AFCEA 2018

Fraunhofer FKIE

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

ISBN 978-3-934401-46-4

BWI
IT für Deutschland

IT für Deutsch-land

BWI: Ihr Partner für die Digitalisierung der Bundeswehr

Die BWI hat die IT der Bundeswehr zu einem standardisierten und zentralisierten IT-System umgebaut, das bereits heute durch seine Leistungsfähigkeit überzeugt. Und die nächste Phase hat schon begonnen.

Als Innovationstreiber entwickeln wir das bestehende System weiter und weiter. Wir analysieren Trends, stellen neue Technologien auf den Prüfstand und überführen sie in konkrete Lösungen für die Bundeswehr-IT: von der „Bundeswehr-Cloud" bis zur sicheren virtuellen Desktop-Infrastruktur. Als IT-Systemhaus der Bundeswehr verstehen wir Ihre Herausforderungen in allen Bereichen und haben die passenden Lösungen schon parat – von der IT-Beratung über die Umsetzung bis hin zum sicheren Betrieb innovativer Lösungen.

@BWI_IT
/BWIITfuerDeutschland
blog.bwi.de

Erfahren Sie mehr
www.bwi.de

Klaus Hardy Mühleck

Foto: BMVg CIT

Sehr geehrte Damen und Herren,

mit Aufstellung der Abteilung Cyber und Informationstechnik zum 01. Oktober 2016 wurde mir die Verantwortung für die Ausgestaltung der Cyber- und Digitalpolitik, die Gewährleistung der Übereinstimmung des IT-Einsatzes mit den politischen, strategischen und operativen Zielen des Ressorts und den IT-Festlegungen der Bundesregierung sowie die Zukunftsentwicklung/ Weiterentwicklung von Cyber/IT-Fähigkeiten übertragen. In diesem ersten Jahr der Abteilung sind so viele erwähnenswerte Aktivitäten gestartet und auch schon erfolgreich durchgeführt worden, dass eine Aufzählung und Darstellung dieses Heft alleine füllen könnte.
Mit Blick auf die vielfältigen Aktivitäten und unter Berücksichtigung sowohl der technologischen Entwicklung als auch des Gefährdungspotentials im „world wide web“ möchte ich hier zwei Aspekte hervorheben, die mir besonders am Herzen liegen und die wir in den Fokus unserer Anstrengungen nehmen.
Da ist zum einen die Verbesserung des Beitrages der Bundeswehr zur gesamtstaatlichen Cybersicherheitsvorsorge und den Aufbau einer wirksamer Cyberverteidigung, insbesondere auch der Systeme im Einsatz. Cybersicherheit und Cyberverteidigung steht im Fokus unserer Maßnahmen. Dies fängt bei den Überlegungen zur Entwicklung neuer Produkte, bspw. unter Berücksichtigung des leitenden Prinzips „security by design“ an und mündet in der konkreten Umsetzung im Cybersicherheitszentrum oder Anwendung im Zentrum Cyberoperationen. Cybersicherheit lässt sich aber nicht alleine und isoliert erreichen, sie ist als permanente gesamtstaatliche Aufgabe gemeinsam zu verstehen und zu bewältigen. Wir müssen dies aktiv mit unseren Partnern in den Bündnissen aber auch gemeinsam mit Politik, Industrie, Wirtschaft und Gesellschaft angehen und gestalten. Der ressortübergreifenden Zusammenarbeit kommt hier eine besondere Rolle zu. Im Rahmen der Cybersicherheitsstrategie 2016 wurde beispielsweise der Ausbau eines gemeinsamen Cyberabwehrzentrums betont, als ein Element einer modernen Cyber-Sicherheitsarchitektur. Darüber hinaus gilt es, auf den Schutz kritischer Infrastrukturen erhebliche zusätzliche Anstrengungen zu legen, wie es uns Beispiele aus dem gar nicht so weit entfernten Geschehen der jüngeren Geschichte deutlich aufzeigen. Die Bundeswehr kann hier mit Kräften und Mitteln beitragen, wenn die entsprechenden Voraussetzungen geschaffen werden.
Als zweite zentrale Herausforderung für den Geschäftsbereich des BMVg möchte ich die Digitalisierung ansprechen. Die Digitalisierung ist in nahezu allen Bereichen des Lebens angekommen und treibt Veränderungsprozesse mit rasanter Geschwindigkeit voran. Dies können und dürfen wir in der Bundeswehr weder negieren noch ignorieren. Sie ist zum Motor der Transformation zu einer „Digitalen Gesellschaft“ geworden. Informationstechnik ist dabei sowohl ein Werkzeug, um Prozesse zu unterstützen und innovative Geschäftsmodelle zu entwerfen, als auch Abläufe und Organisationsformen einschließlich der dazugehörigen Kultur zu ermöglichen, neu zu gestalten und dadurch einen Mehrwert für die Organisation zu erzielen. Auf Informationen kann zunehmend ortsunabhängig, mobil und nahezu in Echtzeit zugegriffen werden. Reale und virtuelle Welt rücken immer näher zusammen und erreichen einen immer höheren Grad der digitalen Vernetzung. Damit eröffnen sich ungeahnte Chancen für Gesellschaft und Staat und natürlich auch für die Bundeswehr als Armee im Einsatz und lernende, sich stetig weiterentwickelnde Organisation. In den vergangenen Monaten wurden bereits viele Einzelinitiativen zur Digitalisierung gestartet. Diese gilt es zu harmonisieren, zu steuern und so zielgerichtet die Digitalisierung der Bundeswehr voranzutreiben. Die Bundesministerin der Verteidigung hat noch im Dezember entschieden unter ihrer Leitung ein Leitungsboard Digitalisierung einzurichten, in dem diese Steuerungsaufgaben wahrgenommen werden sollen. Dadurch wird deutlich, dass Digitalisierung mehr ist als nur eine Frage der Technologie: es geht um die Änderung der Denk- und Handlungsweise, um das „Digitale Selbstverständnis der Bundeswehr“.
Ich gebe aber auch zu, das nicht alles was wir uns vorgenommen haben, bereits realisiert ist oder sich in der Realisierung befindet. Bei einem „Supertanker“ wie der Bundeswehr aus voller Fahrt die Richtung zu verändern ist nur mit langem Atem und über eine große Distanz möglich. Ich bin aber überzeugt, dass wir die richtigen Wege beschrieben und die richtigen Maßnahmen eingeleitet haben.
Die AFCEA Bonn in Unterstützung mit dem Behörden Spiegel hat insbesondere durch die Publikation dieser Sonderausgabe, der Jahresthemensetzung als auch mit der Organisation und Durchführung der Fachausstellungen und vielen weiteren Veranstaltungen in den vergangenen Jahren immer wieder wertvolle Beiträge zur Information im Bereich der Entwicklung von Informations- und Kommunikationstechnologien, zur Diskussion angeregt und Beiträge zur Weiterentwicklung in der Bundeswehr geleistet. Dafür spreche ich meinen Dank und Anerkennung aus. Ich wünsche den Lesern bei der Lektüre dieses Heftes über die einzelnen Beiträge wertvolle Einblicke in die aktuellen und zukünftigen Entwicklungen und freue mich auf interessante Gespräche mit Ihnen auf den kommenden Veranstaltungen.

Ihr Klaus Hardy Mühleck,
Abteilungsleiter Cyber/Informationstechnik (CIT), BMVg

AFCEA 2018

1. AFCEA Bonn e.V. – Digitale Zukunft gestalten!

2. Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

3. AFCEA-Fachausstellung

Impressum: Sonderheft Behörden Spiegel „AFCEA 2018“ **Redaktionelle Leitung:** Reimar Scherz, Behörden Spiegel, Telefon: 0228 / 970 97-83 **Herausgeber** (presserechtlich verantwortlich): R. Uwe Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Berlin/Bonn **Anzeigen:** Beatrix Lotz, Helga Woll **Herstellung:** Spree Service- und Beratungsgesellschaft mbH, Berlin **Satz und Layout:** Susan Wedemeyer, Behörden Spiegel **Fotos:** Autoren, AFCEA Bonn e.V., Fraunhofer FKIE, Behörden Spiegel Archiv **Druck:** KÖLLEN DRUCK & VERLAG GMBH, Bonn **Heftpreis:** 7,50 Euro

Blicken wir gemeinsam nach vorne!

Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V.

Erich Staudacher
Generalmajor a.D.

Foto: Privat

Innere und äußere Sicherheit sind der Schlüssel auch zur digitalen Souveränität Deutschlands, das hat AFCEA Bonn e.V. in seinen Veranstaltungen im Jahr 2017 bereits dargelegt. Dieses Thema lässt uns auch 2018 nicht los, die Digitalisierung aller Lebensbereiche, auch der für die Sicherheit relevanten, schreitet mit rasanter Geschwindigkeit voran. AFCEA blickt deshalb wiederum nach vorne: Die Digitale Zukunft gilt es zu gestalten – und zwar intelligent, vernetzt und sicher!

Denn bei den neuen technischen Lösungen für die öffentliche Verwaltung geht es nicht mehr nur um reine Vernetzung, sondern auch um die sichere Nutzung und andere gemeinsame Gestaltungsfelder der Zukunft. Vor allem intelligente und autonome Systeme bieten neue Chancen, bergen aber auch neue Herausforderung. Aktuelle Entwicklungen und Innovationen werden zudem längst nicht mehr durch den Bedarf staatlicher Institutionen bestimmt. Militär und andere Bereiche der öffentlichen Sicherheit müssen sich den stattfindenden und bereits stattgefundenen Entwicklungen stellen, Wissen aufholen und neue Kompetenzen erwerben.

Zudem wirken auf Streitkräfte und Sicherheitsbehörden durch die Digitalisierung und Automatisierung, im Friedensbetrieb wie im Einsatz, massive Veränderungen, sei es in der Führung, in der Aufklärung, beim Waffeneinsatz oder in der Logistik. Einschlägige technische Entwicklungen etwa bei den sozialen Medien oder im Bereich der Künstlichen Intelligenz sind Treiber gesellschaftlicher Veränderungen geworden, die vom Staat schleunigst eine neue Rolle in regulatorischer Hinsicht als auch in der Förderung disruptiver Technologien abverlangen. Wie bekannt, können Manipulationen in den Sozialen Medien massiven Einfluss auf demokratische Entscheidungen haben. Aber was heißt hier schon „der Staat“? Nur durch eine institutionen- und nationenübergreifende Zusammenarbeit und einen neuen gesellschaftlichen Konsens wird es gelingen, solche Entwicklungen nicht nur zu erleiden, sondern gestalterisch in die richtigen Bahnen zu lenken – intelligent, vernetzt und sicher.

AFCEA Bonn e.V. ist es deshalb ein Anliegen, mit dem Jahresthema „Digitale Zukunft gestalten – Intelligent. Vernetzt.

AFCEA Vorstand und Aufgaben

Geschäftsführender Vorstand

Erich Staudacher, Vorsitzender

Armin Fleischmann, Stv. Vorsitzender, Vorsitzender Programmbeirat

Joachim Mörsdorf, Stv. Vorsitzender und Vertreter Industriebeirat

Hans-Ulrich Schade, Vertreter Beirat BMVg und CIR

Katja Frintrop, Vertreterin Arbeitskreis Young AFCEANs

Christian Hartrott, Geschäftsführer, Schatzmeister, Veranstaltungsmanagement

Weitere Mitglieder

Friedrich W. Benz, Beauftragter Fachausstellung

Andreas Höher, Vertreter Arbeitsgruppe Öffentliche Sicherheit & eGovernment

Franz Bernd Möllers, Sekretär Programmbeirat

Dr. Ansgar Rieks, Vertreter Beirat Streitkräfte

Jochen Reinhardt, Vertreter Arbeitskreis Medien, Pressesprecher

Tobias Schönherr, Vertreter Arbeitskreis Berlin

Götz Stuck, Schriftführer

Wolfgang Taubert, Vertreter Arbeitsgruppe Internationales

Dr. Michael Wunder, Vertreter Beirat Wissenschaft

AFCEA Bonn e.V. ergänzt seine Vorstandsarbeit um thematische Beiräte. Sie stellen jeweils einen Vertreter im Vorstand. Damit will sich die neutrale Informationsplattform besser auf den Austausch mit ihren Mitgliedern konzentrieren und eine bessere Informationsaufbereitung in den Kernthemen erreichen. Zu den Beiräten gehören die Gremien Programmbeirat, der Industriebeirat, der Arbeitskreis Young AFCEANs sowie die Jury des AFCEA Studienpreises.

Sicher.“ seiner traditionellen Rolle als Plattform für die Kommunikation auf diesem Feld mit den federführenden Stakeholdern in Deutschland, als Teil einer internationalen Organisation auch darüber hinaus gerecht zu werden. Wie immer, bildet dabei die Unterstützung der Bundewehr und anderer sicherheitsrelevanter Institutionen in Deutschland der Kern unseres gemeinnützigen Handelns.

Mit dem Thema setzen sich selbstverständlich auch die 32. AFCEA Fachausstellung und das Symposium auseinander. Die traditionelle Einladung an Sie, liebe Leserinnen und Leser, sich in der Diskussion mit uns zu diesem zukunftsweisenden Thema zu beteiligen, möchte ich bekräftigen: Machen Sie mit, helfen Sie mit, unser Land in der Digitalisierung zukunftsfähig zu gestalten. Lassen Sie uns dazu nach vorne blicken!

Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher.

Jochen Reinhardt, Pressesprecher BWI GmbH und Presseangelegenheiten AFCEA Bonn e.V.

Jochen Reinhardt

Foto: BWI/Müller

Das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) Bonn e.V. ist ein Verein ohne kommerzielle und politische Interessen mit über 900 persönlichen und mehr als 90 Firmenmitgliedern. Der deutsche Verein geht auf die Initiative von Angehörigen der Streitkräfte zurück, die 1983 den Austausch rund um Informations- und Telekommunikationstechnik (ITK) im Verteidigungs- und Sicherheitsbereich fördern wollten – immer getreu des eigenen Leitspruches: Mehr Wissen teilen!

Die dazu gehörenden Veranstaltungen eines jeden Jahres stellt AFCEA Bonn e.V. unter ein einheitliches Thema und versucht damit, die wichtigsten IT-Trends und Entwicklungen von allen Seiten zu betrachten. 2018 blickt AFCEA Bonn e.V. nach vorne: „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher." Längst geht es bei neuen technischen Lösungen für die öffentliche Verwaltung nicht mehr nur um Sicherheit und Vernetzung. Intelligente und damit autonome Systeme werden dabei immer häufiger gefordert. Die Entwicklungen wird längst nicht mehr durch den Bedarf der Landes- oder Bündnisverteidigung definiert, das Militär und andere Bereiche der öffentlichen Sicherheit müssen sich den bestehenden Entwicklungen stellen und Wissen aufholen. Maßgebliche technische Entwicklungen wie etwa soziale Medien sind Treiber gesellschaftlicher Entwicklungen geworden, die vom Staat eine neue normsetzende Rolle abverlangen, der dieser Entwicklung erst noch gerecht werden muss. Gleichzeitig entwickeln Manipulationen in den Sozialen Medien massiven Einfluss auf demokratische Entwicklungen.

Intelligent: Künstliche Intelligenz und autonome Maschinen werden den Staat stärker fordern, sowohl in regulatorischer Hinsicht als auch in der Förderung disruptiver Technologieentwicklungen. Wer immer einen Durchbruch bei der Entwicklung künstlicher Intelligenz erzielt, wird nach Ansicht des russischen Präsidenten Wladimir Putin künftig die Welt dominieren. Die Diskussion um die ethische Dimension des autonomen Fahrens ist hier nur ein Vorgeschmack der Entwicklung, bis im nächsten Schritt der Automatisierung beispielsweise durch Machine Learning ganze Branchen und das Arbeiten darin revolutioniert werden wird. Die USA ist in der Diskussion bereits etwas weiter: Intensiv beschäftigt man sich auf der internationalen Ebene mit der Entwicklung autonomer und intelligenter letaler Waffen – längst nicht nur technisch sondern auch mit der Frage der Folgen und in der Diskussion, ob und wie solche Waffen verboten werden sollten. Argumente für und wider kommen dabei nicht nur Vertretern aus Staat und Gesellschaft sondern besonders von Industrievertretern der Digitalisierung.

Vernetzt: Für Streitkräfte ist das Ziel der Vernetzung nichts Neues. „Network Centric Warfare" – bei der Bundeswehr als „Vernetzte Operationsführung (NetOpFü)" eingeführt – soll durch die Vernetzung von Aufklärungs-, Führungs- und Wirksystemen Informationsüberlegenheit herstellen und somit eine teilstreitkräfteübergreifende Überlegenheit in der gesamten Reichweite militärischer Operationen garantieren. Laut Konzeption der Bundeswehr von 2004 müssen die Streitkräfte zur effizienten Durchführung von Einsätzen im multinationalen Rahmen unter den Bedingungen des Informationszeitalters zur NetOpFü befähigt sein. „Die Fähigkeit zur NetOpFü muss sich in allen Kategorien des Fähigkeitsprofils der Bundeswehr widerspiegeln. Wesentliche Voraussetzungen für erfolgreiche NetOpFü sind – neben der Realisierung der streitkräftegemeinsamen und interoperablen Vernetzung – schnelle Führungs- und Entscheidungsprozesse, die Fähigkeit zur Abwehr gegnerischer Informationsoperationen und klare politische, rechtliche sowie strategische und operative Vorgaben." Mit der heutigen Vernetzung und der Digitalisierung entwickeln sich sowohl die Möglichkeiten als auch die Herausforderungen nahezu exponentiell. War in den ersten Jahren netzwerkorientierter Operationen noch technologische Ressourcen eine Garantie für Informationshoheit, steht dank Sozialer Medien oder kostengünstiger und allgemeinverfügbarer Technologien eine vergleichbare Vernetzung auch in Zeiten asymmetrischer Bedrohungen quasi jedermann zur Verfügung.

Sicher: Das Thema ist für AFCEA nichts Neues: Bereits 2017 fokussierte der Verein mit dem Thema „Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität" auf die Grundlage eines digitalen Staats: Sicherheit. Mit der zunehmenden Digitalisierung und der Umsetzung aktueller Technologietrends wachsen die Bedrohungen hinsichtlich der Möglichkeiten digitaler Angriffe. Mit der „Industrie 4.0" geht aufgrund der zunehmenden Vernetzung ebenfalls die Notwendigkeit erhöhter Sicherheitsstandards einher. Gibt es so etwas wie „Sicherheit 4.0"? Die klassische Trennung zwischen innerer und äußerer Sicherheit ist in unserer vernetzten Welt nicht mehr durchgehend möglich.

Veranstaltungen 2018 AFCEA Bonn e.V.

„Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher.“ (April – Dezember 2018)

» 11./12. April
32. AFCEA Fachausstellung mit Symposium
„Digitale Zukunft gestalten – Intelligent.Vernetzt.Sicher.“

» 12. April
Leadership Forum Young AFCEANs

» 14. Mai
Parlamentarischer Abend, Berlin
„Digitalisierung Bundeswehr“

» 05. Juni
Gemeinsame Veranstaltung AFCEA Bonn e.V. mit dem Heer
„Digitalisierung im Heer“

» 14. Juni
AFCEA Fachveranstaltung mit Bitkom, CeBIT
„Künstliche Intelligenz – Chancen und Herausforderungen für innere und äußere Sicherheit“

» 21. Juni
Mitgliederversammlung AFCEA Bonn e.V.

» 09. August
Info-Veranstaltung Young AFCEANs, Berlin

» 30. August
Koblenzer IT-Tagung 2018
„Digitale Zukunft – Architekturen. Plattformen. Anwendungen“

» 13. September
Info-Veranstaltungen Young AFCEANs

» 26. September
Föderales IT-System – Vernetzte Verwaltung
„eGovernment und digitale Souveränität“

» 09./10. Oktober
Gemeinsame Veranstaltung AFCEA Bonn e.V. mit KdoCIR – CCF/ICOS

» 14. November
AFCEA Technologieforum beim Fraunhofer FKIE
„KI und Big Data zur Entscheidungsunterstützung“

» 23. November
AFCEA Mittagsforum mit ESG
„Herausforderung Digitalisierung: Verstehen – handeln – gemeinsam Mehrwert schaffen“

» 03. Dezember
AFCEA Fachveranstaltung
„Digitalisierung der Prozesse – Architekturen. Werkzeuge. Anwendungen“

CITquadrat – Weiterentwicklung des Teilportfolios Cyber/IT

Brigadegeneral Dr. Michael Färber,
Stv. Abteilungsleiter Cyber/Informationstechnik (CIT), BMVg

Dr. Michael Färber
Brigadegeneral

Foto: BMVg CIT

Vorbemerkung

Die Bundeswehr verfügt über eine hoch komplexe und dabei bisher ausgesprochen heterogene IT-Systemlandschaft. Deren Entwicklung erfolgte überwiegend in einzelnen Systemen; jedes System wurde dabei so entwickelt, dass es „quasi für sich allein" betriebsfähig war. Im Ergebnis ist die daraus resultierende Systemlandschaft heute durch eine Vielzahl sehr unterschiedlicher Strukturelemente charakterisiert, die vielfach in „Stove-Pipes" organisiert sind. Die Möglichkeiten einer ganzheitlichen Steuerung dieser Systemlandschaft sind stark eingeschränkt.

Die zukünftige Aufgabenwahrnehmung in ressortgemeinsamen und multinational verteilten, kollaborativen Umgebungen – sowohl im Inland als auch mit Blick auf die Einsatzorientierung der Bundeswehr – erfordert jedoch einen durchgängigen Informations- und Kommunikationsverbund. Dieser Verbund stellt, von der jeweils wahrzunehmenden Aufgabe abgeleitet, „Fähigkeitsbausteine" (IT-Services) zur Verfügung, die den modularen Aufbau von „Ende-zu-Ende" Prozessen ermöglichen. Dabei sind die Bausteine nach einem einheitlichen, durchgängigen Regelwerk zu konstruieren und so aufzubauen, dass für jede Aufgabe möglichst passgenau nur ein Baustein benötigt wird – und nicht eine Vielzahl von heterogenen Bausteinen für denselben Zweck zur Verfügung gestellt wird. Auf diese Weise wird ein hohes Maß an Wiederverwendbarkeit der Bausteine erreicht – ein Aspekt, der auch unter dem Gesichtspunkt der Wirtschaftlichkeit eine große Rolle spielt.

Es bietet sich an, einzelne Bausteine zu logischen Gruppen zusammen zu fassen. Solche Gruppen werden im Folgenden als „(funktionale) Cluster" bezeichnet. Wichtig ist, den Zuschnitt der Cluster so zu wählen, dass daraus eine sinnvolle, nachvollziehbare und möglichst überschneidungsfreie Architektur entsteht, im Folgenden als „Bebauungsplan" bezeichnet. Betrachtungsgegenstand der hier in Rede stehenden Bebauungsplanung ist das „Teilportfolio Cyber/IT (TPfCIT)" als Teil des Leistungsspektrums der Bundeswehr und integraler Bestandteil des Fähigkeitsmanagements.

Das strategische Programm „CITquadrat" baut auf diesen Überlegungen auf und hat zum Ziel, die für eine nachhaltige Weiterentwicklung und Implementierung des TPfCIT notwendigen Voraussetzungen zu schaffen. Dabei sollen die bisherigen „Stove-Pipes" aufgebrochen und soll die bisherige Systemlandschaft durch moderne Steuerungsansätze in die Zukunft geführt werden. Dazu gliedert sich das Programm zunächst in vier Teilprojekte, die später durch weitere Elemente ergänzt werden können:

- **Projekt 1** – Bebauungsplan: Festlegung des „Zuschnitts" für das TPfCIT auf der Basis funktionaler Cluster;
- **Projekt 2** – Steuerungslogik und Prozesse: Umsetzung grundlegender Prinzipien der Governance und des Managements zur Steuerung des Teilportfolios sowie durchgängige Gestaltung der zugehörigen Prozesse;
- **Projekt 3** – Organisation: Umsetzung der notwendigen aufbauorganisatorischen Anpassungen mit Blick auf den Bebauungsplan und die Steuerungslogik;
- **Projekt 4** – Konzeptionelle Dokumente: Erstellung des notwendigen konzeptionellen Rahmens – abgeleitet aus dem Weißbuch der Bundesregierung, der Konzeption der Bundeswehr und den Strategischen Leitlinien Cyber Verteidigung und Digitalisierung.

Das Programm CITquadrat wurde zum 1. Oktober 2017 durch den Abteilungsleiter CIT initiiert und befindet sich zurzeit in seiner initialen Phase. Diese schafft die Voraussetzungen für zwei anschließende, jeweils sechsmonatige Pilotphasen, in denen erste Cluster eingerichtet und die Steuerungslogik erprobt werden sollen.

