick auf das kommende Jahr geben?
Wir werden die 39. Fachausstellung auch wieder hier im World Congress Center und im Plenarsaal durchführen. Da freuen wir uns schon sehr drauf. Jetzt haben wir erstmal ein bisschen Pause und nutzen die Zeit für die Nachbereitung der diesjährigen Veranstaltung. Wir müssen schauen, wie wir den kompletten Bereich ein bisschen konsolidieren und uns weiterentwickeln. Leider mussten wir vielen Firmen absagen. Aufgrund der Mengen- und Größenbeschränkung konnten wir nicht mehr zulassen. Da müssen wir uns etwas einfallen lassen, wie wir das am besten covern. Wir hatten die Außenfläche schon ein bisschen vergrößert, aber irgendwo sind uns flächenmäßig Grenzen gesetzt.
Wir werden natürlich das Thema Nationale Souveränität und Digitalisierung in Deutschland für Deutschland vorantreiben. Künstliche Intelligenz wird eine massive Rolle in den nächsten Jahren spielen, das ist ein Gamechanger. Das müssen wir auch supporten. Digitalisierung in Deutschland nimmt wieder Fahrt auf. Das unterstützen wir. Deutschland muss wieder dahin kommen, wo es schon mal war. Wir können das in Deutschland. Wir müssen uns nur wieder trauen und müssen uns motivieren. Der AFCEA Bonn e. V. ist so ein bisschen der Enabler und das Networking-Instrument, um alle wieder zusammenzubringen, um dies wieder realisieren zu können.

Sehr geehrter Herr General Fleischmann, vielen Dank für die interessanten Informationen und weiterhin viel Erfolg für Ihre wichtige Arbeit!

2. HALBJAHR 2025
TERMINÜBERSICHT

AFCEA Bonn e.V.



AFCEA VERANSTALTUNGEN:

WISSEN AUS ERSTER HAND

TERMIN	VERANSTALTUNG	ORT
III. Quartal 2025 *Tagesveranstaltung*	***Fachveranstaltung mit CIH*** *„Demonstratoren im Bereich KI“*	*Berlin*
01.10.2025 *Tagesveranstaltung*	***Fachveranstaltung mit Zentrum Digitalisierung der Bundeswehr***	*Bonn*
01./02.10.2025	***TECHNET Europe***	*Rom/Italien (AFCEA Europe)*
06.10.2025 *Tagesveranstaltung*	***Fachveranstaltung mit BITKOM und GovTech Campus***	*Berlin*
07.10.2025 *Tagesveranstaltung*	***Partnerevent mit BDSV*** *7. Konvent zur Digitalen Konvergenz*	*Berlin*
06.11.2025 *Tagesveranstaltung*	***Zukunfts- und Technologieforum***	*FKIE, Wachtberg*
25.11.2025 *Tagesveranstaltung*	***Mittagsforum mit Firma Software AG***	*Wissenschaftszentrum Bonn*
3./4.12.2025	***TECHNET Transatlantik***	*Frankfurt (AFCEA Europe)*
08.12.2025 *Abendveranstaltung*	***BOnnF1R3***	*Bonn*

Die Anmeldemöglichkeiten werden in der Regel circa sechs Wochen vor Beginn freigeschaltet.

AFCEA Bonn e.V.

Die führende Austauschplattform für den Dialog von Bundeswehr, Sicherheitsbehörden, Verwaltung, Wissenschaft und Industrie

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

Zum AFCEA-Jahresprogramm mit Anmeldung:

Heimat von Hightech und Ringen um Resilienz

Die 38. AFCEA Fachausstellung vom 27. und 28. Mai im World Conference Center Bonn

Von Jochen Reinhardt, Vorstand Presse- und Öffentlichkeitsarbeit AFCEA Bonn e. V.

Rund 280 Unternehmen und Organisationen stellten bei einer der wichtigsten deutschen IT-Messen für Verteidigung und Sicherheit aus. Zur 38. AFCEA Fachausstellung ins World Conference Center Bonn (WCCB) kamen am ersten Tag rund 4.800 Teilnehmerinnen und Teilnehmer, am zweiten Tag waren es rund 3.000.

„Digitalisierung in Deutschland: Packen wir es an!" Mit diesen Worten eröffnete Generalmajor Armin Fleischmann, Vorsitzender AFCEA Bonn und Abteilungsleiter Planung CIR und Digitalisierung der Bundeswehr im Kommando Cyber- und Informationsraum der Bundeswehr, die 38. AFCEA Fachausstellung.

Die gesamte Ausstellung stand unter dem Eindruck der sicherheitspolitischen Zeitenwende: Der russische Angriff auf die Ukraine befindet sich seit geraumer Zeit in einer brachialen Abnutzungsphase, die Krisenregion Naher Osten ist weiterhin fragil. Verbündete wie die USA, auf die Deutschland und die NATO lange setzten, richten sich neu aus. Gleichzeitig treiben disruptive und digitale Technologien die Entwicklung voran.
Auf der Ausstellung trafen sich Bundeswehr, Sicherheitsbehörden, Verwaltung, Wissenschaft und Industrie zum Austausch, damit Gesellschaft, Staat und Bundeswehr die notwendige Resilienz gegenüber den Bedrohungen erreichen.

Großes Interesse bei der 38. Fachausstellung: Rund 4.800 Teilnehmerinnen und Teilnehmer strömten direkt am ersten Tag in die Hallen.

Keynote am ersten Tag: Nathanael Liminski, Minister für Bundes- und Europaangelegenheiten, Internationales sowie Medien und Chef der Staatskanzlei Nordrhein-Westfalen.

Liminski: Informations- und Kommunikationstechnik als Grundlagen unserer Freiheit

Nathanael Liminski, Minister für Bundes- und Europaangelegenheiten, Internationales sowie Medien und Chef der Staatskanzlei Nordrhein-Westfalen, lobt die Veranstaltung als Schaufenster technologischer Exzellenz, Ort sicherheitspolitischer Orientierung und Forum für alle, die unsere digitale, vernetzte, aber auch verletzliche Welt mitgestalten: „Wer heute über Informations- und Kommunikationstechnik spricht, spricht über die Grundlagen unserer Freiheit."

Der Minister sagte vor den Besuchern in Bonn: „Zeitenwende heißt Verantwortung. Es geht um militärische und zivile Verteidigungsfähigkeit, Resilienz von Kommunikations- und Logistikinfrastruktur sowie dem verantwortungsvollen Einsatz von KI, Sensorik und Automatisierung." Zeitenwende bedeute mehr Zusammenarbeit, mehr Vertrauen, mehr Mut und Partnerschaften. Dafür stehe die AFCEA Fachausstellung. „Nicht nur als Geräteschau, sondern als Ort konkreter Lösungen. Als Ort gemeinsamer Verantwortung."

Dr. Fabian Mehring, Bayerischer Staatsminister für Digitales.

Mehring: Technologien entscheiden über unsere Souveränität

Dr. Fabian Mehring, Bayerischer Staatsminister für Digitales bei der AFCEA-Fachtagung sagte in seiner Rede am zweiten Tag, dem 28. Mai 2025, im alten Plenarsaal des Bundestags in Bonn: „Heute, fast 26 Jahre nach dem Umzug von Parlament und Regierung nach Berlin, stehen Deutschland und Europa erneut an einem historischen Wendepunkt. In einer Welt, in der Daten der Schatz der Zukunft sind und Technologien wie KI, Cloud und Quantencomputing über unsere Souveränität entscheiden, geht es wieder um Grundsatzfragen."

Der Minister machte in seiner Rede deutlich, dass die bittere Lehre aus der Energieabhängigkeit gegenüber Russland eindeutig sei: „Bei digitalen Schlüsseltechnologien dürfen wir uns nicht erpressbar machen lassen. KI und Co. entscheiden, wer künftig souverän handelt und wer abhängig bleibt. Wir brauchen im europäischen Verbund ein gesundes Maß an digitaler Souveränität und echte Wahlfreiheit bei Infrastruktur und Technologien. Das gelingt nur, wenn wir mehr Europa wagen und unsere Stärken bündeln." Er forderte alle auf, Deutschland zur Heimat von Hightech zu machen.

Auch am zweiten Tag war die Fachausstellung gut besucht.

Vortrags- und Ausstellungsprogramm
Zum vierten Mal fand die Messe im World Conference Center in Bonn statt. Neben Keynotes und Vorträgen im Plenarsaal des Deutschen Bundestages ergänzten zahlreiche Zusatzformate die traditionelle Ausstellung auf acht Ausstellungsflächen, darunter eine Sonderausstellungsfläche für junge Start-ups und ein Recruiting-Element, organisiert durch die Emerging Leaders AFCEA Bonn e. V. (ELA) in Kooperation mit dem Berufsförderungsdienst Köln.
Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) Bonn e. V. umfasst als gemeinnützig anerkannter Verein ohne kommerzielle Interessen über 1.000 persönliche und weit 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. AFCEA Bonn bietet seinen Mitgliedern und der interessierten Öffentlichkeit ein Spezialforum zu moderner Informations- und Kommunikationstechnologie.
Gegründet wurde AFCEA International 1946 von Angehören der US-Streitkräfte zur Verbesserung des Fernmeldewesens. Der deutsche Verein geht auf die Initiative von Soldaten zurück, die 1983 den Austausch rund um Informations- und Kommunikationstechnik im Verteidigungs- und Sicherheitsbereich fördern wollten. Eingebettet in eine internationale Organisation zählt AFCEA Bonn e.V. heute zu den etabliertesten Dialogplattformen für diese Themen.

Die 39. AFCEA Fachausstellung findet im kommenden Jahr am 12. und 13. Mai statt.

Generalmajor Armin Fleischmann vor historischer Kulisse.