Im Folgenden werden die vier Projekte des Programms CITquadrat näher beschrieben:

Projekt 1 – Bebauungsplan

Das TPfCIT ist auf der Basis des durch den Integrierten Planungsprozess (IPP) vorgegebenen Regelwerks in das Gesamtportfolio des GB BMVg integriert. Die notwendigen Absprachen erfolgen zwischen den Abteilungsleitern Planung und CIT. Das TPfCIT umfasst derzeit neun Cluster, die gängigen Konstruktionsprinzipien folgen, allerdings noch der weiteren Schärfung bedürfen. „Dahinter" liegen derzeit ca. 400 CPM-Projekte (von den insgesamt etwa 2.500 Projekten der Bundeswehr). Der Bebauungsplan ist sowohl mit den Architekturrichtlinien des Bundes als auch mit der NATO C3 Classification Taxonomie kompatibel. In einer ersten Festlegung wurden die folgenden neun Cluster beschrieben:

1. **Anbindung und Vernetzung:** Das Cluster plant und entwickelt Kommunikationsservices, die zur Verbindung einzelner Systeme erforderlich sind (z.B. Satellitenkommunikation, Fähigkeit zum Aufbau von Kernnetzen inkl. Netz-

knoten, Managementfunktionalitäten, digitaler Richtfunk, WLAN usw.);

2. **Infrastruktur und Cloud:** Das Cluster bildet die Grundlage für die Bereitstellung von Infrastrukturdiensten in einer verteilten und /oder zentralisierten Umgebung zur Unterstützung von Stabsarbeit im Friedensbetrieb sowie im Rahmen von Einsätzen und Übungen. Dazu gehören Rechen-, Speicher- und Netzwerkdienste, die als Basis für Rechenzentrums- oder Cloud-Computing Implementierungen genutzt werden können;
3. **Kollaboration und elektronische Verwaltungsarbeit (eVA):** Das Cluster umfasst (elektronische) Kollaborationsmöglichkeiten, welche auf offenen und kommerziell verfügbaren Standards basieren, ausreichend gemäß den Vorgaben des GB BMVg gesichert sind und die Anforderungen der NATO erfüllen;
4. **Enterprise Resource Planning (ERP):** Das Cluster plant und entwickelt als Core-Services die funktions- und organisationsübergreifende Unterstützung für bundeswehrweit querschnittlich genutzte administrative Prozesse und die Community of Interest (COI) Services zur Unterstützung logistischer Prozesse;
5. **GeoInformationsservices:** Das Cluster bietet einen netzwerkbasierten Zugriff auf qualitativ hochwertige Raster-, Vektor- und Geländedaten, die in unterschiedlichem Format und in unterschiedlicher Komplexität verfügbar sind. Sie stellen besondere Anforderungen an das Sammeln, Konvertieren, Speichern, Abrufen, Verarbeiten, Analysieren, Erstellen und Anzeigen von geografischen Daten und Informationsdiensten (Daten mit Raumbezug);
6. **Analytics und Simulation:** Das Cluster plant und entwickelt Analytics- und Simulations-Services, mit denen Informationen für eine verbesserte Entscheidungsfindung, Vorhersagefähigkeit, aber auch Anomalie-Erkennung, Modellierung und Simulationsunterstützung gesammelt, ausgewertet, präsentiert und verteilt werden können. Ziel ist, Tools (lernende Verfahren) für eine Verbesserung von operativen bzw. Managemententscheidungen zur Verfügung zu stellen. Das Cluster ist ein zentraler Baustein zum Erreichen von Informationsüberlegenheit;
7. **Community of Interest Services (COIS):** Das Cluster plant und entwickelt nicht-ERP-basierte COIS zur Unterstützung von Nutzergruppen, die an übergreifenden Zielen und Aufgaben, Missionen oder Geschäftsprozessen gemeinschaftlich arbeiten. Dieses Cluster ist wesentliche Schnittstelle zu den verschiedenen Nutzergruppen (Kunden).
8. **Informationssicherheitsservices:** Das Cluster plant und entwickelt Services zur Herstellung, Überwachung und Gewährleistung von Informationssicherheit;
9. **Management und Control Services:** Das Cluster plant und entwickelt IT-Services, die für die Steuerung und Administration des TPfCIT benötigt werden.

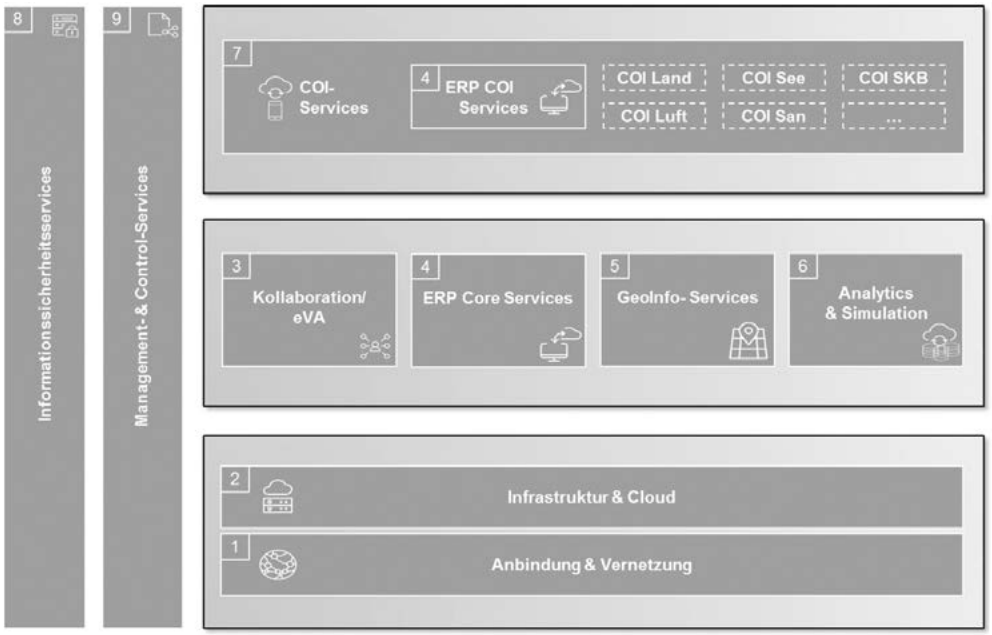


Abbildung 1 zeigt die derzeit neun Cluster im Überblick

Projekt 2 – Steuerungslogik und Prozesse

Ein nach der Systematik des Bebauungsplanes entwickeltes, komplexes Gesamtsystem (zugrundeliegender Gedanke eines Systems von Systemen, „System of Systems“) bedarf der Entwicklung einer angepassten Steuerungslogik. Die Verantwortung für die Weiterentwicklung der Cluster wird zukünftig ganzheitlich in ministeriellen Referaten liegen. Diese „Cluster Referate“ werden nach dem Prinzip Aufgabe – Kompetenz – Verantwortung (AKV) befähigt. Es ist vorgesehen, für jedes Cluster eine „Cluster-Strategie“ zu erstellen, die der Abteilung Planung als bedarfsbegründendes Dokument angezeigt und in die Mittelfristplanung des GB BMVg aufgenommen wird.

Der CIO steuert die Cluster mit Hilfe eines „CIO Council Teilportfolio Cyber/IT“, das sich im Januar 2018 konstituiert hat und seitdem in regelmäßigen Abständen tagt. Das Council ist im Kern ein abteilungsinternes Gremium, das anlassbezogen auch Teilnehmer aus anderen ministeriellen Abteilungen einlädt. Zudem sind regelmäßig auch Teilnehmer aus dem nachgeordneten Bereich (beispielsweise Kdo CIR, BAAINBw, bei Bedarf BWI) anwesend.

Das Management des TPfCIT wird im nachgeordneten Bereich durch Kdo CIR und BAAINBw unter enger Einbindung der BWI verantwortet. Auf dieser Ebene wird ablauforganisatorisch ein Management Board eingerichtet, das die operative Umsetzung der ministeriellen Vorgaben steuert.

Die Inhalte von Governance und Management des TPfCIT orientieren sich an „Best Practices“ – den formalen Rahmen setzt hier „COBIT 5“, ein Rahmenwerk für das Management und

die Steuerung der Unternehmens-IT[1]. Im Rahmen der konzeptionellen Arbeiten wurden relevante Steuerungsbausteine im Sinne eines „Good Practice Bundeswehr“ identifiziert. Diese werden mit dem durch die Abteilung CIT zu verantwortenden Prozessmodell harmonisiert, das drei Leistungsprozesse umfasst:

- „Cyber-/IT-Governance und Informationssicherheit gewährleisten“;
- „IT-Services bereit stellen“;
- „Geoinformationswesen sicherstellen“.

Die Prozesse werden derzeit formal ausgestaltet und finden Eingang in das Prozessportal des BMVg – als erster Leistungsprozess überhaupt ist der Leistungsprozess „Geoinformationswesen sicherstellen“ in diesem Portal abgebildet.
Die Aktivitäten des Programms CITquadrat steuert der CIO über ein eigenes Format, das „CIO Council CITquadrat“.

Projekt 3 – Organisation

Um eine sachgerechte Aufgabenwahrnehmung und Zusammenarbeit im Sinne der Systematik des Bebauungsplanes und entlang der neuen Prozesse und Steuerungslogik zu ermöglichen, werden beteiligte Bereiche aufbauorganisatorisch entsprechend ausgestaltet. Wie bereits begründet, sollen in der Abteilung CIT im BMVg Cluster-Referate eingerichtet werden, die nach dem AKV-Prinzip eine ganzheitliche Verantwortung für die zukunftsfähige Ausgestaltung des jeweiligen Clusters übernehmen. Daneben werden Querschnittsreferate einzurichten sein, die funktional und methodisch übergreifende Aufgaben wie beispielsweise (Integrierte) Planung, Architekturmanagement, Innovationsmanagement, Management & Control und Informationssicherheit übernehmen.
Das KdoCIR wird komplementäre Kompetenzzentren einrichten, die ebenfalls der „Cluster-Logik“ folgen und die jeweilige Fähigkeitsentwicklung steuern. Das KdoCIR nimmt zum 1. April 2018 eine dieser Systematik entsprechende erste Gliederung ein. Im BAAINBw sollen Programme eingerichtet werden, die gleichfalls der Clusterlogik folgen und die Realisierung der in den Clustern hinterlegten Fähigkeiten steuern.

Projekt 4 – Konzeptionelle Dokumente

Als Folgedokumente zu den bereits zuvor genannten Dokumenten „Weißbuch der Bundesregierung“, „Konzeption der Bundeswehr“ sowie „Strategische Leitlinie Cyber-Verteidigung“ und „Strategische Leitlinie Digitalisierung“ sind gemäß des zentralen Regelungsmanagements des GB BMVg Fachstrategien zu erstellen. Sie operationalisieren und verfeinern die in den vorgenannten Dokumenten formulierten Vorgaben. Der Idee eines durchgängigen methodischen Gerüstes für eine nachhaltige Weiterentwicklung des TPfCIT folgend, sollen die zu erstellenden Fachstrategien den „konzeptionellen Kopf“ für die im Weiteren zu detaillierenden Prozessbeschreibungen und Steuerungselemente bilden. Diesem Gedanken folgend, werden in der Abteilung CIT zurzeit folgende Fachstrategien erarbeitet:

- Fachstrategie Cyber-/IT-Governance (enthält auch Informationssicherheit);
- Fachstrategie IT-Services;
- Geoinformationsstrategie der Bundeswehr.

Weitere Dokumente sollen dann die konzeptionellen Vorgaben in operationelles Handeln umsetzen.

Warum CITquadrat?
CITquadrat steht für den Matrixgedanken beim organisatorischen Umbau im BMVg und im nachgeordneten Bereich. Im Ministerium wird in den „Cluster-Referaten“ die permanente Weiterentwicklung der in den Clustern hinterlegten Fähigkeiten betrieben. Daneben gibt es in der Abteilung Elemente, die querschnittliche Aufgaben wahrnehmen und für diese Aufgaben den Cluster-Referaten ein verbindliches Regelwerk zur Verfügung stellen, damit das Gesamtsystem in sich konsistent aufgebaut und in einen nachhaltigen Betrieb überführt werden kann. Diese Konstruktion erinnert an eine Matrix, die ja in der grafischen Darstellung häufig die Form eines Quadrates aufweist.
Das Programm CITquadrat hat die „Ablauflinie“ überschritten. Es wird nun darauf ankommen, das Programm konsequent umzusetzen, vor allem aber auch mit einer adäquaten strategischen Kommunikation und einem zielorientierten und adressatengerechten Veränderungsmanagement zu begleiten, um alle Stakeholder auf dem anspruchsvollen Weg mitzunehmen.

Der Inspekteur des Heeres, Generalleutnant Jörg Vollmer, bei seinem Vortrag zur Eröffnung der AFCEA-Fachausstellung 2017
Foto: Stefan Veres

1 Control Objectives for Information and Related Technology

10 Jahre AFCEA Bonn e.V. Studienpreis

Dr.-Ing. Michael Wunder, Abteilungsleiter, Fraunhofer-Institut FKIE und Beirat im Vorstand AFCEA Bonn e.V.

Dr.-Ing. Michael Wunder

Foto: privat

Der Zweck von AFCEA Bonn e.V. ist gemäß seiner Satzung die Förderung der Bildung, Forschung und Wissenschaft auf den Gebieten der Informations- und Kommunikationstechnik. Seit 10 Jahren ist die Organisation eines Studienpreises fester Bestandteil der Vereinsarbeit. Die beiden Bundeswehrhochschulen in Hamburg und München sowie die Hochschulen im näheren räumlichen Umfeld des Vereins, nämlich die Universität Bonn, die Hochschule Bonn-Rhein-Sieg sowie die Universität Koblenz-Landau (Campus Koblenz) und die Hochschule Koblenz, sind feste Partner. Zusätzlich werden ab 2018 auch die beiden Aachener Hochschulen (RWTH und FH) ihre besten Kandidaten auswählen und deren Abschlussarbeiten für den AFCEA Studienpreis vorschlagen.

Weil es um die Auslese der jeweils Besten an den beteiligten Hochschulen geht, ist die Anzahl der eingereichten Arbeiten überschaubar. Das anfänglich beim Studienpreis angesetzte Preisgeld in Höhe von 10.000 Euro ist inzwischen auf 20.000 Euro angehoben worden. Der Anreiz für die wissenschaftlichen Spitzenkräfte ist bewusst hoch gesetzt und soll helfen, die Bedeutung herausragender Leistung in technischen Disziplinen als wichtigen Beitrag für unsere Gesellschaft, herauszustellen.

Prämiert werden Master- und Magisterarbeiten, die auf den Gebieten

- Angewandte Informatik
- Nachrichtentechnik
- Automatisierungstechnik

erstellt wurden. Auch Bachelorarbeiten sind zugelassen. Für sie gelten dieselben Maßstäbe. Bewertungskriterien sind der erzielte Erkenntnisgewinn, der Praxisbezug, die Schlüssigkeit der Gedankenführung und die Klarheit der Darstellung.