Impressum

Sonderpublikation
AFCEA Fachausstellung 2025
ISSN 0933-3355

MITTLER REPORT

Verlag · Herausgeber
Mittler Report Verlag GmbH
Beethovenallee 21 · 53173 Bonn
Telefon: +49 (0) 228 / 25 90 03 44
E-Mail: info@hardthoehenkurier.de
www.hardthoehenkurier.de

Ein Unternehmen der Gruppe TAMM Media

Geschäftsführer
Peter Tamm

Verlagsleiterin
Sylvia Fuhlisch

Redaktion
Chefredakteur: Michael Horst V.i.S.d.P. (mh)
Telefon: +49 (0) 228 / 35 00 881
Mobil: +49 (0) 173 / 28 91 728
E-Mail: m.horst@mittler-report.de
E-Mail: redaktion@hardthoehenkurier.de

Stellvertretender Chefredakteur:
Stefan Axel Boes (sab)
Telefon: +49 (0) 30 / 86 32 42 662
E-Mail: s.boes@mittler-report.de

Mitarbeiter Redaktion:
Friedrich K. Jeschonnek, Johann R. Fritsch, Knut Görsdorf (kg), Burghard Lindhorst, Dr. Gerd Portugall
E-Mail: redaktion@hardthoehenkurier.de

Fotograf: Socrates Tassos

Marketing · Head of Sales
Michael Menzer
Telefon: +49 (0) 228 / 35 00 866
Mobil: +49 (0) 151 / 15293872
E-Mail: m.menzer@mittler-report.de

Anzeigenkoordination: Karin Helmerath
Telefon: +49 (0) 228 / 25 900 344
E-Mail: k.helmerath@mittler-report.de

Marketing · Anzeigen
Stephen Barnard, Telefon: +49 (0) 228 / 35 00 886,
E-Mail: s.barnard@mittler-report.de

Stephen Elliott, Telefon: +49 (0) 228 / 35 00 872,
E-Mail: s.elliott@mittler-report.de

Thomas Liebe, M.A., Telefon: +49 (0) 228 / 25 900 350,
Mobil: +49 (0) 176 / 24 13 02 29,
E-Mail: t.liebe@mittler-report.de

Susanne Sinß, Telefon: +49 (0) 40 / 70 70 80 310,
E-Mail: s.sinss@hansa-online.de

Layout
AnKo MedienDesign GmbH
Telefon: +49 (0) 2225 / 608 67 42
E-Mail: info@anko-mediendesign.de

Offizieller Partner:

Generalleutnant a. D. Frank Leidenberger im intensiven Gespräch mit Michael Horst während der 38. AFCEA Fachausstellung in Bonn.

Es ist jetzt Zeit zu tun, was nötig ist!

Nachgefragt bei …

Generalleutnant a. D. Frank Leidenberger, CEO und Vorsitzender der Geschäftsführung der BWI GmbH

Sehr geehrter Herr Leidenberger, das Leitthema der AFCEA Fachausstellung 2025 „Zeitenwende in der nationalen Sicherheit – Resilienz durch disruptive digitale Lösungen" hat sich seit dem letzten Jahr nicht geändert. Sind wir aus Ihrer Sicht in der digitalen Zeitenwende zu langsam, was muss sich ändern und welche wesentlichen Folgerungen hat das für die BWI?
Die klare Antwort ist ja, wir sind nicht schnell genug. An vielen Stellen hat man den Eindruck, dass einige in Deutschland glauben, man müsse nur abwarten und dann wird sich alles wieder zum Guten wenden. Aber unabhängig davon, ob Präsident Trump nun gerade mit oder ohne NATO plant und unabhängig davon, wie sich die Situation in der Ukraine weiterentwickelt, müssen wir Deutschland und die Bundeswehr wieder verteidigungsfähig machen. Sieht man sich die neuesten Entwicklungen an, wird überdeutlich klar, dass Digitalisierung und Technologien wie KI und Cloud dabei eine signifikante Rolle spielen. Um Schritt halten zu können, brauchen wir daher für Deutschland eine entsprechend moderne Rechenzentrums- und Kommunikationsinfrastruktur, die sicher und performant ist. Hier spielen „private" Clouds, Multi-Cloud und KI-Rechenzentren eine wichtige Rolle. Der Bund sollte sich auf den Weg machen und beispielsweise KI-Rechenzentren für staatliche Aktivitäten zur Verfügung stellen und diese wichtigen Infrastrukturfragen nicht mehr einzelnen Initiativen überlassen. Wir müssen darüber hinaus ehrlich zu uns selbst sein: Sind

Durchgängig an beiden Tagen immer gut besucht: der Stand der BWI während der 38. AFCEA Fachausstellung in Bonn.

unsere Prozesse so, wie wir sie heute haben, der Situation angemessen? Können wir es uns leisten, auf die Goldrandlösung zu warten, statt endlich auf Tempo zu setzen? Dieses Umdenken in den Köpfen ist nötig. Nur dann werden wir in der Lage sein, uns für die aktuelle und zukünftige geopolitische Situation angemessen aufzustellen.

Schluss mit Zuschauen – Zeit loszulegen! Was und wen konkret meinen Sie damit? Ist der „Whatever it takes"-Ansatz zielführend?
Eine Schlüsselfrage ist, ob es uns gelingt, die Produktion der Verteidigungsindustrie so zu beschleunigen, dass sie nicht mehr durch die derzeitigen, eher bürokratischen Prozesse des Regierungs- und Verwaltungshandelns gebremst ist. Denn was müssen wir eigentlich erreichen? Wir müssen die Produktion unserer Waffen- und Einsatzsysteme von Anfang an als industriellen Prozess der Massenfertigung begreifen und ihn frühzeitig von der Rohstoffbeschaffung bis hin zum Endprodukt durchgängig denken. Wir müssen niedrige Hardware-Kosten erreichen und diese mit hochwertiger Software – und hier liegt der Schlüssel zur Überlegenheit – verbinden. Das ist das neue Ökosystem, das wir gestalten müssen, bei dem IT eine wesentliche Rolle spielen wird. Dafür ist es wichtig, dass wir aufhören, die Zeitenwende nur zu beobachten und darüber zu reden – es ist jetzt Zeit zu tun, was nötig ist.

Die BWI gibt auf dem Messestand Einblicke zu Projekten, die dazu beitragen, die IT der Bundeswehr automatisierter, reaktionsschneller und resilienter zu machen. Was bedeuten Cloud, Data Analytics und Automation für die Fähigkeiten der Streitkräfte?
Ohne diese Technologien werden Streitkräfte künftig nicht bestehen können. Bei militärischen Konflikten geht es zuallererst um Tempo. Wer schneller Informationen hat, wer schneller reagieren kann, der ist im Vorteil. Dies gilt für die letzte Meile genauso wie für alle Prozesse und Abläufe im Hintergrund. Über eine Cloud lassen sich Anwendungen, Plattformen und Infrastrukturen als skalierbare Services schneller, flexibler und effizienter zur Verfügung stellen. Sie ist aber auch Grundlage für den Datentransfer unmittelbar im Einsatz. Data Analytics hilft bei der Auswertung der entstehenden Datenmengen. Das ist in vielen Bereichen wichtig, wird aber auch bei der Aufklärung eine Rolle spielen, wenn zum Beispiel Drohnendaten ausgewertet werden müssen. Automation hilft uns dabei, Prozesse schneller und effizienter zu gestalten und letzten Endes auch Fehler zu vermeiden. Gerade bei einer dem Umfang nach kleinen Armee, die aber schlagkräftig sein soll, spielt diese Effizienz eine wichtige Rolle.

Die AFCEA Bonn e.V. hat sich zu einer der etabliertesten Dialogplattformen für die IT- und Kommunikationsbranche entwickelt. Sind Sie zufrieden mit dem Interesse der zivilen und besonders militärischen Besucher oder spüren Sie noch Skepsis?
Ich glaube, Skepsis ist das falsche Wort. Bei den militärischen Besuchern herrschte weitestgehend Klarheit darüber, in welcher Situation sich Deutschland und die Bundeswehr befinden und was jetzt getan werden muss.
In unserer Gesellschaft insgesamt setzt sich die Erkenntnis, dass Deutschland plötzlich wieder selbst gefragt ist, seine demokratischen Werte zu verteidigen – was Geld kostet und zur Not auch militärische Mittel erfordert –, nur langsam durch. Ich glaube, statt Skepsis herrscht im zivilen Umfeld eher Unsicherheit, was die aktuelle Situation für uns als Land in Europa und für jeden einzelnen bedeutet und was genau jetzt passieren muss. Hier müssen Politik, Wirtschaft, Bundeswehr und Forschung die Köpfe zusammenstecken, den konkreten Bedarf analysieren und einen gemeinsamen Lösungsweg definieren, den alle mittragen. Ja, das wird Geld kosten und nicht alles wird morgen fertig sein – aber der Weg ist alternativlos. Deutschland muss wieder verteidigungsfähig werden. Für sich selbst und natürlich zusammen mit seinen Partnern.

Sehr geehrter Herr Leidenberger, vielen Dank für die interessanten Informationen und weiterhin viel Erfolg für Ihre wichtige Arbeit!

Private Cloud der Bundeswehr erhält Google-Anteil

Von Gerhard Heiming

©MRV/Gerd Heiming

Informationen zur pCloudBw am Stand der BWI während der 38. AFCEA Fachausstellung in Bonn.

Die ab 6. Januar in Betrieb gegangene private Cloud der Bundeswehr (pCloudBw) erhält bis Ende 2027 zwei neue physikalisch getrennte Cloud-Instanzen. Die BWI GmbH, der Betreiber der pCloudBw, beschafft in einem Rahmenvertrag die Lösung Google „Cloud Air-Gapped".

Die Lösung wird von der Google Cloud Public Sector – Deutschland GmbH geliefert, wie die BWI am 26. Mai mitgeteilt hat.
Bis Ende 2027 wird die BWI nach eigener Angabe damit eine weitere Cloud-Umgebung in den eigenen Rechenzentren aufbauen und betreiben. Sie soll Teil der private Cloud der Bundeswehr werden. Mit der Google Cloud Air-Gapped sollen zwei physikalisch getrennte Cloud-Instanzen aufgebaut werden: für die Verarbeitung offener sowie geschützter Daten.
Die BWI will die Lösung des Herstellers Google Cloud in den bundeswehreigenen Rechenzentren physisch vollständig von anderen Google-Systemen oder Netzwerken isoliert (air-gapped) installieren und betreiben. Die Bundeswehr besitze so zu jeder Zeit die Kontrolle über die eigenen Daten und komme damit ihrer Anforderung nach Informations- und Datensicherheit nach.

Das Vorhaben ist Teil der Cloud-First-Strategie der Bundeswehr und damit der BWI, die ihre IT-Services künftig grundsätzlich cloudbasiert bereitstellen wird. Google Cloud ist damit nun der zweite Lieferant von Lösungen für die pCloudBw. Die BWI will in Zukunft verstärkt Open Source Software in der pCloudBw einsetzen, um damit ihrem Anspruch nach digitaler Souveränität nachzukommen.
„Wir verstehen die kritische Bedeutung der Datensicherheit, insbesondere für die Bundeswehr. Unsere Lösungen sind darauf ausgelegt, sie mit dem höchsten Maß an Sicherheit und Kontrolle auszustatten", sagte Tara Brady, President EMEA Google Cloud.
„Die Google-Plattform ist Teil unseres Multi-Cloud-Ansatzes", so Frank Leidenberger, Chief Executive Officer der BWI. Mit der Vorgehensweise werde die BWI einseitige Abhängigkeiten verringern und so zur digitalen Souveränität der Bundeswehr beitragen. Gleichzeitig könne so für jede operative Anforderung die wirtschaftlichste Cloud-Lösung genutzt werden. „Mit Google Cloud Air-Gapped als Teil der pCloudBw erhält die Bundeswehr eine Lösung, die sie aktiv steuern kann und damit ihre Handlungsfähigkeit ausbaut", so Leidenberger.

BWI GmbH – primärer Digitalisierungspartner der Bundeswehr

Die BWI ist eines der größten IT-Service-Unternehmen in Deutschland. In Frieden, Krise und Krieg erbringt sie für die Bundeswehr stabile, sichere und effiziente IT-Services im Inland und Ausland. So trägt sie zur kontinuierlichen Erhöhung der Führungs- und Einsatzfähigkeit sowie Kampfkraft der Streitkräfte bei. Seit ihrer Gründung 2006 hat die BWI ihr Leistungsportfolio enorm erweitert. Sie berät kompetent. Sie entwickelt zügig auch neue IT-Lösungen für die Bundeswehr – „innovativ by design". Und sie ist zentrale Kraft beim Auf- und Ausbau eines resilienten Partner-Ökosystems. Als attraktiver Arbeitgeber gewinnt und bindet die BWI hochqualifizierte Kräfte, welche die Bundeswehr-IT aus Überzeugung voranbringen. So stehen inzwischen über 7.700 Mitarbeitende bundesweit als „Team of Teams" hinter der Vision der BWI: für die Bundeswehr-IT und damit die digitale Zukunftsfähigkeit Deutschlands zu sorgen.

Einsatzerprobte Cybersicherheit

Für Multi-Domain Operations von heute & morgen!

GEHEIM | EU SECRET | NATO SECRET | COMMON CRITERIA

infodas Cross Domain Solutions und Cybersecurity-Beratung

Sichere Interoperabilität für ein souveränes Europa.

info@infodas.de
+49 221 70912-0
INFODAS GmbH / www.infodas.com

infodas
connect more. be secure.

DefenceCareer

... Ihre Mission startet hier!

Suchbegriff, Position

Ort, PLZ 25km

Job finden

EXKLUSIV AUF UNSEREN WEBSITES

ES&T EUROPÄISCHE SICHERHEIT & TECHNIK

SOLDAT & TECHNIK

Hardthöhen-KURIER

IHRE NEUE JOBBÖRSE

im Bereich Military-Interest

DefenceCareer – Die neue Online-Jobbörse im Bereich Military-Interest, die Ihnen ermöglicht, gezielt Fach- und Führungskräfte mit der Affinität zu Defence und Wehrtechnik zu erreichen und durch passendes Employer Branding für Ihr Unternehmen zu gewinnen!

Scannen Sie den QR-Code oder erfahren Sie mehr auf: **defencecareer.de**

Kontakt:
CONET-Gruppe
Dominik Rüber
Senior Vice President
Sales Defense
Bundeskanzlerplatz 2
53113 Bonn
info@conet.de
www.conet.de

Partnerschaftlich. Zukunftsorientiert.
Für eine digitale Verteidigung.

Die CONET-Gruppe unterstützt als IT Full-Service Provider eine Vielzahl von Kunden im Defense-Markt (wie beispielsweise Bundeswehr, BWI und viele weitere) zuverlässig auf dem Weg in die digitalisierte Zukunft. Die Unternehmensgruppe mit Hauptsitz in Bonn und weiteren Standorten in Deutschland, Österreich, in der Schweiz sowie in Kroatien ist maßgeblich an wichtigen Entwicklungs- und Transformationsprozessen in der Informationstechnologie des Verteidigungssektors beteiligt. Mit starker Branchenexpertise aus mehr als 35 Jahren IT-Erfahrung investieren wir gezielt in Schlüsseltechnologien wie Künstliche Intelligenz, Cloud und Cyber, um innovative Projektansätze zu entwickeln und einen Beitrag zur digitalen Verteidigung zu leisten.

Kontakt:
Bechtle AG
E-Mail: zpls-r1753@bechtle.com
Telefon: 0228 6888 400
www.bechtle.com

Bechtle zählt zu den erfolgreichsten IT-Dienstleistern in Europa. Mit 15.800 Mitarbeitenden, mehr als 100 IT-Systemhäusern sowie IT-Handelsgesellschaften in 14 Ländern Europas ist Bechtle stets nah dran an seinen Auftraggebern. Die Kombination aus Direktvertrieb von IT-Produkten mit umfassenden Dienstleistungen aus den Systemhäusern heraus macht Bechtle zum IT-Zukunftspartner im Public Sector. Aber auch Beständigkeit ist eine Stärke von Bechtle. Seit mehr als 15 Jahren ist Bechtle zuverlässiger Rahmenvertragspartner diverser Rahmenverträge des BAAINBw, so auch seit 2009 durchgehend für die 2./3. Rechnerebene.

Das herstellerübergreifende Produkt- und Leistungsportfolio reicht von Standard- und Individual-Hard- und -Software, Open Source Produkten, Hybrid- und Multi-Clouds, IT-Security hin bis zu disruptiven digitalen Lösungen.
Gemeinsam mit den Herstellerpartnern HPE Aruba, Dell Technologies, Nvidia, NetApp, Bechtle Logistik Apple Authorised Reseller sowie Planet Solutions zeigte Bechtle ein eindrucksvolles Portfolio aus den Themengebieten der Rechenzentrumsausstattung mit Servern sowie Speichersysteme, Netzwerk- & Funktechnik, Künstliche Intelligenz zur Verwaltung von Dokumenten- & Vorschriftenlagen.

Die Bedrohung durch Russland im Cyber- und Informationsraum

Von Nikolaus Sperling, Joint Intelligence Center Kommando CIR

„Putin greift hybrid an. […] Wir müssen uns vorbereiten, um uns Putins Bedrohung selbstbewusst entgegenstellen zu können", warnte Verteidigungsminister Boris Pistorius Ende 2024. Hybride Bedrohungen sind nicht konventionell militärisch oder lassen sich nicht eindeutig einem Verursacher zuordnen.

Neben den zu erzielenden Effekten ist das vorrangige Ziel ein glaubhaftes Abstreiten, um eine juristische Aufarbeitung zu verhindern. Russland hat Maßnahmen im hybriden Spektrum bereits zu Zeiten der Sowjetunion doktrinär verankert, um seine Ziele auch unterhalb des sichtbaren Einsatzes eigener Streitkräfte zu erreichen. Dazu wird unter anderem auf Spionage, Sabotage sowie paramilitärische Gruppierungen zurückgegriffen. Ein besonderer Fokus liegt jedoch auf dem Wirken im Cyber- und Informationsraum. Dies beinhaltet Cyberattacken und die Beeinflussung der öffentlichen Meinung, beispielsweise durch auf den jeweiligen Gegner angepasste Desinformationskampagnen. Gesteuert und ausgeführt wird dies vor allem durch russische Nachrichtendienste oder instrumentalisierte Dritte, sogenannte Proxys. Nach russischem Verständnis ist es rechtmäßig, im Falle „unfreundlicher Handlungen ausländischer Staaten […] asymmetrische Maßnahmen zu ergreifen." Basierend hierauf ist damit aus Sicht Russlands auch die Anwendung hybrider Maßnahmen im Ukrainekrieg legitimiert.

©BwiChristian Prawos

Cyberangriffe als „Rache" für die deutsche Ukraine-Unterstützung? Verteidigungsminister Boris Pistorius und der ukrainische Präsident Wolodymyr Selenskyj besuchen ukrainische Soldaten während der Ausbildung in Sanitz.