Im Zeitraum 2008 bis 2017 wurden insgesamt 105 Arbeiten eingereicht, von einer achtköpfigen Jury mit Persönlichkeiten aus Wissenschaft, Industrie und Amtsseite mit großem Engagement und sehr hohem persönlichem Aufwand durchgearbeitet und akribisch bewertet. Insgesamt 130.000 Euro wurden bisher an 36 Preisträger ausgeschüttet. Die einzelnen Preisgelder lagen bislang zwischen 1.000 Euro und 6.000 Euro.

In diesem Jahr wird der Verein seinen Studienpreis zum 11. Mal am 30. August 2018 verleihen. Zu den Gepflogenheiten beim Studienpreis gehört, dass der Hauptpreisträger dem Publikum der Koblenzer IT-Tagung in einem dreiminütigen Statement die Quintessenz der siegreichen Arbeit erläutert. Alle bisher gekürten Preisträger haben diese Herausforderung sehr souverän gemeistert und gezeigt, dass man auch in sehr kurzer Zeit Fakten verständlich „rüberbringen“ und das Publikum fesseln kann.

Einige der Preisträger haben respektable Karrieren gemacht – vielleicht hat der AFCEA Studienpreis die eine oder andere Karriere etwas beflügelt. Die gute Resonanz bei den beteiligten Hochschulen, auserlesene und lesenswerte Arbeiten, würdige Preisträger und der Zuspruch aller Vereinsmitglieder sind Ansporn für AFCEA Bonn e.V., den Studienpreis auch weiterhin zu organisieren.

Leutnant Marcel Antzek, erster Preisträger aus dem Jahr 2017, erläutert den Inhalt seiner Arbeit im nachfolgenden Artikel.

Preisverleihung 2017

Foto: BAAINBw

Covert Channels – Instrumentalisierung regulärer Protokollspezifikationen zur verdeckten Angriffskoordination

Leutnant Marcel Antzek, AFCEA Preisträger 2017, Universität der Bundeswehr München

Marcel Antzek
Leutnant

Foto: Privat

Innerhalb der letzten Jahre ist branchenübergreifend eine kontinuierliche Intensivierung und Professionalisierung von gezielten Angriffen auf produktive Unternehmens- und Behördeninfrastrukturen zu konstatieren. Im Kontext dieser Angriffe werden oftmals vom Angreifer kompromittierte Drittsysteme zu sogenannten Bot-Netzen zusammengeschlossen, welche im weiteren Angriffsverlauf als dezentrales, hierarchisches Kommunikationselement eingesetzt werden. Auf Basis dieser Netzstruktur realisiert der Angreifer sowohl die Informationsdistribution im Rahmen der Angriffskoordination als auch die finale Exfiltration der akquirierten Daten nach erfolgter Kompromittierung der Infrastruktur.

Problematisch ist dabei aus Angreifer-Perspektive die effektive Verschleierung der genutzten Kommunikationsstrukturen, welche zur Minimierung des induzierten Detektionsrisikos innerhalb der kompromittierten Netzinfrastruktur beitragen soll. Hierzu werden zunehmend verschiedene Derivate verdeckter Informationskanäle (engl. Covert Channels) eingesetzt, welche basierend auf defizitären Protokollspezifikationen Kommunikationsdaten und Bot-Netz-Instruktionen in ungenutzte Paketbereiche des regulären Datenverkehrs integrieren. Auf diese Weise kann eine unerkannte Daten-Exfiltration realisiert werden, sodass eine Detektion des laufenden Angriffs anhand des kritischen Kommunikationsfaktors vermieden werden kann.

Neben der Integration verdeckter Informationen in für zukünftige Verwendung reservierte Protokollfelder existieren auch subtilere Mechanismen, welche beispielsweise auf Basis der Groß- und Kleinschreibung einzelner Datenfelder oder der paketinternen Anordnung optionaler Headerstrukturen die verdeckte Informationscodierung realisieren (siehe Grafik). Alternative Implementierungen nutzen des Weiteren zeitliche Korrelationen in der Ankunftszeit von Paketen mit arbiträrem Inhalt, indem Ankunftsraten der Datenpakete über ein definiertes Zeitintervall protokolliert und aus der dabei generierten, diskretisierten Ankunftsverteilung die vom Angreifer codierten Informationen extrahiert werden. Die Diversität möglicher Implementierungen ist dabei sehr hoch, da theoretisch jedes unspezifizierte Protokoll-Bit zur Informationscodierung genutzt werden kann; zusätzlich sind Kombinationen von verschiedenen Covert Channels zur Erweiterung des verfügbaren Kommunikationskanals denkbar.

Die Installation dedizierter Gegenmaßnahmen gestaltet sich dabei als komplex, da eine zu restriktive Konfiguration der Netzumgebung mit der regulären Nutzung von instrumentalisierten Diensten und Protokollen interferiert. Mögliche Ansatzpunkte zur Prävention und Detektion werden durch anomalie-basierte Netzanalysen repräsentiert, welche Abweichungen vom regulären Datenverkehr detektieren und damit gezielte Analysen initiieren können; um den potentiellen Angriffsvektor durch Covert Channels final minimieren zu können, ist jedoch primär die Sensibilisierung von administrativen Fachpersonal für diese bisher weitestgehend unbekannte Problematik erforderlich.

Daten	Header-Inhalt										
Original:	C	o	n	n	e	c	t	i	o	n	: keep-alive
Modifikation:	C	O	N	n	e	C	t	i	O	n	: keep-alive
Information:	0	0	0	1	1	0	1	1	0	1	$=109_{10}$, „m“ in ASCII-Code

Young AFCEANs: Ausgezeichnete Angebote

Auch in 2017 konnte das Bonner Chapter mit seinen Young AFCEANs Aktivitäten überzeugen. AFCEA International zeichnete das Chapter im Rahmen der West 2018 in vier von fünf Kategorien aus. Ron Simon, Capgemini, erhielt den Distinguished Young AFCEAN Award für seine Aktivitäten in Berlin. Alexander Kreth, German Air Force, wurde für seine Aktivitäten im Köln Bonner Raum mit dem Regional Distinguished Young AFCEAN Award ausgezeichnet.

Das Bonner Chapter selbst erhielt den Young AFCEAN Chapter Award und den Model Young AFCEAN Program Award.

Interesse dabei zu sein?
AFCEA bietet für seine Mitglieder bis 40 Jahre (Young AFCEANs) neben dem Angebot der Fachausstellung, der Koblenzer IT-Tagung und Fachveranstaltungen weitere besondere Aktivitäten: Zum Vernetzen und Austauschen werden den jungen Fach- und Führungskräften sowie Hochschulabsolventen eigene Fach- und Karriereveranstaltungen im Bonner und Berliner Raum angeboten.

Aktivitäten mit anderen AFCEA Chaptern – vor allem mit Young AFCEANs aus Kaiserlautern und dem Eifeler Chapter – ergänzen das Angebot. Gemeinsam besuchen wir beispielsweise Forschungslabore verschiedener IT-Firmen, die CeBIT oder die Air Base Ramstein.

Weitere Informationen und Termine zu aktuellen Veranstaltungen findet Ihr unter www.afcea.de. Ansprechpartnerin für die Young AFCEANs Veranstaltungen ist Katja Frintrop (Katja.Frintrop@afcea.de).

„Digitale Zukunft gestalten“ – aus Industrieperspektive

Die inhaltliche Umsetzung und Ausgestaltung des Jahresprogramms bei AFCEA Bonn e.V. erfolgt durch verschiedene Gremien aus Bundeswehr, Behörden, Wissenschaft und Industrie, die sich alle dem Motto „Mehr Wissen teilen“ verschrieben haben. Der Industriebeirat (IBR) als Vertreter der rund 90 Mitgliedsfirmen bringt Themenvorschläge für Jahresthema und Veranstaltungen ein. Dieses Gremium hat zum Jahresthema „Digitale Zukunft gestalten - Intelligent. Vernetzt. Sicher.“ zwei Beiträge aus seinem Kreis ausgewählt, die das Thema aus verschiedenen Industrie-Perspektiven beleuchten.

Schockwellen in der Digitalisierung und ihr Einfluss auf militärische Systeme

Franz-Bernd Möllers, Sekretär AFCEA Programmbeirat, Senior Account Manager beim Industriebeiratsunternehmen Atos Deutschland

Franz-Bernd Möllers

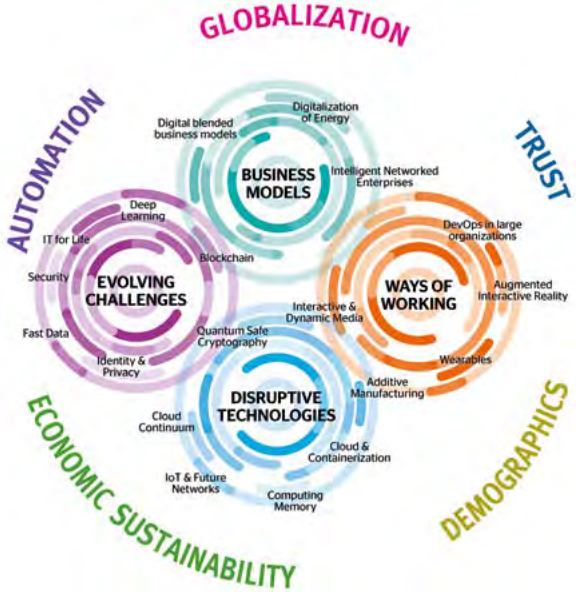
Foto: privat

Neue Technologien entwickeln sich immer rasanter. Vor allem durch disruptive Innovationen entstehen neue Märkte und Lösungen, die etablierte Systeme oft unerwartet treffen und diese teilweise vom Markt fegen und damit die Welt verändern. Schon heute ist zu erkennen, dass Technologien sich in der Gesellschaft bemerkbar machen und diese werden in Zukunft die Geschäfts- und Arbeitswelt immer schneller und stärker beeinflussen. Neue Geschäftsmodelle und Technologieanwendungen, die im Konsumentenbereich bereits tonangebend sind, dominieren zunehmend auch die geschäftlichen Bereiche. Dies löst eine Folge geschäftlicher Umwälzungen aus, die als „digitale Schockwellen“ bezeichnet werden und alle Bereiche der Wirtschaft und des gesellschaftlichen Lebens beeinflussen werden. Digitale Schockwellen werden nicht nur IT-Fähigkeiten erheblich verbessern. Sie werden sich vielmehr auf Wertschöpfungs- und Wirkungsketten in allen Branchen immens auswirken. So wie bei physikalischen Wellenausbreitungen gibt es auch bei digitalen Schockwellen Interferenzen. Manche der Wellen verstärken Impulse der Digitalisierung, manche löschen sie aus. Einige werden sich mehr, andere weniger auswirken, einige bringen neue Chancen, andere bringen neue potentielle Risiken.

Quellen der digitalen Schockwellen können sein:

Business Models: Auf der Grundlage branchenweiter Datenplattformen, die dem bewussten Austausch von Entwicklungs-, Produktions-, Betriebs- und Marktdaten dienen, entstehen vernetzte und intelligente Unternehmen. Blockchain-Technologien liefern dabei eine Möglichkeit, vertraglich bindende Transaktionen durchzuführen und diese zu überprüfen.

Ways of Working: Automatisierung, Communities und Digital Leadership werden die Arbeitswelt radikal verändern. Der Arbeitsplatz der Zukunft wird virtuell, kollaborativ und flexibel sein. Routinetätigkeiten werden zunehmend von Maschinen



Quelle: Atos Ascent Journey 2020

übernommen. Die Benutzeroberflächen werden neben der Optik künftig auch alle anderen Sinne ansprechen. Als Beispiel sind hier Wearables genannt, die immer häufiger genutzt werden, sie zeigen bereits jetzt ihr disruptives Potenzial.

Disruptive Technologies: Quanten-Computing und IoT-Netzwerke sind zwei Beispiele die erahnen lassen, welche massiven Umwälzungen mittelfristig zu erwarten sind und sich auch signifikant auf den Sicherheitssektor auswirken werden.

Evolving Challenges: Die Nachfrage nach besseren und gleichzeitig einfacher umzusetzenden Cyber-Sicherheitslösungen wird steigen. Fortschritte in der Medizintechnik und Lebensmittelherstellung eröffnen nie geahnte Möglichkeiten, die eine Vielzahl ethischer Fragen nach sich ziehen, die bei Überlegungen zur Bioinformatik berücksichtigt werden müssen.

Was heißt das für militärische Systeme?