Russlands Maßnahmen im Cyber- und Informationsraum im Russland-Ukraine-Krieg

Vor Beginn des Angriffes auf die Ukraine etablierte Russland das Narrativ, im Donbass fände ein Genozid an der prorussischen Bevölkerung statt. Die Verbreitung dieser Behauptung durch Putin und hochrangige Politiker verlieh ihr das nötige Gewicht. Parallel dazu wurde das Narrativ medial in Russland in hoher Taktung aufgegriffen. Proxys, die offiziell nicht in Verbindung mit Russland stehen, platzierten das Narrativ darüber hinaus im Westen. Hierdurch sollte die „Spezialoperation" Russlands gegenüber der eigenen Bevölkerung und dem Westen legitimiert werden. Dieser Ablauf stellt das gängige Vorgehen Russlands zur Beeinflussung des Meinungsbildes dar. Die Narrative, der Angriff Russlands auf die Ukraine sei durch die fortschreitende NATO-Ost-Erweiterung erzwungen worden sowie die vermeintliche Existenz amerikanischer Biowaffenlabore in der Ukraine, sind weitere Beispiele für russische Desinformation hinsichtlich des Russland-Ukraine-Krieges.
Zeitgleich zum Angriff auf die Ukraine 2022 führte Russland eine massive Cyberattacke auf den Satellitennetz-Anbieter Viasat durch, was großflächige Ausfälle ziviler und militärischer Kommunikation innerhalb der Ukraine zur Folge hatte. Als Kollateralschaden brachen Serviceverbindungen von bis zu 5.000 Windrädern in Europa zusammen. Ein weiterer schwerwiegender russischer Cyberangriff Ende 2023 legte tagelang den ukrainischen Telekommunikationsanbieter Kyivstar für rund 24 Millionen Nutzer lahm. Darüber hinaus setzt Russland Cyberspionage in der Ukraine ein, um Informationen zu sammeln und künftige Angriffsziele auszukundschaften.

Russlands Maßnahmen im Cyber- und Informationsraum gegen Deutschland

Auch EU- und NATO-Staaten sind ein ständiges Ziel hybrider Bedrohungen Russlands. Eine Zunahme russischer Maßnahmen im Cyber- und Informationsraum erfolgte vor dem Hintergrund der Ukraine-Unterstützungsleistungen. So geriet auch Deutschland ins Visier: Um auf die deutsche Ukraine-Unterstützung einzuwirken, versuchte Russland unter anderem, die Bundestagswahl zu beeinflussen. Weiterhin wird durch Russland regelmäßig impliziert, dass eine Unterstützung der Ukraine eine Ausweitung des Krieges oder den Einsatz von Atomwaffen nach

sich ziehen könnte. Zur Verbreitung dieser Narrative erstellen Russland und dessen Proxys auch Internetseiten, die täuschend echt seriöse Nachrichtenseiten imitieren. Deren Berichte scheinen russische Narrative zu bestätigen.
Weiterhin setzt Russland Cyberattacken gegen Deutschland ein, darunter Cyberspionage, die meist durch sogenanntes Phishing eingeleitet wird. Dabei werden unter Vorspielen falscher Tatsachen Zugangsdaten erbeutet, um in IT-Netzwerke einzudringen. Von besonderem Interesse sind dabei Deutschlands Pläne zur Ukraine-Unterstützung. Darüber hinaus ist Deutschland Ziel prorussischer Hacktivisten (Kofferwort aus Hacker und Aktivisten), also von Cyberakteuren, die ideologisch motiviert agieren. Diese setzen meist Überlastungsangriffe ein, sogenannte DDoS-Attacken (Distributed Denial-of-Service). Dies sind massenhaft parallel stattfindende Zugriffe auf Webseiten und deren Server, was zu temporären Ausfällen führen kann. Seit Ende 2024 sind regelrechte DDoS-Kampagnen gegen Deutschland zu beobachten. Dabei werden die Angriffe als „Rache“ für die deutsche Ukraine-Unterstützung dargestellt. In der Regel entsteht dabei kein bleibender Schaden. Primär wird hierdurch das öffentliche Meinungsbild beeinflusst.

Was folgt?
Stetes Ziel Russlands ist es, durch hybride Bedrohungen westliche Gesellschaften und Bündnisse zu spalten. Deshalb erwartet die NATO auch künftig hybride Maßnahmen Russlands. Um dem begegnen zu können,

©BwI/Maximilian Bosse

Lagebeobachter aus dem Kommando CIR im Nationalen IT-Lagezentrum BSI: unverzichtbare Partner in der Abwehr von Cyberangriffen in Deutschland.

©BwI/Anne Weinrich

Generalleutnant Alexander Sollfrank, Befehlshaber des Operativen Führungskommandos der Bundeswehr, spricht beim ersten Stresstest des Operationsplans Deutschland am 20. November 2024 in Berlin.

©BSI

Infografik zu Phishing-Angriffen vom Bundesamt für Sicherheit in der Informationstechnik.

überarbeitet die NATO seit Ende 2024 ihre Strategie zur Abwehr hybrider Bedrohungen. Diese soll sicherstellen, dass Infrastruktur besser vor Sabotage geschützt wird, ein verstärkter Austausch lagerelevanter Erkenntnisse stattfindet und geklärt wird, wie adäquat auf hybride Aktivitäten reagiert werden kann.

Weiterhin gehen NATO, Bundeswehr und Deutschland davon aus, dass Russland Ende der Dekade in der Lage wäre, die NATO großmaßstäblich anzugreifen. Deutschland würde hierbei in seiner Funktion als Drehscheibe für verbündete Kräfte ein vorrangiges Ziel sein. In diesem Rahmen werden auch hybride Aktivitäten erwartet, beispielsweise in Form von Cyberangriffen zu Sabotage- oder Spionagezwecken. Um auf dieses Szenario gesamtstaatlich vorbereitet zu sein, entwickelt die Bundeswehr unter Beteiligung einer Planungsgruppe aus Bund, Ländern, Kommunen, Blaulichtorganisationen und Wirtschaft den „Operationsplan Deutschland".

Möglichkeiten des Handelns

Laut einer Umfrage des Digitalverbandes Bitkom befürchten 61 Prozent der Befragten Cyberangriffe auf Deutschland und denken, dass die Behörden hierauf schlecht vorbereitet sind. Tatsächlich sind die Bundesbehörden, auch abseits des „Operationsplans Deutschland", sensibilisiert. Maßnahmen gegen hybride Bedrohungen sind zum Beispiel Haftbefehle, Sanktionen oder das Sperren von Medien, die Desinformation verbreiten. Zudem befassen sich in Deutschland verschiedenste Instanzen mit hybriden Bedrohungen, darunter Sicherheitsbehörden und Nachrichtendienste. Um den Bedrohungen ressortübergreifend begegnen zu können, bestehen Kooperationen wie das Nationale Cyber-Abwehrzentrum, das sich mit der Abwehr elektronischer Angriffe auf IT-Infrastrukturen Deutschlands befasst. Ein Gremium, das sich mit der Beeinflussung der öffentlichen Meinung befasst, ist die „Task Force gegen Desinformation" des Bundesministeriums des Inneren. An beiden Formaten nehmen Angehörige verschiedener Dienststellen der Bundeswehr teil, die dem Kommando Cyber- und Informationsraum, dem Führungskommando der Teilstreitkraft Cyber- und Informationsraum, unterstellt sind. Es vereint wesentliche Fähigkeiten der Bundeswehr in diesem Bereich. Folgende Dienststellen sind besonders in die Erkennung und Abwehr hybrider Bedrohungen involviert:

- Das Kommando Informationstechnik-Services stellt Informationstechnik-Services für die Bundeswehr bereit, überwacht das IT-System der Bundeswehr und gewährleistet die Führungsfähigkeit der Bundeswehr im Inland und Einsatz.
- Das Zentrum für Cyber-Sicherheit der Bundeswehr stellt den Schutz der Bundeswehr-IT sicher, reagiert auf Angriffe und wirkt bei externen, nationalen wie internationalen Partnern mit.
- Das Zentrum Cyber-Operationen befasst sich mit offensiven und defensiven Cyber-Operationen im Rahmen der Landes- und Bündnisverteidigung. Außerdem liefert es Beiträge zur Resilienz eigener IT-Systeme und zeigt der militärischen und politischen Führung Handlungsmöglichkeiten auf, um auf Krisenlagen zu reagieren.
- Das Zentrum Operative Kommunikation der Bundeswehr ist befähigt, auf externe gegnerische Akteure einzuwirken. Hierzu erfasst und bewertet es u. a. das öffentliche Meinungsbild in den Verursacherländern und untersucht, welche Maßnahmen zu dessen Beeinflussung eingesetzt werden können.

Auch der Mensch spielt eine wichtige Rolle in der Abwehr hybrider Bedrohungen im Cyber- und Informationsraum: Sowohl Cybersabotage als auch -spionage werden oftmals durch Phishing-Attacken eingeleitet. Es gilt also, sämtliche Nachrichten, die entsprechende Daten abfragen, kritisch zu prüfen. Weiterhin ist Vorsicht bei der Auswahl und dem Speichern von Passwörtern geboten. Diese können erraten oder, sofern in Browsern oder Systemen gespeichert, beim Eindringen in ein System direkt abgerufen werden. Außerdem gilt es, Inhalte von (sozialen) Medien kritisch zu prüfen und auf deren Quelle oder Impressum zu achten, um nicht selbst Opfer von Desinformation zu werden oder unwissentlich weiterzuverbreiten. Durch solche einfachen Methoden kann hybriden Bedrohungen im Cyber- und Informationsraum bereits in ihren Anfängen erfolgreich begegnet werden.

Hybride Maßnahmen durch Russland im Cyber- und Informationsraum sind ernst zu nehmende Bedrohungen. Sie werden engmaschig durch die Bundeswehr und andere Instanzen des Bundes beobachtet. Neben der durchgehenden Aufklärungsarbeit werden qualifizierte Gegenmaßnahmen auf erkannte Aktivitäten vorbereitet, um so die Sicherheit Deutschlands zu gewährleisten.

Gamechanger Satellitenkommunikation

Die Rolle der Satellitenkommunikation auf dem digitalen Gefechtsfeld

Von Oberstleutnant i.G. Markus Gelhausen und Fregattenkapitän Dr. Martin Hellmann,

Kommando Cyber- und Informationsraum

Moderne Kriegsführung und militärische Operationen sind ohne die Nutzung des Weltraums nicht mehr vorstellbar. Disruptive Technologien wie Künstliche Intelligenz, Hyperschallwaffen und Robotik haben den Charakter bewaffneter Konflikte bereits jetzt grundlegend verändert und ein Ende dieser Entwicklung ist nicht absehbar.

Durch diese technologischen Entwicklungen werden insbesondere auch die Waffensysteme schneller, präziser und wirksamer. In diesem sich wandelnden Umfeld stellt sich die Bundeswehr der Herausforderung, ihre Weltraumfähigkeiten weiterzuentwickeln und an die Zeitenwende anzupassen.

Weltraumoperationen und Einsatzunterstützung aus dem Weltraum

Die weltraumbezogenen Aktivitäten der Bundeswehr werden unter dem Begriff „Dauereinsatzaufgabe Weltraumnutzung" zusammengefasst. Unterschieden wird dabei zwischen Weltraumoperationen und der Einsatzunterstützung aus dem Weltraum. Weltraumoperationen sind Aktivitäten zu Schutz und Verteidigung militärischer Weltraumsysteme und fallen in den Verantwortungsbereich des bei der Luftwaffe verorteten Weltraumkommandos der Bundeswehr. Die Teilstreitkraft Cyber- und Informationsraum (TSK CIR) hingegen ist für die Einsatzunterstützung aus dem Weltraum zuständig.

Die Teilstreitkraft CIR ist als zentraler militärischer Nutzer des Weltraums etabliert. In diesem Rahmen leisten weltraumgestützte Systeme einen wesentlichen Beitrag zur Informations- und Wirkungsüberlegenheit durch das dimensionsübergreifende Zusammenwirken im Sinne von Multi-Domain Operations. Ein wesentliches Alleinstellungsmerkmal der TSK CIR ist, dass sie über alle Satellitensysteme der Bundeswehr verfügt. Darüber hinaus nutzt sie die Services einer Vielzahl ziviler Satellitensysteme, um den Umfang der Unterstützungsleistungen qualitativ und quantitativ zu erweitern. Durch eine enge Zusammenarbeit der TSK Cyber- und Informationsraum

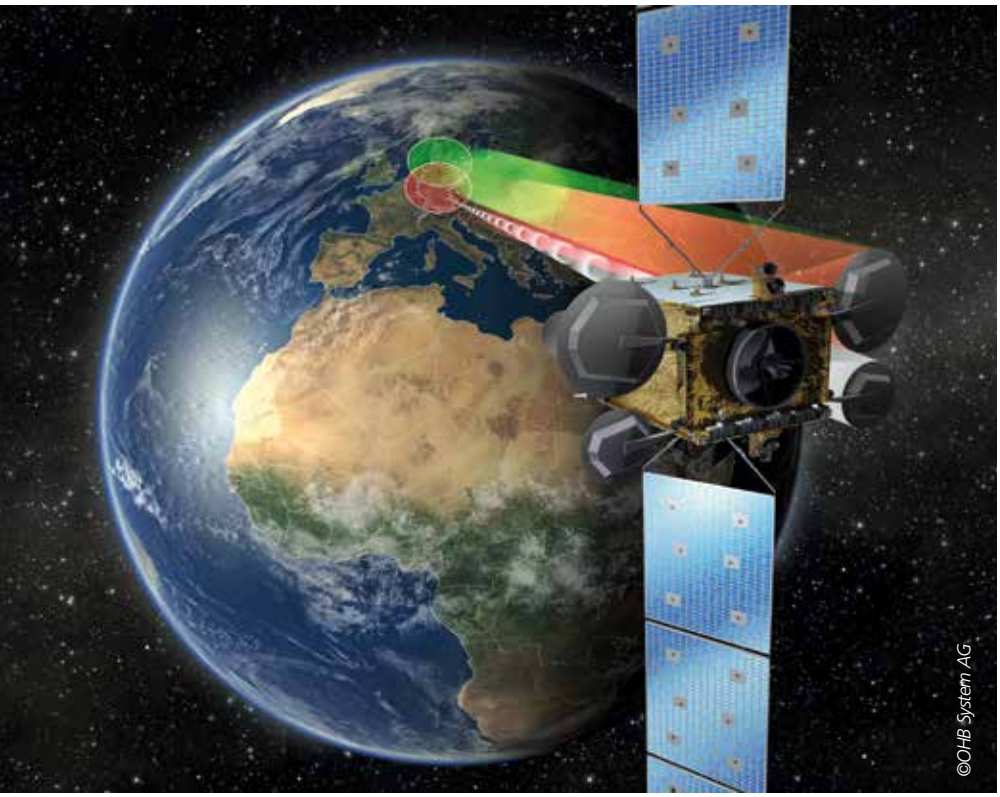
©Bw/Stefan Uj

Die Bodenstation von SATCOMBw ist Teil des Service Delivery Point: Im Gefecht folgt der Service Delivery Point dem Gefechtsstand und stellt durch die Kommunikationsanbindung die Führungsfähigkeit sicher.

mit dem Weltraumkommando der Bundeswehr in Uedem erfolgt eine koordinierte und auf militärische Bedarfe ausgerichtete Nutzung des Weltraums. Das Weltraumkommando unterstützt dabei aktuell das Kommando CIR im Wesentlichen durch die Bereitstellung der Weltraumlage.

Erfahrungen und Reaktionen

Der Angriffskrieg Russlands gegen die Ukraine hat die immense Bedeutung moderner Satellitenkommunikation (SatCom) für die Kriegsführung im 21. Jahrhundert deutlich vor Augen geführt. Die Erfahrungen aus diesem Konflikt zeigen, dass leistungsfähige und robuste SatCom-Systeme einen entscheidenden Vorteil auf dem digitalen Gefechtsfeld darstellen und maßgeblich zur Informationsüberlegenheit beitragen. Sie zeigen insbesondere aber auch die Abhängigkeit von diesen Systemen und die sich daraus ergebende Notwendigkeit einer verlässlichen Nutzung.



Der geostationäre Kommunikationssatellit Heinrich Hertz stärkt die nationale Kompetenz im Bereich der Satellitenkommunikation.

Eine der wichtigsten Lehren aus dem Ukrainekrieg ist die zentrale Rolle kommerzieller Satellitensysteme wie Starlink für die militärische Kommunikation. Die Ukraine konnte durch den Zugang zu diesem System ihre Kommunikationsfähigkeiten aufrechterhalten, selbst als terrestrische Infrastrukturen zerstört wurden. Dies verdeutlicht die Notwendigkeit für Streitkräfte, auf ein breites Spektrum von SatCom-Ressourcen zurückgreifen zu können, um durch Redundanz Resilienz zu gewährleisten.

Gleichzeitig hat der Konflikt die Verwundbarkeit von Satellitensystemen gegenüber elektronischer Kriegsführung und Cyberangriffen offengelegt. Russland setzt massiv Störsender ein, um ukrainische Kommunikation und GPS-Signale zu beeinträchtigen. Dies unterstreicht die Bedeutung von robusten, störresistenten SatCom-Systemen für moderne Streitkräfte. Die Fähigkeit, auch unter widrigen elektronischen Bedingungen kommunizieren zu können, ist für die Führungsfähigkeit entscheidend und damit für den Erfolg militärischer Operationen essenziell.

Weiterentwicklungen

Als Reaktion auf diese Erkenntnisse entwickeln Streitkräfte weltweit, einschließlich der Bundeswehr, zunehmend vernetzte und integrierte Multi-Orbit-Satellitenkonstellationen. Diese Systeme kombinieren Satelliten in verschiedenen Umlaufbahnen – geostationär (GEO), mittlere Erdumlaufbahn (MEO) und niedrige Erdumlaufbahn (LEO) –, um die Vorteile der jeweiligen Orbits zu nutzen. GEO-Satelliten bieten eine konstante regionale Abdeckung, während LEO-Konstellationen globale Abdeckung mit geringerer Latenz ermöglichen. MEO-Satelliten stellen einen Kompromiss zwischen beiden dar.

Die Bundeswehr setzt bei der Weiterentwicklung ihrer SatCom-Fähigkeiten auf eine Kombination aus nationalen und europäischen Infrastrukturen. Das SATCOMBw-System, bestehend aus den COMSATBw-Satelliten, bildet das Rückgrat der militärischen Satellitenkommunikation. Die geplante Modernisierung dieses Systems mit einem Investitionsvolumen von 1,4 Milliarden Euro unterstreicht die hohe Priorität, die der Satellitenkommunikation beigemessen wird.

Ein Meilenstein in der Weiterentwicklung deutscher SatCom-Fähigkeiten ist der 2023 gestartete Satellit Heinrich Hertz. Dieser geostationäre Kommunikationssatellit dient nicht nur wissenschaftlichen Zwecken, sondern verfügt auch über eine militärische Nutzlast. Er ermöglicht die Erprobung neuer Technologien unter realen Weltraumbedingungen und stärkt die nationale Kompetenz im Bereich der Satellitenkommunikation.

Auf europäischer Ebene plant die EU mit dem IRIS²-Projekt (Infrastructure for Resilience, Interconnectivity and Security by Satellite) den Aufbau einer eigenen Multi-Orbit-Konstellation. Diese soll bis 2031 knapp 300 Satelliten umfassen und sowohl zivile als auch militärische Kommunikationsdienste bereitstellen. IRIS² ist als europäische Antwort auf kommerzielle Systeme wie Starlink konzipiert und soll die strategische Autonomie Europas im Bereich der Satellitenkommunikation stärken. Das System soll auch weitere Nutzlasten beinhalten, um neben Kommunikationsdiensten auch weitere weltraumgestützte Services anbieten zu können. Deutschland stellt den Großteil der Finanzierung und wird daher auch maßgeblich Art und Umfang dieser Services mit beeinflussen.