- Die Arbeiten und Tätigkeiten werden mehr und mehr ersetzt durch vernetzte und ferngesteuerte Systeme wie Drohnen und Roboter. Dies wird sich insbesondere bei Sensoren, Effektoren und bei Command-und-Control-Systemen auswirken.
- Viele Aufgaben können unabhängig vom Ort des Arbeitsplatzes in einer sicheren Umgebung umgesetzt werden.
- Die Soldaten vor Ort werden durch virtuell angereicherte Informationen im Sichtfeld (beispielsweise Smart Glasses oder Head Mounted Displays) unterstützt.
- Der Vernetzungsgrad (Internet of Things, IoT) wird beim Militär immer stärker Einzug halten. Der dadurch entstehende Anstieg an Datenverbindungen und das rasante Anwachsen des Datenvolumens muss nicht nur gemanagt werden. Darüber hinaus ist es erforderlich die Systeme, möglichst in Echtzeit, durch vorausschauende Instandhaltung (predictive maintenance) zu überwachen und frühzeitig zu warten.
- Datenverschlüsselungsverfahren, die heute noch als hochsicher gelten, werden zukünftig mithilfe bestimmter Quanten-Algorithmen überwunden. Unternehmen, aber auch die öffentliche Verwaltung und insbesondere die Behörden mit Sicherheitsaufgaben und die Bundeswehr, müssen sich hierauf vorbereiten.
- Der Cyberkrieg wird immer realer. In manchen Fällen ist das Gefährdungspotential durch IT-Angriffe höher als durch konventionelle Waffen. Das Hacken von kritischen Infrastrukturen kann die Fähigkeit von Nationen, zu funktionieren und sich zu verteidigen, beeinflussen.

In der Vergangenheit wurden technische Entwicklungen oft durch militärische Erfordernisse gefördert und vorangetrieben. Dies ist in vielen Bereichen überholt. Die Entwicklungszyklen im Endverbrauchermarkt sind so schnelllebig, dass der übliche Beschaffungsprozess, gerade im militärischen IT-Umfeld, nur noch hinterher hinkt. Eine deutlich agilere Vorgehensweise ist hier dringend empfehlenswert.

Strategisches IT-Management: Die Herausforderungen der Digitalisierung meistern

Joachim Mörsdorf, Sprecher Industriebeirat AFCEA Bonn e.V. & Michael Exner, Geschäftsführer des Industriebeiratsunternehmens CONET

Joachim Mörsdorf

Foto: Privat

Michael Exner

Foto: Privat

Nach der Globalisierung sieht sich die Welt mit der Digitalisierung der nächsten großen Herausforderung gegenüber. Lebens- und Arbeitswelten rücken zusammen, vernetzen sich enger und werden von Kommunikation und Interaktion stärker durchdrungen, was gleichermaßen Risiken wie auch Chancen birgt.

Dies betrifft im besonderen Maße die IT und damit auch die Bundeswehr als Betreiber und Nutzer eines der größten IT-Systeme in Europa. Die IT wird sich zukünftig stark verändern und neu geordnet. Wurde in der Vergangenheit der Schwerpunkt oft auf Controlling und Rechnungswesen gelegt, muss die IT heute viele zusätzliche Anforderungen erfüllen. Eine IT-Strategie der Zukunft benötigt daher eine viel stärkere Flexibilität und Transparenz über alle Prozesse.

Wer aber dabei nicht schlüssig definiert, welche Ziele er mit der Digitalisierung verfolgt, wird sich in den vielfältigen Möglichkeiten verlieren oder in fruchtlosen Einzelmaßnahmen verrennen.

Enterprise Architecture Management – Herzstück eines strategischen IT-Managements

Das Enterprise Architecture Management (EAM) leistet hier einen wesentlichen Beitrag, indem es Geschäftsprozesse und Informationstechnik enger miteinander verknüpft und die Organisation als Ganzes betrachtet. Dazu stellt es eine bewährte Methodik und universelle Sprache zur Dokumentation des Ist-Zustands ebenso wie zur Festlegung und Verfolgung der konkreten Ziele zur Verfügung.

Dabei gilt es aber auch, das EAM nicht isoliert, sondern im Zusammenhang mit dem kompletten Lebenszyklus zu betrachten, zu dem weitere wichtige Teildisziplinen gehören – von Anforderungs-, Projekt- und Qualitätsmanagement über Service-, System- und Lizenzmanagement bis hin zu IT-Controlling, IT-Governance, IT-Recht & Compliance und nicht zuletzt das IT-Security-Management.

Mit einem modernen, Tool-gestützten EAM lässt sich über alle diese Aspekte ein zielorientiertes, strategisches IT-Management realisieren, das die Anforderungen von heute erfüllt und gleichzeitig die Herausforderungen von Morgen vorhersagen und adressieren hilft.

Informationsüberlegenheit – fundamentale Basis für die Operationsführung

Wenn auch die Herausforderungen des digitalen Zeitalters für die eigenen Prozesse und die Aufgabenerfüllung meist im Vordergrund stehen, ergeben sich durch neue digitale Möglichkeiten aber auch deutliche Chancen.

So etwa bei der Aufklärung und Lagebeurteilung im Rahmen einer umfassenden Cyber Defense. Nie zuvor gab es so viele Quellen, die sich zur Informationsgewinnung im Führungsprozess nutzen lassen. In einem aktuellen Forschungsprojekt etwa werden denkbare Szenarien untersucht, um unter Einsatz von marktverfügbaren Komponenten (COTS) über ein feldverwendungsfähiges, schnell verlegbares und sich selbst WLAN-basiert organisierendes Ad-hoc-Netzwerk zumeist verschlüsselte Datenströme zu sammeln und weiterzugeben. Werden diese mit den methodischen und technischen Ansätzen der Krypto-Analyse zeitgerecht entschlüsselt und mittels Big-Data-Verfahren ausgewertet, tragen die gewonnenen Informationen zu einer entscheidenden Informationsüberlegenheit bei.

Diese beiden Schlaglichter illustrieren treffend das Spannungsfeld zwischen den Herausforderungen und den Chancen der Digitalisierung. Auch zukünftig wird es darauf ankommen, in einer vertrauensvollen Zusammenarbeit zwischen Wirtschaft, Industrie und Bundeswehr den Weg zur digitalisierten Streitkraft zu begleiten. Die Mitglieder der AFCEA sind dafür bestens gerüstet!

OHB System AG: Innovative Systemlösungen aus bewährter Hand

Die zunehmende Digitalisierung bedarf einer verlässlichen und vertrauenswürdigen Infrastruktur. Raumfahrtbasierte Lösungen der OHB System AG sind integraler Bestandteil solch kritischer Elemente und für zivile und militärische Anwender bereits zum alltäglichen Umgang geworden. OHB ist auf Komplettlösungen für Satellitensysteme für Telekommunikation, Navigation und Erdbeobachtung spezialisiert. Sie werden durch Lösungen für luftgestützte Systeme ergänzt.

Die Satellitenkommunikation wird mit der OHB-Produktlinie SmallGEO bedient. Die Heinrich Hertz-Mission (Abbildung) mit ihrem SATCOMBw-Anteil, EDRS-C mit einer Laserkommunikationsnutzlast, H36W-1 mit flexiblen digitalen Nutzlasten sowie die vollelektrisch angetriebene Variante ELECTRA basieren auf dieser flexiblen Plattform. Im Bodensegment erweiterte OHB die Leistungsfähigkeit der Ankerstation Gerolstein um eine UHF-DAMA Fähigkeit; im Luftfahrtbereich ist OHB Kernpartner im Vorhaben FCAS.

Das für die Bundeswehr entwickelte, hergestellte und betriebene System SAR-Lupe zur raumgestützten Radar-Aufklärung ist seit mehr als zehn Jahren im Einsatz und wird durch das Nachfolgesystem SARah ergänzt und abgelöst werden. OHB realisiert den nationalen Hyperspektralsatelliten EnMAP, dessen Daten die Klassifikation von Landnutzungen und die Detektion von Anomalien auf der Erdoberfläche ermöglichen werden. Sechs MeteoSat Wettersatelliten der dritten Generation (MTG) und ein elektro-optisches System für die Bundesregierung ergänzen das Portfolio der OHB in der Erdbeobachtung.

Durch die Beauftragung mit 34 Galileo FOC Satelliten für die Europäische Union hat sich OHB auch im Bereich des hochpräzisen *Positioning, Navigation and Timing* etablieren können. OHB sieht sich im Innovationswettbewerb bestens platziert und wird auch bei kommenden nationalen und europäischen Programmen die über Jahrzehnte aufgebaute Expertise zur Verfügung stellen.

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr

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

Digitale Zukunft – Architekturen, Plattformen, Anwendungen

Die digitale Zukunft wird auch in der Bundeswehr vieles tiefgreifend verändern. Organisation, Waffensysteme, Prozesse müssen neu, digital gedacht werden. Die Bundeswehr muss jetzt die Chancen und Möglichkeiten der Digitalisierung noch konsequenter für sich nutzen, gleichzeitig aber zunehmenden Bedrohungen im Cyber- und Informationsraum konsequent begegnen. Hierfür benötigt sie ein „Digitales Selbstverständnis".
Es bedarf einer systematischen und zügigen Vorgehensweise, um den Herausforderungen für das gesamte Aufgabenspektrum der Bundeswehr in einer sich rapide wandelnden IT-Umwelt gewachsen zu sein, ohne sich technologischen Defiziten und Fehlentwicklungen auszuliefern. Dabei bilden operationell wie systemtechnisch einheitliche Architekturen die unverzichtbare Grundlage für die Realisierung und den Betrieb hochgradig wirksamer, interoperabler (Waffen-)Systeme für derzeitige und künftige Einsatzerfordernisse. Nur auf Grundlage von Architekturen können zeitgemäße, effiziente IT-Lösungen durch alle für die Sicherheit Deutschlands verantwortlichen Organisationen sinnvoll und kohärent verwirklicht werden. Architekturen wirken sich jedoch nicht nur aktiv auf Gestalt und Struktur der Plattformen (Waffen- oder IT-Systeme) sowie Anwendungen aus – ihre Konzipierung wird umgekehrt auch durch bereits existente oder vorgegebene Anwendungen und Plattformen beeinflusst. Wo verlaufen die Grenzlinien für diesen Einfluss?

Diese Zusammenhänge und damit in Verbindung stehende Fragen mit ihren Auswirkungen auf die Ausrüstung der Bundeswehr unter den Bedingungen der Digitalisierung von Technik, Industrie und Gesellschaft zu diskutieren, ist unser Anliegen bei der **Koblenzer IT-Tagung** am **30. August 2018**. Hierzu laden wir Sie ein und freuen uns, Ihnen ein interessantes Programm sowie einen unterhaltsamen Abend bieten zu können, verbunden mit der Möglichkeit zu vielen Gesprächen.

Ort:	Rhein-Mosel-Halle, Julius-Wegeler-Straße 4, 56068 Koblenz		
Datum/Zeit:	Donnerstag, 30.08.2018	09:00 – 18:30 Uhr	(Einlass 08:00 Uhr)
	mit „Koblenzer Abend"	18:30 – 21:00 Uhr	
Teilnehmer:	Bundesministerium der Verteidigung; Kommandobehörden, Ämter, Dienststellen- und Truppenteile der Bundeswehr; Behörden, Organisationen aus dem Bereich der öffentlichen Sicherheit (BOS); Institute, Verbände; Universitäten und Hochschulen; Industrie mit Schwerpunkt Informations- und Kommunikationstechnik; internationale Gäste		
Fachliche Leitung:	Brigadegeneral Jens-Olaf Koltermann, Abteilungsleiter Informationstechnik BAAINBw Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V.		
Programm:	+ aktuelle Informationen unter www.afcea.de und www.baainbw.de		
Kostenbeitrag:	+ Eintritt**:** 90,- €, einschließlich „Koblenzer Abend" + Öffentlicher Dienst und AFCEA-Mitglieder**:** Eintritt 20,- € Tagungspauschale, Teilnahme am Koblenzer Abend: 20,- € zusätzlich		

AFCEA Bonn e.V., Borsigallee 2, 53125 Bonn, Tel.: 02 28 / 9 25 82 52, Fax: 02 28 / 9 25 82 53
BAAINBw, Ferdinand-Sauerbruch-Str. 1, 56073 Koblenz, Tel.: 0261 / 13354 8143, Fax: 0261 / 13354 8470

Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

KI-BASIERTE ENTSCHEIDUNGS-UNTERSTÜTZUNG

Fraunhofer FKIE unterstützt die Streitkräfte auch im Bereich »Advanced Analytics & Machine Learning«. Intelligente Assistenzsysteme sorgen für Informationsüberlegenheit.

KI im Einsatz – Advanced Analytics & Machine Learning für sicherheitskritische Anwendungen

Prof. Dr. Peter Martini, Institutsleiter des Fraunhofer FKIE

Prof. Dr. Peter Martini
Foto: Fraunhofer FKIE

„Künstliche Intelligenz“ (KI) ist ein schillernder Begriff, der sich einer genauen Definition entzieht, aber dennoch – oder gerade deshalb? – in aller Munde ist. In ihrer seriösen Variante ist KI allgegenwärtig im zivilen und hochgradig relevant im militärischen Bereich. Denn der militärische Einsatz von KI im Sinne von Machine Learning, Sensordatenfusion oder Advanced Data Analytics ist längst nicht mehr eine Frage des „ob“, sondern vielmehr des „wie“. Und genau hier setzt Fraunhofer FKIE mit seinen F&T-Aktivitäten an: Forschungsgegenstand sind dabei nicht die Grundlagen der Künstlichen Intelligenz, sondern die Anwendung von Methoden der KI in ausgewählten Einsatzgebieten. Zum Tragen kommt hier der FKIE-eigene Leitspruch: „Vom Einsatz her gedacht“.