Die Vermaschung dieser verschiedenen SatCom-Systeme ist entscheidend für die Befähigung der Bundeswehr zum Führen von Multi-Domain Operations (MDO). MDO

erfordern eine nahtlose Vernetzung aller Streitkräfte und Sensoren über alle Dimensionen hinweg – Land, Luft, See, Weltraum und Cyberspace. Satellitenkommunikation spielt hierbei eine Schlüsselrolle, indem sie die notwendige Konnektivität für den Informationsaustausch zwischen diesen Dimensionen bereitstellt.
Moderne SatCom-Systeme ermöglichen es, Aufklärungsdaten von Satelliten, unbemannten Luftfahrzeugen und Bodensensoren in Echtzeit zu fusionieren und an Entscheidungsträger und Einsatzkräfte an nahezu jeden Ort der Welt zu übermitteln. Dies verbessert das Lagebild erheblich und ermöglicht schnellere und präzisere Entscheidungen. Die hohe Bandbreite moderner Satellitensysteme erlaubt zudem die Übertragung großer Datenmengen, was für die Steuerung unbemannter Systeme und die Nutzung von KI-gestützten Entscheidungshilfen unerlässlich ist.

Die Cybersicherheit
Ein weiterer wichtiger Aspekt ist die Cybersicherheit von Satellitensystemen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Stärkung der Cybersicherheit von Weltrauminfrastrukturen als strategisches Ziel definiert. Dies umfasst sowohl den Schutz der Bodenstationen als auch die Sicherung der Satelliten selbst gegen Cyberangriffe und elektronische Störmaßnahmen.

Die Zukunft der militärischen Satellitenkommunikation liegt in hochgradig vernetzten, resilienten Systemen, die verschiedene Orbits und Technologien kombinieren. Die Bundeswehr plant den Aufbau einer vernetzten Multi-Orbit-Gesamtarchitektur, die flexibel auf steigende Anforderungen reagieren kann. Diese soll neben Satellitenkommunikation auch Fähigkeiten zur weltweiten abbildenden und signalerfassenden Aufklärung umfassen.

Fazit
Zusammenfassend ist festzuhalten, dass Satellitenkommunikation ein echter Gamechanger auf dem modernen Gefechtsfeld ist. Sie ermöglicht erst die Umsetzung des Ziels der NATO einer „MDO enabled Alliance", insbesondere durch Verbesserung der multinationalen dimensionsübergreifenden Führungsfähigkeit. Die Erfahrungen aus dem Ukraineкrieg haben die strategische Bedeutung resilienter SatCom-Systeme unterstrichen. Deutschland und Europa investieren daher massiv in den Ausbau ihrer Weltraumfähigkeiten, um im digitalen Zeitalter handlungsfähig zu bleiben. Die Herausforderung wird darin bestehen, mit der rasanten technologischen Entwicklung Schritt zu halten und gleichzeitig die Sicherheit und Resilienz dieser kritischen Infrastrukturen zu gewährleisten.

Vernetzung militärischer Systeme mit der Rheinmetall Battlesuite

Auf der AFCEA Fachausstellung stellten Rheinmetall und blackned die Rheinmetall Battlesuite vor, eine Plattform zur Vernetzung militärischer Systeme auf dem Gefechtsfeld.

©MRV

Timo Hass, Chief Digital Officer der Rheinmetall AG und Leiter des Clusters „Digitalisation", im Gespräch mit Michael Horst.

Konnektivität, die digitale Verbindung zwischen Soldaten und Fahrzeugen, zwischen Fahrzeugen untereinander und beispielsweise auch zwischen Drohnen und Fahrzeugen auf dem digitalen Gefechtsfeld ist ein echter „Gamechanger", stellte CEO Armin Papperger auf der Hauptversammlung der Rheinmetall AG am 13. Mai fest. Um die Digitalisierung der Bundeswehr effektiv unterstützen zu können, hat das Unternehmen in der Division Electronic Solutions das Cluster „Digitalisation" eingeführt, das sich dem Thema Software Defined Defence mit Megatrends wie Künstliche Intelligenz, Battlefield Management und Drohnen-Technologie widmet.

Basis Tactical Core

Timo Hass, Chief Digital Officer der Rheinmetall AG und Leiter des Clusters „Digitalisation", stellte die Rheinmetall Battlesuite als Kernelement für die Fähigkeit, konventionelle Waffensysteme mit unbemannten Systemen zu vernetzen, vor. Damit werde eine synergistische Wirkung erzielt, bei der die Vorteile beider Welten – die Präzision und Flexibilität besatzungsloser Systeme und die Robustheit und Vielseitigkeit konventioneller Systeme – zur Geltung kommen. Mit der Battlesuite werde der Informationsraum in Echtzeit zusammengeführt: von der unmittelbaren Kampfzone bis zu den hinteren Bereichen, von See, Land und Luft.

Basis der Battlesuite ist das Tactical Core, eine offene Middleware von blackned, die quasi als Betriebssystem die Infrastruktur bereitstellt. Das Tactical Core wird derzeit in Gefechtsfahrzeuge und Waffensysteme der Bundeswehr implementiert. Darauf setzen Applikationen auf, die die benötigten militärischen Fähigkeiten realisieren. Sie ermöglichen den Zugriff auf Kommunikationskanäle, auf Sensoren für Aufklärung und Warnung, auf Effektoren. Die Informationen werden in Echtzeit KI-gestützt ausgewertet und lagegerecht dargestellt. Damit können in verbundenen Kampfverbänden Bewegung, Zielerfassung und Feuerkraft synchronisiert und die Gefechtswirksamkeit mechanisierter Verbände erheblich gesteigert werden. Die schnelle Verarbeitung und Bereitstellung von Daten besatzungsloser Luft-, See- und Bodenfahrzeuge erhöhen die operationelle Transparenz.

Battlesuite gleich App Store

Die Battlesuite ist der App Store, in dem die Anwendungen zur Realisierung der unterschiedlichen Funktionen bereitgestellt werden. Die Apps sind zum Teil von Rheinmetall eigens entwickelt. Es werden aber Applikationen strategischer Partner eingebunden. Die Apps kommunizieren mit dem Tactical Core über Programmierschnittstellen (Application Programming Interface, API). An dieser Stelle überprüft Rheinmetall die Einhaltung der vorgegebenen technischen Standards und ob nicht zulässige Kommunikation stattfindet.

Die Battlesuite wird ebenengerecht konfiguriert und macht dem jeweiligen Nutzer die Funktionen für eine optimale Aufgabendurchführung verfügbar.

Die modulare Lösung ermöglicht nahtlose Interoperabilität zwischen heterogenen Systemen, unabhängig vom Alter, technologischem Standard oder Hersteller. Dabei schützt der mehrschichtige Ansatz kritische Daten und Kommunikationskanäle. Die KI-basierte Plattform fungiert dabei als taktischer Datennebel, der Daten sammelt, speichert, synchronisiert und allen Anwendungen präsentiert – unabhängig von einzelnen Applikationen und der aktuellen System- und Netzwerkstruktur. Die Rheinmetall-Lösung ist darauf ausgelegt, nahtlos in Multi-Security-Domain-Umgebungen zu operieren.

Stand des Projekts

Ab Mitte 2026 soll die Battlesuite verfügbar sein, um Tests durch den Auftraggeber durchzuführen. Zu Ende des Jahres erwartet Rheinmetall, dass die Battlesuite für die Nutzung freigegeben wird. Erste Anwendung soll die Battlesuite in der soeben in Dienst gestellten Panzerbrigade 45 „Litauen" finden.

Souveräne Digitalisierung als Basis eines handlungsfähigen Verteidigungssektors

Als verlässlicher Partner der Bundeswehr und der deutschen Rüstungsindustrie liefern wir sichere, innovative und einsatzfähige IT-Systeme.

- Expertise in komplexen Architekturen und Prozessen der Bundeswehr, EU und NATO
- Führend in den Bereichen Cybersicherheit und KI
- Starkes Partnernetzwerk mit Fokus auf Souveränität und Innovation
- Erfahrung im Einsatz von Data und AI für Unternehmen in dynamischen Märkten

Weitere Infos: www.materna.de/bw

MATERNA

©MRV/Socrates Tasso (2)

Dirk Walther (l.) mit HHK-Chefredakteur Michael Horst am Stand von ND SatCom auf der AFCEA Fachausstellung.

Produkte und Lösungen von ND SatCom sind „military approved“ und können definitiv im Einsatz bestehen!

Interview mit Dirk Walther, Leiter Geschäftsbereich Defence der ND SatCom GmbH

Sehr geehrter Herr Walther, zuverlässige und sichere Kommunikationsverbindungen sichern den militärischen Erfolg. Was zeichnet Ihre Produkte im Wesentlichen aus?
Unsere Produkte und Lösungen zeichnet neben technologischer Exzellenz eine sehr hohe Zuverlässigkeit aus. Gerade für militärische Anwendungen ist es von hoher Relevanz, dass die Lösung im Einsatz besteht und zuverlässig funktioniert. Hierauf wird bei ND SatCom stets großer Wert gelegt, ebenso wie auf die Feldverwendungsfähigkeit. Unsere Produkte sind „military approved“ und bestehen auch in herausfordernden Umgebungen sicher.

Sind Ihre Produkte „kriegstauglich“ und gibt es hinsichtlich des Einsatzspektrums besondere Einschränkungen?
Die Produkte und Lösungen von ND SatCom sind, wie in der vorangegangenen Antwort skizziert, „military approved“ und können definitiv im Einsatz bestehen. Dies selbstverständlich in definierten Szenarien und Gefechtsstandumgebungen – ein Satellitenterminal verfügt für sich selbst genommen natürlich nicht über einen wirksamen Schutz gegen feindlichen Beschuss oder – noch aktueller – gegen feindliche Drohnenbedrohung.

Konnten die Erfahrungen aus den aktuellen Kriegen in Ihre Produkte einfließen? Kommen Ihre Systeme weltweit zum Einsatz?
Erfahrungen aus laufenden kriegerischen Auseinandersetzungen fließen bei uns laufend in den Produktentwicklungsprozess ein, ebenso wie konkrete, aktuelle Anforderungen unserer militärischen Kunden. Die Kunden der Business Unit Defence der ND SatCom sind dem europäischen NATO-Bereich zuzuordnen – der europäische Bereich der wertebasierten Grundordnung sozusagen.

Die ND SatCom GmbH ist für besonders innovative Lösungen bekannt. Was bieten Sie dem interessierten Publikum auf der AFCEA in diesem Jahr?
Dieses Jahr stellen wir die motorisierte Variante unseres Multiband FlyAway Terminals, das MFT 1500 X

Motorized, vor. Die Motorisierung ermöglicht durch die automatische Ausrichtung und Satellitenverfolgung eine schnelle Einsatzbereitschaft, da die Antenne in weniger als einer Minute und mit minimalem Personalaufwand präzise ausgerichtet werden kann. Dies reduziert die Rüstzeit erheblich und ermöglicht eine nahezu sofortige Herstellung einer stabilen Kommunikationsverbindung – ein entscheidender Vorteil bei zeitkritischen Einsätzen.
Neben der Motorisierung ist das MFT 1500 X Motorized auch multi-orbitfähig und kann in geostationären und nicht-geostationären Orbits eingesetzt werden, was eine hohe Flexibilität bei der Auswahl der Satellitensysteme bietet. Diese Vielseitigkeit macht es ideal für den Einsatz in abgelegenen Gebieten, bei Katastropheneinsätzen oder in militärischen Operationen, wo terrestrische Netzwerke unzuverlässig oder nicht verfügbar sind. Der modulare Aufbau des Systems erleichtert Wartung und Reparaturen, während der integrierte logistische Support von ND SatCom sicherstellt, dass Kunden weltweit von einer zuverlässigen Versorgung und technischem Support über den gesamten Lebenszyklus profitieren.
Darüber hinaus ist das System so konzipiert, dass es unter extremen Umgebungsbedingungen betrieben werden kann. Die robuste Bauweise, kombiniert mit der leichten und modularen FlyAway-Technologie, ermöglicht einen schnellen Transport und Aufbau, was das Terminal besonders für mobile Kräfte attraktiv macht. Ob für Echtzeit-Datenübertragung, Sprachkommunikation oder Videoübertragung – das MFT 1500 X bietet eine skalierbare und sichere Kommunikationslösung, die sich an die spezifischen Bedürfnisse der Kunden anpassen lässt.

Welche innovativen Techniken kommen in Ihrem Kernprodukt SKYWAN bei der Nutzung und der Abwehr von Bedrohungen aus dem Cyberraum zur Wirkung?
Im Bereich der Satellitenkommunikation ist SKYWAN eine Technologie mit einem hohen Ansehen bei Regierungs- und Militärkunden. Das Hauptmerkmal der SKYWAN-Technologie ist deren Aufbau auf der Mesh- und Hubless-Topologie, welche eine direkte Verbindung zwischen verschiedenen Stationen im Netzwerk ermöglicht, unabhängig von ihrem Standort und ohne fester Hub-Station. Dies ermöglicht eine effiziente Kommunikation zwischen verschiedenen Teilen des Netzwerks und stellt sicher, dass die Kommunikation auch dann fortgeführt werden kann, wenn ein oder mehrere Stationen nicht verfügbar sind.
SKYWAN bietet außerdem sowohl COMSEC (Kommunikationssicherheit) als auch TRANSEC (Übertragungssicherheit) zum Schutz vor Abhör- und Überwachungsversuchen. COMSEC gewährleistet, dass die Inhalte der Kommunikation sicher sind, während TRANSEC dafür sorgt, dass die Kommunikation selbst vor Abhörversuchen geschützt ist. Durch die Unterstützung von Mesh- und Hubless-Topologie, COMSEC und TRANSEC ermöglicht SKYWAN eine effiziente Kommunikation, schützt vor Abhör- und Mithörversuchen und gewährleistet die Kontinuität des Betriebs auch unter widrigen Bedingungen.

AFCEA Fachausstellung 2025

Dabei ermöglicht das in SKYWAN implementierte softwaredefinierte Funkgerät (SDR), sich durch Anpassung auf geänderte Bedrohungslagen und Anforderungen einzustellen. Das bietet unseren Kunden Zukunftssicherheit, da sich die bestehende Infrastruktur ohne größere Investitionen um neue Funktionen und Fähigkeiten erweitern lässt.

Die AFCEA Bonn e.V. hat sich zu den etabliertesten Dialogplattformen für die IT- und Kommunikationsbranche entwickelt. Sind Sie zufrieden mit dem Interesse der zivilen und besonders militärischen Besucher?
Wir sind mit der diesjährigen AFCEA sehr zufrieden! Spätestens am späten Vormittag des ersten Tages war uns klar, dass mit einem sehr hohen Besucherandrang zu rechnen ist, wurde doch die Warteschlange im Eingangsbereich immer länger. Die hohe Besucherfrequentierung an unserem Stand – natürlich vorrangig potenzielle Kunden aus dem militärischen Umfeld – hielt dann auch tatsächlich bis zum Ende des zweiten Tages an. Insofern war die AFCEA – gemessen am Besucherinteresse – ein voller Erfolg.

Sehr geehrter Herr Walther, vielen Dank für die interessanten Informationen und weiterhin viel Erfolg besonders bei der Realisierung der innovativen Lösungen.

Auf der diesjährigen AFCEA Fachausstellung präsentierte ND SatCom sein motorisiertes Terminal MFT 1500 X.

AFCEA Bonn e. V. lädt zum ersten Bonner IT-Dialog am 1. Oktober 2025

Kriegserklärung übersehen?

Die Rolle des Zentrums Digitalisierung der Bundeswehr im Umgang mit hybriden Bedrohungen

Die aktuelle Bedrohungslage ist ernst. Als Seiteneffekt zum Krieg in der Ukraine erleben wir die harte Realität eines hybriden Konflikts in Europa, der weit über die Grenzen des Gefechtsfeldes hinausgeht. Cyberangriffe, Desinformation und die Manipulation kritischer Infrastrukturen sind längst Realität – auch in Europa und in Deutschland.

Globale Vernetzung und technologischer Fortschritt verstärken die Möglichkeiten hybrider Kriegsführung und stellen uns vor neue Herausforderungen. Die Bedrohung ist allgegenwärtig und erfordert ein breites Bewusstsein in der Bevölkerung sowie eine resiliente und interoperable NATO.

©MRV/Socrates Tasso (3)

Von der Bedarfsdecker- zur Bedarfsträger-Perspektive: Auf die AFCEA Fachtagung folgt der Bonner IT-Dialog.

Wie können wir uns schützen?

Haben wir als AFCEA im Rahmen der Koblenzer IT-Tagung in den letzten Jahren die Sicht des Bedarfsdeckers BAAINBw betrachtet, ist es nun an der Zeit, die zukünftigen Planungen und Programme aus Sicht der Bedarfsträger mithilfe des Zentrums Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) in den Fokus zu rücken. Hierfür bietet das neue Format „Bonner IT-Dialog" eine Plattform. Experten aus Militär, Industrie, Forschung und Zivilgesellschaft diskutieren über aktuelle Herausforderungen und innovative Lösungsansätze:

- Zukunftsweisende Technologien: Aussteller und Bundeswehr präsentieren innovative Technologien zur Abwehr hybrider Bedrohungen.
- Die Rolle des ZDigBw: Erfahren Sie, wie das Zentrum die Digitalisierung der Streitkräfte vorantreibt und zur Stärkung der Cyberabwehr beiträgt.
- Vorhaben der Bundeswehr: Informieren Sie sich über aktuelle Projekte und Strategien der Bundeswehr im Bereich der hybriden Kriegsführung.
- Impulse von hochrangigen Speakern: Gewinnen Sie exklusive Einblicke von führenden Experten aus Politik, Militär und Wissenschaft.
- Hybride Bedrohungen: Diskutieren Sie mit, wie Deutschland und das Zentrum Digitalisierung der Bundeswehr auf mögliche hybride Bedrohungen vorbereitet sind und welche Maßnahmen ergriffen werden.

Seien Sie dabei und gestalten Sie die Zukunft der Sicherheit mit! *(AFCEA)*

©MRV

Kontakt:
Stephanie Balk
Key Account Managerin
Conrad Electronic SE
Klaus-Conrad-Str. 1
92240 Hirschau
stephanie.balk@conrad.de
www.conrad.de

Conrad Electronic: Ihr zuverlässiger Partner für Technik – seit über 100 Jahren
Seit 1923 steht Conrad für Qualität und Innovation. Heute bieten wir als Sourcing Platform über zehn Millionen Produkte und Services für Geschäftskunden, Behörden und die Bundeswehr. Einkaufsverantwortliche und Bedarfsträger aus Facility Management, Logistik, MRO oder Fuhrpark decken so ihren gesamten technischen Bedarf aus einer Hand und profitieren von maßgeschneiderten E-Procurement-Lösungen.

Unsere Highlights auf der AFCEA 2025:
- Bambu Lab X1E 3D-Drucker: Schnelle Fertigung von Ersatzteilen und Prototypen mit Hochleistungsmaterialien,
- Parat Ladekoffer: Schutz für sensible Elektronik und mobile Ladestation für Kommunkationstechnik,
- iSafe MOBILE-Geräte: Robuste und sichere Kommunikation selbst in extremen Umgebungen.

Für mehr Autonomie, Sicherheit und Effizienz der Truppe.


© Michael Horst

Kontakt:
ND SatCom GmbH
Graf-von-Soden-Strasse
88090 Immenstaad
Deutschland
Email: info@ndsatcom.com
Tel.: 07545 / 939-0
www.ndsatcom.com

MULTI-BAND FLYAWAY TERMINAL MFT 1500 X Motorized

Das Beste aus zwei Welten –
Taktische Mobilität trifft auf strategische Stabilität!

Das MFT 1500 X vereint zwei entscheidende Eigenschaften in einem System:
- Die Flexibilität einer FlyAway-Antenne – schnell verlegbar, kompakt und für minimalen Personalaufwand konzipiert.
- Die Stabilität einer Deployable Groundstation – robust, wetterfest und für den Langzeiteinsatz ausgelegt.