Gerade im militärischen Bereich unterliegt KI besonderen Bedingungen. Was vorrangig interessiert, ist die Unterstützung von intelligentem Handeln auf der Basis eines angemessenen Lagebewusstseins. Bezogen auf originär militärische Anwendungen geht es vorrangig um Systeme, die rational und logisch handeln und hierzu große Datenmengen adäquat auswerten und verdichten, vorgegebene Probleme lösen, Prozesse optimieren, Vorschläge unterbreiten (Entscheidungsunterstützung), den Nutzer verstehen und seine Intention erkennen. Kurz gesagt: Benötigt werden intelligente Assistenzsysteme.

Der Mensch bleibt im Mittelpunkt

Vieles lässt sich mit KI automatisieren, aber selbst die leistungsstärksten KI-Systeme sind zuweilen erschreckend „dumm“. Der Mensch kann/muss/soll Fehlfunktionen erkennen und kompensieren – damit bleibt er mit seiner natürlichen Intelligenz und mit seinem Verantwortungsbewusstsein im Mittelpunkt der Handlungsprozesse.

Die Risiken bei naiver Nutzung sind einerseits systemseitig: Zahlreiche KI-Ansätze weisen zwar auf statistische Auffälligkeiten hin, nicht aber auf Kausalität. Als unmittelbare Grundlage für Entscheidungen mit weitreichender Verantwortung sind derartige Ansätze nur in Spezialfällen einsetzbar. Von zentraler Bedeutung ist, ob für angestrebte Einsatzgebiete überhaupt hinreichend viel brauchbares Trainingsmaterial vorliegt – und ob dieses Trainingsmaterial nicht eventuell bereits manipuliert ist. Andererseits kann auch der Benutzer selbst ein Risiko darstellen, etwa wenn das System soweit automatisiert agiert, dass es alle Standardfälle eigenständig und völlig ohne Eingreifen oder auch nur Mitdenken des Benutzers verarbeiten kann, bei einem besonders schwierigen Fall jedoch unvermittelt der Benutzer selbst die Entscheidung treffen muss. Hier tritt ein, was Bainbridge bereits 1983 in „Ironies of Automation“ beschrieben hat: Die Automation hat zu einer Entlastung des Menschen geführt, er hat weniger zu tun und seine kognitiven Fähigkeiten verkümmern, weil sie nicht oft genug gebraucht und damit trainiert werden. Ist der Mensch jetzt mit einer sehr schwierigen Entscheidung konfrontiert, ist er nicht mehr in der Lage, diese zu treffen.

In beiden Fällen ist die Einbindung des Menschen in die in der Maschine ablaufenden Prozesse von vorrangiger Bedeutung. Der Mensch muss bei Command and Control als Entscheider und als Träger von Verantwortung „im Loop“ oder zumindest hinreichend nah an automatisierten Prozessen gehalten werden.

Das Fraunhofer FKIE entwickelt hierfür Interaktionskonzepte und Human-Machine-Interfaces, die nicht nur den speziellen Anforderungen wie Usability, User Experience und multimodaler Interaktion gerecht werden, sondern sich auch an natürliche menschliche Interaktionsformen sowie an den jeweiligen Zustand des Benutzers anpassen – ob der Benutzer nun vor einer Wand aus Bildschirmen sitzt, in einem automatisierten Fahrzeug oder beim abgesessenen Einsatz auf sein Smartphone schaut.

Auch zu diesem Zweck werden wiederum Methoden der KI eingesetzt, beispielsweise um Situations- oder Verhaltensmuster sowie kognitive Problemzustände zu erkennen oder um die Assistenzfunktionen dynamisch an die Benutzerzustände anzupassen.

Künstliche Intelligenz in der Anwendung

KI bzw. Machine Learning wird bei Fraunhofer FKIE darüber hinaus in weiteren Bereichen in die Anwendung gebracht. Einen ausschnitthaften Überblick zeigen wir Ihnen auf den folgenden Seiten. Allgemein lässt sich sagen, dass mithilfe von KI die aufgrund des technologischen Fortschritts bei Sensoren und Sensorsystemen anfallenden Massendaten, Big Data also, handhabbar gemacht werden. So haben FKIE-Wissenschaftler ein System entwickelt, das automatisiert Texte – zum Beispiel aus den sozialen Medien – klassifizieren und auf diese Weise etwa Fake News und Meinungsbeeinflussung erkennen kann.

Oder sie setzen KI zur Vorselektion und Klassifikation von Funksignalen ein. War es früher noch Kern des Strebens, überhaupt Funksignale in dem breiten Spektrum der Frequenzen aufzuspüren bzw. zu detektieren, hat sich die Schwierigkeit heute grundlegend verschoben: Massen von bereits innerhalb der Sensordaten detektierten Einzelsignalen müssen nun klassifiziert und vorselektiert werden, um die relevanten aus ihnen herauszufiltern und zu einem Lagebild zu verdichten. Nur so liefern sie einen wichtigen Beitrag zur Unterstützung der Aufklärungskette.

Verantwortungsbewusst ausgewählte und mit Kausalität verknüpfte KI-Verfahren wie die Bayes'schen Schätzer dienen der militärischen Entscheidungsunterstützung. So kann etwa ermittelt werden, mit welcher Wahrscheinlichkeit Sensordaten einem bestimmten physikalischen Phänomen zuzuordnen sind: Auf diese Art können z. B. die an einem Luftkampf beteiligten Kampfjets via Radar detektiert, klassifiziert und über längere Zeit hinweg verfolgt werden.

Auch im Bereich der IT- und Cybersicherheit ist Maschinelles Lernen eine sinnvolle, wenn nicht sogar notwendige Ergänzung, um mit den Techniken der Angreifer wie auch mit der Schnelligkeit der Angriffswerkzeuge mithalten zu können. Maschinelles Lernen kann hier dazu beitragen, verborgene Muster in den sich rasant verändernden Daten mit hoher Genauigkeit zu erkennen, die Kompromittierung der Systeme im Falle eines Angriffs zu analysieren und auf diese Weise eine große Menge an Angriffen auf die eigenen Systeme zu verarbeiten.

Leitthema „KI-basierte Entscheidungsunterstützung für den Cyber- und Informationsraum"

Die Kompetenzen des Fraunhofer FKIE sind breit gefächert. Dies veranschaulichen auch die Beiträge, die auf den folgenden Seiten facettenreich und sehr unterschiedlich das Leitthema „KI-basierte Entscheidungsunterstützung für den Cyber- und Informationsraum" beleuchten.

Ergänzt wird diese Darstellung durch einen Gastbeitrag von der Universität der Bundeswehr München.

Prof. Dr. Frank Kurth, Forschungsgruppenleiter „Aufklärung und Störung" in der Abteilung „Kommunikationssysteme", erläutert in gleich zwei Beiträgen den Einsatz von KI in seinem Bereich, zum einen, wie Deep Learning zur Erschließung von Massendaten für die Funkaufklärung genutzt werden kann, und zum anderen gemeinsam mit Dirk von Zeddelmann aus dem KdoStratAufkl die Möglichkeiten und Grenzen von KI-Methoden für die Sprachsignalverarbeitung. Nicht die Sprache, sondern vielmehr textuelle Informationen hat Prof. Dr. Ulrich Schade, Forschungsgruppenleiter „Informationsanalyse" in der Abteilung „Informationstechnik für Führungssysteme", im Blick. Er stellt ein Klassifikationstool vor, das Massendaten aus den Sozialen Medien, insbesondere aus Twitter, automatisiert mittels Machine Learning nach bestimmten Kriterien sortieren kann. Ein besonders spannender aktueller Anwendungsfall ist die Identifizierung von „Fake News".

Dr. Tobias Albertsson und Viviane Zwanger aus der Abteilung „Cyber Analysis & Defense" zeigen den Einsatz von Machine Learning einerseits für eine Entscheidungsübersicht zur Bewertung von Domänen auf und andererseits für ein Assistenzsystem zur Erkennung von Ähnlichkeiten in Programmen zur Unterstützung der Täterattribution.

KI hilft bei der Klassifizierung und Vorselektion massenhafter Daten zur Erstellung eines Lagebildes. Bei Fraunhofer FKIE wird diese Technologie u. a. im Bereich der Cyber Abwehr und für die Informationsklassifizierung eingesetzt. Foto: Fraunhofer FKIE

Auch Dr. Michael Gerz, Forschungsgruppenleiter „Interoperability & Testing" in der Abteilung „Informationstechnik für Führungssysteme", hat einen weiten Blick auf das Thema KI im Einsatz und diskutiert mögliche Verbesserungen von Führungsinformationssystemen durch KI. Währenddessen fokussiert Dr. Thomas Alexander, Abteilungsleiter „Human Factors", ganz klar auf die Unterstützung bei der Umgebungswahrnehmung und der physischen Leistungsfähigkeit des abgesessenen Soldaten mittels intelligenter Assistenzsysteme.

Auch Assistenzsysteme wie „Click & Grasp", das von Dr. Dirk Schulz, Abteilungsleiter „Kognitive Mobile Systeme", vorgestellt wird, setzen KI-Methoden ein: Hierbei geht es um eine Technologie, die mithilfe von Robot Vision das Greifen von beliebigen Objekten mit einem Roboterarm sehr erleichtert.

In Zusammenhang mit Benutzungsschnittstellen für Mensch-Maschine-Systeme verweist Dr. Carsten Winkelholz, Forschungsgruppenleiter „Informationsvisualisierung und Interaktion" in der Abteilung „Mensch-Maschine-Systeme", auf kognitive Modelle und Architekturen zu deren Gestaltung und Entwicklung.

In seinem Artikel „Von KI zum teilautomatisierten, hochautomatisierten oder autonomen Fahren?" befasst sich Prof. Dr. Frank Flemisch mit dem Thema des Autonomen Fahrens und seiner Zukunft.

Richtig und verantwortungsbewusst eingesetzt bieten die Techniken, die gemeinhin unter dem Begriff „KI" zusammengefasst werden, ein immenses Zukunftspotenzial, das wesentliche Fortschritte auch in Bereichen ermöglicht, die klassischer IT nur schwer zugänglich sind.

Deutlich gewarnt werden muss hingegen vor einem naiven Einsatz von KI-Techniken, die sich zwar in zivilen Bereichen ohne Sicherheitsrelevanz großer Beliebtheit erfreuen, aber keine Nachvollziehbarkeit von Bewertungen bzw. Entscheidungen unterstützen. Mit diesem wichtigen Thema und mit angrenzenden Fragestellungen befasst sich Dr. Felix Govaers, stellvertretender Abteilungsleiter „Sensordaten- und Informationsfusion", in seinem Beitrag zur kritischen Reflexion zum Einsatz von Künstlicher Intelligenz im wehrtechnischen Umfeld.

KI-basierte Cybersicherheit: Von Unterstützend, Automatisiert bis Autonom

Prof. Dr. Gabi Dreo Rodosek, Christian Dietz, Dennis Kergl,
Forschungsinstitut CODE, Universität der Bundeswehr München

Prof. Dr. Gabi Dreo Rodosek
Foto: privat

Christian Dietz
Foto: privat

Dennis Kergl
Foto: privat

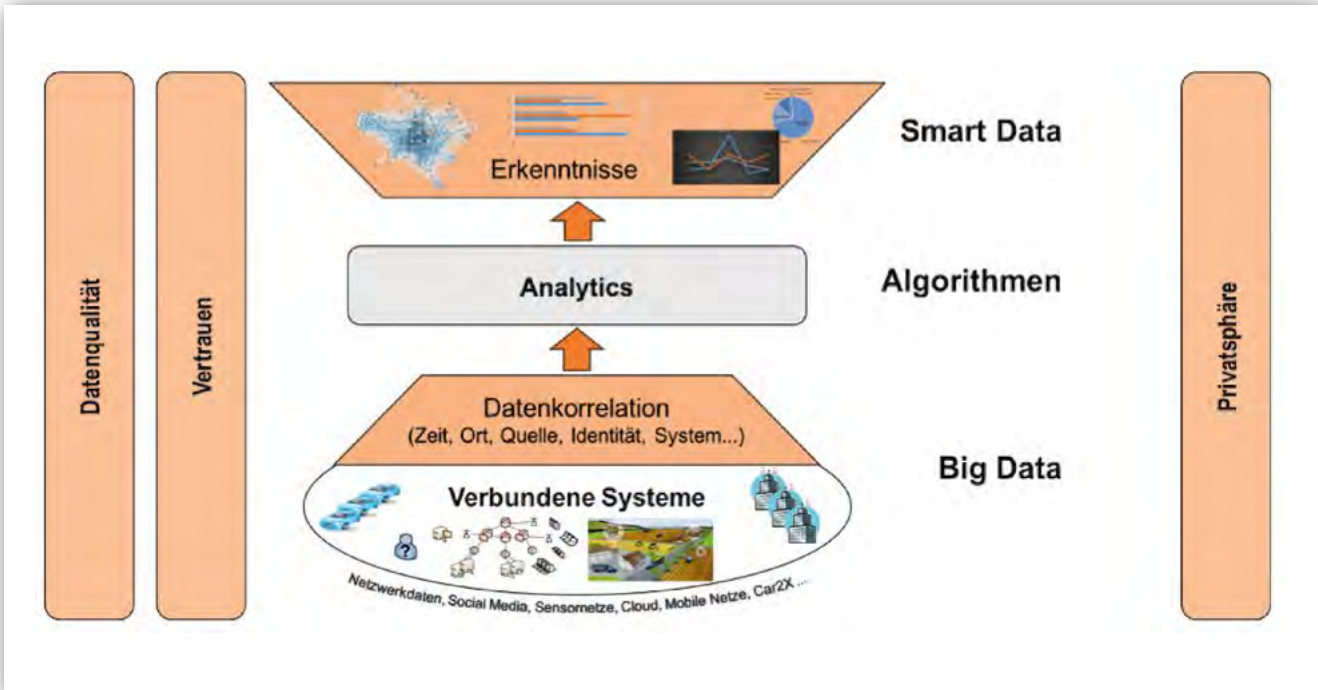
Die Informations- und Kommunikationstechnologie (IKT) entwickelt sich rasend schnell. Durch die immer höhere Anzahl vernetzer Systeme, die stetig wachsenden Datenmengen und die Entwicklung zum Internet of Everything wird auch die Angriffsfläche immer größer. Cyberangriffe steigen nicht nur in der Quantität, sondern auch in der Qualität. Um den komplexen Herausforderungen zu begegnen, ist die Entwicklung innovativer Sicherheitslösungen auf Basis von Künstlicher Intelligenz (KI) und insbesondere Maschinellen Lernens unabdingbar.

Die Basis der automatisierten Entscheidungsunterstützung sind die zugrundeliegenden Daten, die entweder strukturiert oder unstrukturiert vorliegen. Sie spielen eine zentrale Rolle in der Sicherstellung der Qualität des Gesamtsystems und für den erfolgreichen Einsatz von KI. Am Forschungsinstitut CODE (Cyber Defence) der Universität der Bundeswehr München werden unterschiedliche Fragestellungen mit geeigneten Verfahren u.a. des Maschinellen Lernens adressiert. Der Stellenwert des Forschungsbereichs der KI am Forschungsinstitut CODE wird u. a. durch die Schaffung von zwei neuen W3-Professuren in den Bereichen „Data Science“ und „Machine Learning“ deutlich. Des Weiteren liefert KI als Querschnittstechnologie die Basis für mehrere andere Forschungs- und Anwendungsbereiche am Forschungsinstitut CODE.

Derzeit wird am Lehrstuhl von Prof. Dreo an selbstlernenden Systemen zur Erkennung von Cyberattacken in Rechnernetzen geforscht, die automatisierte Maßnahmen, abhängig von einer Risikobewertung, einleiten können, um die nächsten Schritte eines laufenden Angriffs zu unterbinden und weitere Ereignisse dieser Art zu verhindern. Diese als „Automated Response“ bezeichnete Vorgehensweise ist zentraler Bestandteil zukünftiger Cybersicherheitslösungen und Teil einer Cybersicherheitsstrategie. Zu einer solchen Strategie gehört auch die vorausschauende (predictive) Vereitelung zukünftiger Angriffe, beispielsweise durch die frühzeitige Erkennung vorhandener Schwachstellen in Systemen, die an das Internet angeschlossen sind. Zu diesem Zweck wird u. a. an Methoden geforscht, um aus öffentlich zugänglichen Daten aus sozialen Medien Informationen über laufende Angriffe auf Internetdienste zu gewinnen. Dazu kommen Techniken des Maschinellen Lernens (supervised) zum Einsatz, die eine sprachunabhängige Erkennung der relevanten Ereignisse ermöglichen soll. Die Verknüpfung dieser neu gewonnenen Information mit Informationen über technische Eigenschaften der angegriffenen Systeme bietet die Möglichkeit, in diesem Kontext Wissen über mögliche, bisher unbekannte Schwachstellen (so genannte Zero-Days) zu gewinnen.

Einsatz von KI zur sprachunabhängigen Klassifizierung von Inhalten in sozialen Medien (Tweets) zur globalen Erkennung von relevanten Ereignissen, um Angriffe auf unbekannte Schwachstellen in Web-Diensten zu detektieren.
Foto: © Forschungsinstitut CODE, UniBw München

Um dieses neuartige Verfahren zu ermöglichen, ist der Einsatz von KI-Methoden an verschiedenen Stellen erforderlich. Unstrukturiert vorliegenden Daten müssen automatisch klassifiziert werden, um nachgelagerte Prozessschritte mit strukturierten Daten zu versorgen. Für eine korrekte Klassifizierung wird der Klassifikator vorab mit tausenden Beispielen trainiert und



Von Big Data zu Smart Data.

Foto: © Forschungsinstitut CODE, UniBw München

laufend an den sich ständig verändernden Datenstrom aus den sozialen Medien angepasst. Dieses kontinuierliche Lernen ermöglicht eine gleichbleibend gute Klassifizierungsrate, wohingegen statische Systeme im zeitlichen Verlauf stetig ungenauer werden. Auf diese Weise können aus unstrukturierten Rohdaten, wie beispielsweise über die öffentlichen Schnittstellen von Twitter verfügbar (vgl. Abbildung 1), Ereignisse erkannt werden, deren statistische Merkmalsverteilung als Grundlage für die Erkennung unbekannter Schwachstellen dient. Im Gegensatz zu herkömmlichen Verfahren werden hierbei nicht die Inhalte selbst als Ziel betrachtet, sondern deren Korrelation mit technischen Details (z. B. Softwareprodukt und -version) der betroffenen Systeme zur Gewinnung von neuem Wissen über Angriffe und Schwachstellen genutzt. Dieses Wissen ermöglicht es beispielsweise, Abwehrmechanismen automatisch anzupassen oder die genauere Analyse möglicher Schwachstelle zu initiieren und Sicherheitspatches zu erstellen.

Ein weiteres Beispiel des Einsatzes von KI-Ansätzen ist die proaktive Detektion von Botnetzen, also die Detektion von Botnetzen bevor diese für Cyberangriffe genutzt werden. Durch die stetige Weiterentwicklung von Botnetzen hin zu hochgradig flexiblen Crimeware-as-a-Service-Plattformen in Kombination mit verschiedensten Verschleierungstechniken, wie z. B. Verschlüsselung von Command-and-Control-Informationen, hybriden P2P-Infrastrukturen und Fast-Flux, ergeben sich primär zwei Herausforderungen. Zum einen können schnell neue Varianten einer Botnetzfamilie mit modifiziertem Verhalten entstehen und zum anderen erschweren die genannten Verschleierungstaktiken die schnelle und effiziente Erstellung von Indikatoren und Signaturen für die klassische Erkennung komplexer Botnetzinfrastrukturen und Verhaltensmuster. Um diesen Herausforderungen gerecht zu werden, ist die Analyse immer größerer Datenmengen zur Extraktion dieser komplexen Verhaltensmuster und Zusammenhänge notwendig. Des Weiteren müssen Klassifikatoren flexibel angepasst, kombiniert oder neu erstellt werden können bzw. sich selbstständig rekonfigurieren. Schon heute leisten Methoden der KI hierzu einen essenziellen Beitrag, um mit der Entwicklungsgeschwindigkeit von Botnetzen und anderer Malware schritthalten zu können. Hierdurch wird eine automatisierte Anpassung von Klassifikatoren ermöglicht, welche mit konventionellen Methoden nicht effizient durchführbar ist.

Insbesondere neuronale Netze erwiesen sich hier in der Vergangenheit als hilfreiches Mittel für die Klassifikation von Botnetzen. Aktuelle Entwicklungen wie z. B. Self-organizing Maps (SOM) oder Deep Learning, welches sich auf mehrschichtige neuronale Netze stützt, bergen ein großes Potential im Bereich der Botnetzdetektion und sind daher im Fokus aktueller Forschung.

Die bereits genannten Beispiele verdeutlichen sehr gut die allgemeine Problemstellung der Gewinnung von relevanten Erkentnissen aus den immensen Datenmenge von „rohen“ Daten. Ein weiteres Beispiel ist die Erstellung eines operativen Cyberlagebilds mit der Zielsetzung, durch den Einsatz von KI proaktiv auf mögliche Cyberrisiken und Cyberbedrohungen hinzuweisen. Wie in Abbildung 2 visualisiert, stehen dabei drei Aspekte im Vordergrund: (1) die Datenqualität, (2) das Vertrauen sowohl in die Gewinnung von rohen Daten als auch in die Analytics und (3) die Sicherstellung der Privatsphäre. Dabei ist das Vertrauen in die Analytics bzw. in die Algorithmen einer der wesentlichen Aspekte. Der Aspekt der Privatsphäre ist für die Erstellung eines Cyberlagebilds nicht auschlaggebend; es findet Anwendung in anderen Bereichen.

Nicht zuletzt ist die Robustheit der gängigen Verfahren des Maschinellen Lernens gegen Angriffe selbst von Interesse. Es wird erwartet, dass die Häufigkeit, Schwere und Effektivität derartiger Angriffe bei zunehmender Verbreitung von KI an Bedeutung gewinnen.

Deep Learning zur Erschließung von Massendaten für die signalbasierte Aufklärung

Prof. Dr. Frank Kurth, Forschungsgruppenleiter „Aufklärung und Störung“, Abteilung „Kommunikationssysteme“, Fraunhofer FKIE

Prof. Dr. Frank Kurth

Foto: Fraunhofer FKIE

Leistungsfähige Methoden zur Signaldetektion sorgen in verschiedenen Einsatzszenarien für die automatische Erfassung von weiterzuverarbeitenden Zielsignalen in großer Zahl. Häufig droht jedoch eine Überlastung des vorhandenen Personals bei der Weiterverarbeitung der resultierenden Massendaten. Wesentlich sind daher leistungsfähige Methoden zur zielgerichteten Klassifikation von Zielsignalen in Verbindung mit einer Vorselektion potenziell relevanter Daten. Bislang werden solche Aufgaben aufgrund des komplexen benötigten Vorwissens um Signalstrukturen, relevante kennzeichnende Merkmale und Kontextbedingungen von erfahrenem Personal erledigt.

Moderne, auch gerne dem Bereich der Künstlichen Intelligenz zugeordnete Methoden des Maschinellen Lernens (ML), bieten sich hier als Möglichkeit an, bestimmte Aufgaben der Signalklassifikation zu automatisieren und somit den menschlichen Bearbeiter zu entlasten. Hierzu zählen insbesondere Methoden aus dem Bereich des Deep Learnings wie Neuronale Netze, die in den letzten Jahren durch das Aufkommen neuer Methoden und die Verfügbarkeit paralleler Rechenstrukturen für signifikante Fortschritte in vielen Anwendungsgebieten des ML gesorgt haben.

In diesem Beitrag wird anhand dreier Beispiele illustriert, wie Methoden des Deep Learnings im Bereich der signalbasierten Aufklärung eingesetzt werden können.

Bitfolgen-Klassifikation

Eine Aufgabenstellung in der Fernmeldeaufklärung besteht darin, erfasste Signale bestimmten bekannten Funkverfahren zuzuordnen. Die mittels Breitbanddetektion vorselektierten Signale werden dabei einzeln mit möglichen, bekannten Verfahren verglichen. Weil Modulationsart und Bandbreite von Signalen des in Frage stehenden Verfahrens bekannt sind, ist es möglich, diese Tests auf eine Bitmustererkennung zu reduzieren. Somit kann das zu testende Signal probeweise in eine Bitfolge demoduliert und das demodulierte, digitale Signal auf spezifische Muster untersucht werden. Da sich diese Vorgehensweise zur Verfahrenserkennung in der Vergangenheit bewährt hat, stellt sich die Frage, wie für neue oder bislang unbekannte Übertragungsverfahren solche, zur Verfahrensklassifikation nutzbare, charakteristische Bitmuster bestimmt werden können.

Als Lösungsansatz hierzu wurden am Fraunhofer FKIE Klassifikationsmethoden für Bitfolgen basierend auf Convolutional Neural Networks (CNN) und Deep Belief Networks (DBN) entwickelt. Zur Untersuchung der Leistungsfähigkeit dieses Ansatzes wurde eine Einteilung von Bitfolgen in Komplexitätsklassen vorgenommen, wobei eine höhere Komplexitätsklasse eine höhere Schwierigkeit bei der Erkennung des der Bitfolge zugrundeliegenden Verfahrens bedeutet. Beispielsweise bezeichnet Komplexitätsklasse 1 reine Muster, Komplexitätsklasse 2 Wiederholungen und Komplexitätsklasse 3 boolesche Zusammenhänge zwischen drei Bits, wie etwa eine Parität. Untersuchungen haben dann gezeigt, dass die eingesetzten tiefen neuronalen Netze noch Bitfolgen der Komplexitätsklasse 5 erkennen können und auch selbst beim Vorliegen verschiedener Arten von Signalverzerrungen noch eine gute Erkennungsleistung erbringen. Im Vergleich hierzu hat der Mensch bereits Probleme bei der Erkennung eines Musters der Komplexitätsklasse 3.

Da ein leistungsfähiger Klassifikator basierend auf neuronalen Netzen in der Regel aber keine expliziten Aufschlüsse über die zugrundeliegenden Bitmuster liefert, bestehen zukünftige Aufgaben, neben weiteren konkreten Praxistests, in der automatischen Extraktion von für den Benutzer interpretierbaren Charakterisierungen eines interessierenden Funkverfahrens.