Perfekt für den Einsatz in mobilen Kommando- und Kommunikationsinfrastrukturen – sei es im Feldlager, im Headquarter oder bei temporären Operationen.

Technologie, die sich bewegt. Verbindung, die bleibt.

Nachgefragt bei …

Marcel Taubert, Vice President Defence & Space der secunet Security Networks AG

HHK-Chefredakteur Michael Horst im Gespräch mit Marcel Taubert von secunet (r.).

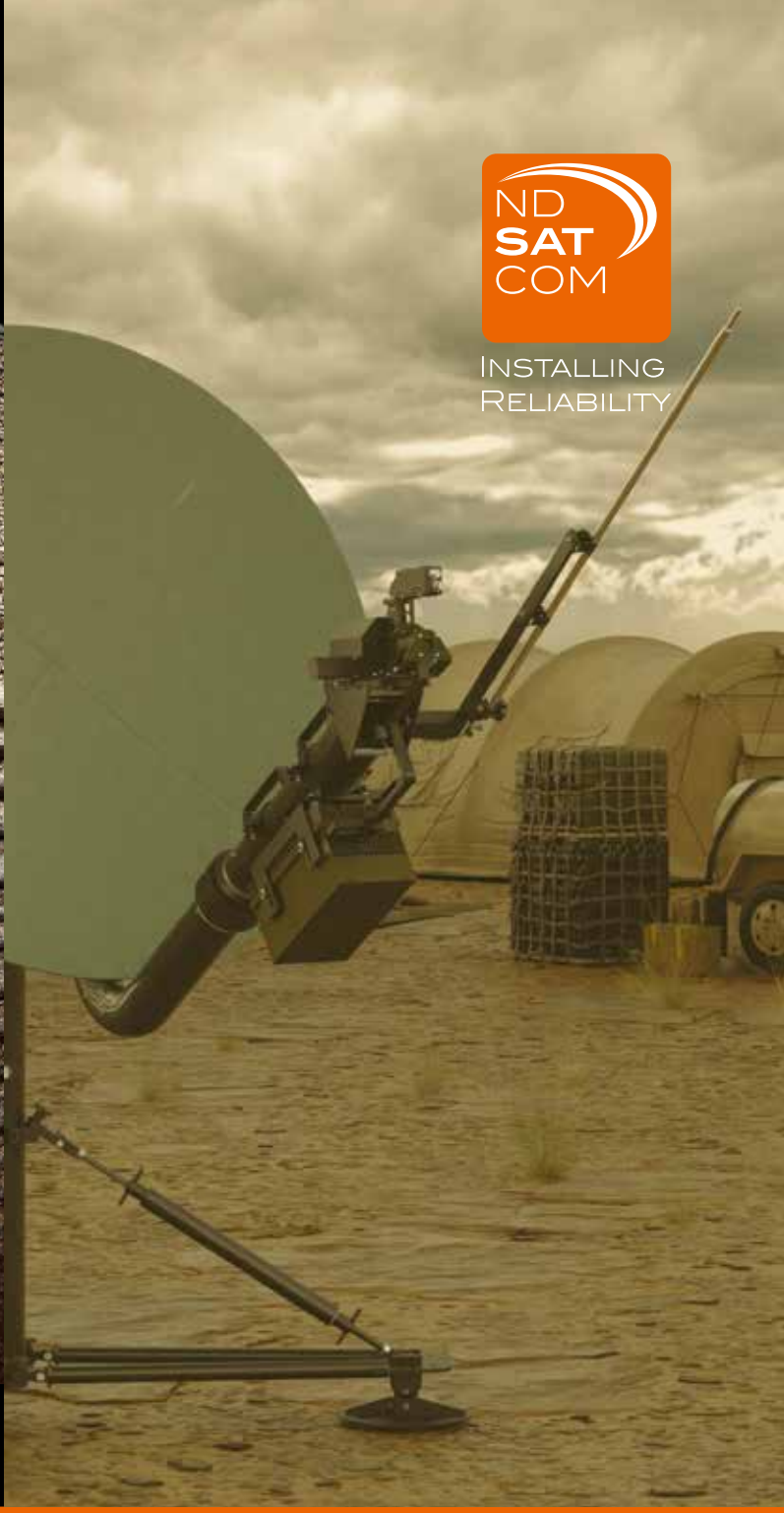
Sehr geehrter Herr Taubert, digitale Infrastrukturen müssen widerstandsfähig, flexibel und zukunftssicher sein. Inwiefern ermöglichen Ihre Lösungen digitale Anwendungen im Hochsicherheitsbereich?
Unser Portfolio dient als zentraler Enabler der Digitalisierung, indem es flexible, sichere Anwendungen über unterschiedliche Sicherheitsdomänen und Informationsräume hinweg ermöglicht. Von nicht eingestuften Anwendungsfällen über VS-NfD bis hin zu GEHEIM sowie den entsprechenden NATO- und EU-Klassifizierungen bieten wir Lösungen, die höchsten Sicherheitsanforderungen gerecht werden.
Unsere Plattformen kommen in kritischen Infrastrukturen, beispielsweise auch bei europäischen Satellitenprojekten, sowie in hochsensiblen militärischen Szenarien der Bundeswehr zum Einsatz und werden durch das BSI, europäische Partnerbehörden und die SECAN (Anm. Red.: NATO Information Security and Evaluation Agency) zugelassen. Besonderen Fokus legen wir auf Flexibilität und Mobilität, weshalb Teile unseres Portfolios auch unter militärischen Bedingungen einsetzbar und speziell gehärtet sind.

Welche Lösungen präsentieren Sie auf der AFCEA und wozu werden diese genutzt?
Wir zeigen hier unser umfassendes Produktspektrum von mobilen Lösungen zur VS-Kommunikation auf iOS- und Android-Basis bis hin zu hochsicheren Systemen für den GEHEIM-Bereich. Unsere Technologien bilden das Rückgrat sicherer Kommunikationsnetze, wie etwa des German Mission Network. Ein Highlight ist die SINA Cloud, die bis GEHEIM eingesetzt werden kann. Sie bildet zugleich einen zentralen Ankerpunkt für das SINA-Portfolio, denn eine sichere Cloud erfordert sichere Plattformen als Basis. Ergänzt durch ein Managementsystem zur übergreifenden Administration, erlaubt diese Architektur einen skalierbaren, domänenübergreifenden Einsatz.
Mit Blick auf künftige Operationskonzepte leistet die SINA Cloud einen Beitrag zur Multi-Domain Capability: Sie ermöglicht die Verarbeitung, Bereitstellung und Weitergabe eingestufter Informationen über unterschiedliche Sicherheits- und Operationsdomänen hinweg – ob in stationären, mobilen oder verteilten Szenarien. Sie bildet damit das Fundament vernetzter Operationsführung, wie sie im Rahmen moderner C4ISR-Strukturen und des Paradigmas „Software Defined Defence“ zunehmend gefordert wird.

Wie können Ihre Produkte zur „Kriegstauglichkeit“ Deutschlands beitragen und welche Rolle spielt dabei das Konzept der Informationsüberlegenheit im Rahmen Ihrer Sicherheitslösungen?
Militärische Überlegenheit basiert heute zunehmend auf der Fähigkeit, Informationen schnell und sicher zu verarbeiten sowie effektiv zu nutzen. Die alte Maxime „Wer schneller schießt und besser trifft, gewinnt den Feuerkampf“ gilt unverändert. Entscheidend ist dabei die Informationsüberlegenheit, da sie die Basis für Führungs- und schließlich Wirkungsüberlegenheit bildet. Genau hier setzen unsere SINA-Lösungen an: Sie gewährleisten die sichere Verarbeitung und Übermittlung kritischer Informationen – auch in komplexen und hybriden Bedrohungsszenarien. So schaffen wir die Voraussetzungen dafür, dass militärische Führung ihre Überlegenheit behaupten und weiter ausbauen kann.

Mit welchen innovativen Technologien ermöglichen Ihre Lösungen schon heute den sicheren Einsatz sensibler Anwendungen wie KI, und wie trägt dies zur langfristigen digitalen Souveränität militärischer und ziviler Institutionen bei?
Mit der Integration von Post-Quanten-Kryptografie ist unser Produktportfolio bereits heute auf zukünftige Cyberbedrohungen vorbereitet. Zudem bieten wir mit unserer Technologie die Möglichkeit, KI-Anwendungen sicher auch mit GEHEIM-klassifizierten Daten einzusetzen. Damit ermöglichen wir neue operative Möglichkeiten im Hochsicherheitsbereich und stärken zugleich die langfristige digitale Souveränität militärischer sowie ziviler Institutionen in Deutschland und Europa. Unsere Lösungen stehen somit für eine proaktive Gestaltung digitaler Sicherheit und Souveränität, die Informationsüberlegenheit nicht nur absichert, sondern strategisch nutzbar macht.

Herr Taubert, herzlichen Dank für das Gespräch.



NDSATCOM

INSTALLING RELIABILITY

www.ndsatcom.com

MFT 1500 X MOTORIZED – DAS BESTE AUS ZWEI WELTEN

- FLEXIBEL UND ROBUST
- LANGLEBIG UND LEISTUNGSFÄHIG
- ZUGLEICH MULTI-ORBIT-FÄHIG

Technologie, die sich bewegt. Verbindung, die bleibt.

©MRV/Socrates Tassos (3)

Hardthöhen-KURIER

FÜR EIN STARKES EUROPA

Das Team des **Hardthöhenkuriers** bedankt sich bei den Organisatoren der AFCEA Bonn e.V. sowie den Ausstellern und Besuchern der Fachausstellung 2025 sehr herzlich für ihre Unterstützung und ihr Interesse!

©privat

Vielen Dank wiederum an unseren Fotografen Socrates Tassos für seine professionelle Arbeit!