Robuste Sprecherklassifikation

Ein wesentlicher Beitrag zur Datenreduktion im Bereich erfasster Sprachsignale ist die Verwendung geeigneter Klassifikatoren, beispielweise zur gezielten Ermittlung von Landessprachen oder Sprechern. Am FKIE wurden im Zuge verschiedener Vorhaben die wichtigsten Methoden zur Sprecherklassifikation nach dem Stand der Technik implementiert und durch eigene Ansätze erweitert. Erweiterungen betreffen hierbei die Verwendung komplementärer, die menschliche Sprache charakterisierender Merkmale sowie die gezielte Kombination mehrerer verfügbarer Ansätze zur Dimensionsreduktion der einen Sprecher charakterisierenden Merkmalsdaten. Neuronale Netze kommen hier erfolgreich im Schritt der Methodenkombination zum Einsatz, da sie eine automatisierte Auswahl von Mischungsgewichten innerhalb eines komplexen Optimierungsproblems erlauben.

Tests auf Standard-Testkorpora zur Sprecherklassifikation zeigen, dass mittels des vorgeschlagenen Kombinationsansatzes

auch für Daten von schlechter Qualität, wie etwa Telefonie mit Störgeräuschen, eine signifikante Verbesserung der Klassifikationsleistung erzielt werden kann.

Neue Methoden des Deep Learnings

Bei allen Erfolgen von tiefen neuronalen Netzen in zahlreichen Anwendungen gibt es immer noch zahlreiche offene Fragen, gerade in Bezug auf die Interpretierbarkeit der Ergebnisse. So ist die Beantwortung von Fragen wie „Was wird von dem benutzen neuronalen Netz genau erkannt?“, „Was wird als einsatzrelevant klassifiziert?“ oder „Was kann das Netz nicht erkennen?“ für den konkreten Einsatz oftmals von hoher Bedeutung. Ein inhärentes Problem vieler populärer Netzstrukturen wie etwa der CNNs ist nämlich die oben bereits angesprochene, eingeschränkte Interpretierbarkeit.
Einen Schritt zur Beantwortung dieser Fragen bieten Projected Belief Networks (PBNs). Dies sind spezielle generative Modelle, die, wie ein am Fraunhofer FKIE erzieltes Forschungsergebnis zeigt, passend zu einem vorhandenen neuronalen Netz konstruiert werden können. Mithilfe der PBNs können dann automatisch Beispiele für die Klasse der durch das Netz erkannten Signale generiert werden. Dies verbessert einerseits

Deep Learning funktioniert über Netzstrukturen und besteht aus mehreren "Lagen". Input und Output sind bekannt, was innerhalb dieser Lagen geschieht, bleibt jedoch auch den Forschern verborgen. *Foto: Fraunhofer FKIE*

das Verständnis der Funktionsweise des Netzes und erlaubt es andererseits, Fehler zu korrigieren.
Arbeiten im Bereich der PBNs sind noch relativ jung, aber sehr vielversprechend. In Zukunft sollen die Netze auf verschiedene konkrete Szenarien im Aufklärungsbereich angewendet werden und somit existierende Ansätze, wie oben in den Bereichen der Bitfolgen- und Sprecherklassifikation illustriert, unterstützen.

Auswertung von Social Media

Prof. Dr. Ulrich Schade, Forschungsgruppenleiter „Informationsanalyse“, Abteilung “Informationstechnik für Führungssysteme“, Fraunhofer FKIE

Prof. Dr. Ulrich Schade

Foto: Fraunhofer FKIE

Die sogenannten „Sozialen Medien“ stellen eine wichtige und interessante Informationsquelle dar, da sich mit ihrer Hilfe Informationen (und Fehlinformationen) dezentral und schnell verbreiten. Die Auswertung dieser Medien ist daher aus vielen Blickwinkeln heraus relevant. Ein nicht zu unterschätzender Anteil bei einer solchen Auswertung entfällt dabei auf die Analyse von Meta-Daten, was im Folgenden zunächst an einem einfachen Beispiel erläutert werden soll. Daran anschließend wird erläutert, wie die Analyse von Meta-Daten auch für die Erkennung von „Fake News“ eingesetzt werden kann.

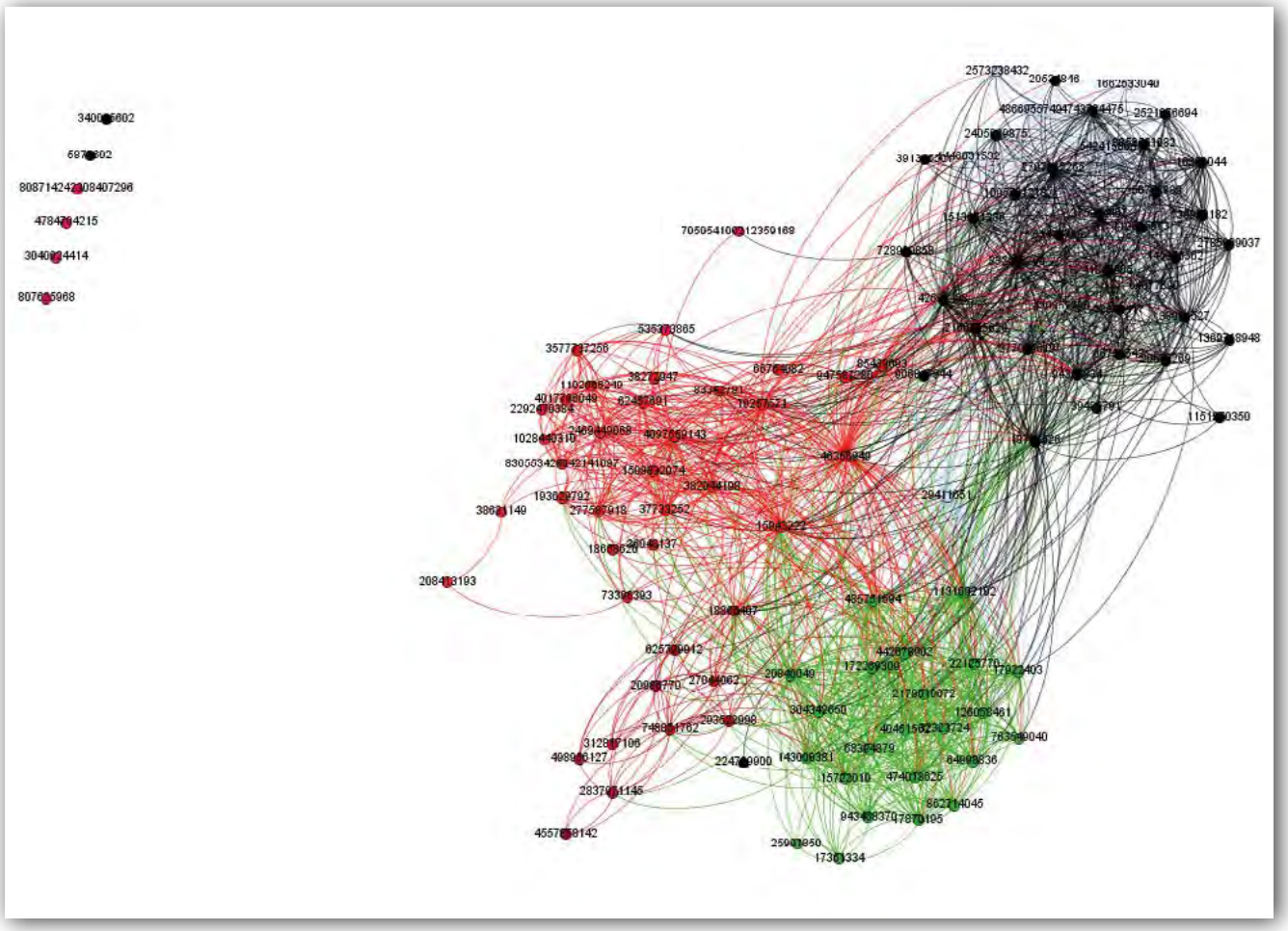
Meta-Daten von „Social Media“-Beiträgen umfassen unter anderem die Zeitangabe, zu der der Beitrag ins Netz gestellt wurde, Angaben zum „Reply“ und Angaben zum Sender (ID, Benutzername, Follower usw.). Neben diesen Meta-Daten und dem eigentlichen Inhalt des Beitrags gibt es etwa bei Twitter noch die Hash-Tags, die einen Hinweis auf den Inhalt des Beitrags liefern, die aber auch wie die Meta-Daten statistisch ausgewertet werden können. Tatsächlich können die Hash-Tags genutzt werden, um ein Korpus von Beiträgen zu einer Thematik anzulegen. Dazu wird zunächst ein Hash-Tag vorgegeben, unter dem das Zielthema vermutlich diskutiert wird, etwa „#brexit“ für die Brexit-Diskussion direkt vor der Abstimmung. Bei der Erstellung eines ersten Korpus mit diesem Hash-Tag als Filter können dann weitere, für das Zielthema relevante Hash-Tags bestimmt werden, im Beispiel etwa „#strongerin“, „#leave“ oder während der Abstimmung „#ivoted“. Unter Nutzung all dieser Hash-Tags als Filter kann dann ein das Zielthema repräsentierendes Korpus zusammengetragen werden.

Bei den eigentlichen Meta-Daten sind vor allem diejenigen für eine Analyse von Interesse, die sich mit dem Ziel der Erstellung von Kommunikationsnetzwerken auswerten lassen. Um dies zu illustrieren, haben wir vor der Bundestagswahl ein Twitter-Korpus erstellt, in dem die Tweets der zu dem Zeitpunkt im Bundestag vertretenen Abgeordneten (die Tweets über deren offizielle Twitter-Accounts) und die zugehörigen Replies enthalten sind. Daraus lässt sich ein Netzwerk dazu erstellen, wer mit wem Tweets austauscht, welches sich über die Häufigkeit des Austausches filtern lässt. Abbildung 1 zeigt eine solche Filterung, wobei Knoten und Verbindungen (nach Sender) entsprechend der Parteizugehörigkeit gefärbt sind (schwarz für CDU/CSU, rot für die SPD, grün für „Bündnis 90/Die Grünen“ und lila für „Die Linke“). Aus der Abbildung wird deutlich, dass es Kommunikationsstränge gibt, die zwischen den Parteigrenzen verlaufen. Die Ausprägung sogenannter „Echo Chambers“ ist allenfalls im Ansatz sichtbar.

Bei der Entwicklung eines Tools zur Erkennung von „Fake News“ sind wir pragmatisch vorgegangen. Ausgangspunkt war unser Tool zur Klassifizierung von Texten, das für die Erkennung von „Fake News“ angepasst wurde. Bei der eigentlichen Aufgabe wird dann den Nutzern gezeigt, wie dem Tool „Social Media“-Beiträge zur Verfügung gestellt werden. Dies führte zur Eingabe von Trainingskorpora, wobei ein solches Korpus jeweils aus zwei Mengen von Beispielen besteht. Die erste dieser Mengen besteht aus solchen Beispielbeiträgen, die durch den Nutzer als „Fake News“ klassifiziert werden, und die zweite Menge aus solchen, die dem Nutzer nicht als „Fake News“ gelten. Diese Mengen wurden dann für das Training des Tools (KI-Anwendung: Maschinelles Lernen) genutzt. Danach konnte das trainierte Tool als Filter verwendet werden. Ein solcher resultierender Filter erkennt natürlich nicht wirklich „Fake News“, sondern Beiträge, die den Beispielen, die der Nutzer als „Fake News“ vorklassifiziert hat, ähnlich sind. Können diese Beispiele im Wesentlichen einer Quelle oder einer Thematik zugeordnet werden, werden primär „Fake News“ aus dieser Quelle bzw. über diese Thematik als „Fake News“ erkannt, andere „Fake News“ aber nicht. Obwohl dieses Vorgehen, die Lösung des Wahrheitsproblems pragmatisch umgeht, ist für viele Nutzer dieser Schritt bereits zielführend. Texte, die von ihnen als „Fake News“ eingestuft werden und an denen sie primär interessiert sind, werden mit unserem pragmatischen Ansatz gefunden.

Bei der beschriebenen Erkennung von „Fake News“ aus „Social Media“-Beiträgen spielen Meta-Daten eine wichtige Rolle. Das Training des Klassifikationstools erfolgt ebenso wie die Klassifikation selbst über die Auswertung von sogenannten Merkmalen, die in Vektoren zusammengefasst werden, sodass die Ähnlichkeit als Abstand von Vektoren behandelt werden kann. Als Merkmale werden dabei insbesondere auch Meta-Daten genutzt. Beispielsweise weisen eine sehr hohe Rate, mit der ein Sender „Social Media“-Beiträge veröffentlicht, sowie bestimmte Follower-Strukturen darauf hin, dass der entsprechende Sender ein Bot ist, was die Wahrscheinlichkeit eines „Fake News“-Beitrags deutlich erhöht. Erklärungen und Begründungen dieser Art ergeben sich auch für den hier skizzierten Ansatz dadurch, dass neuste Entwicklungen aus dem Bereich „Explainable Artificial Intelligence“ (XAI) dazu genutzt werden, diejenigen Merkmale zu bestimmen, die das

Tool als grundlegend für seine Klassifikationsentscheidungen betrachtet. Das Verhalten des Tools wird für den Nutzer damit nachvollziehbar, was weitere Erkenntnisse dazu, was „Fake News“ ausmacht, vermittelt.



Austausch von Tweets innerhalb der Parteien und über Parteigrenzen hinweg. *Foto: Fraunhofer FKIE*

Managed Security Services bieten bestmöglichen Schutz vor Cyber-Angriffen

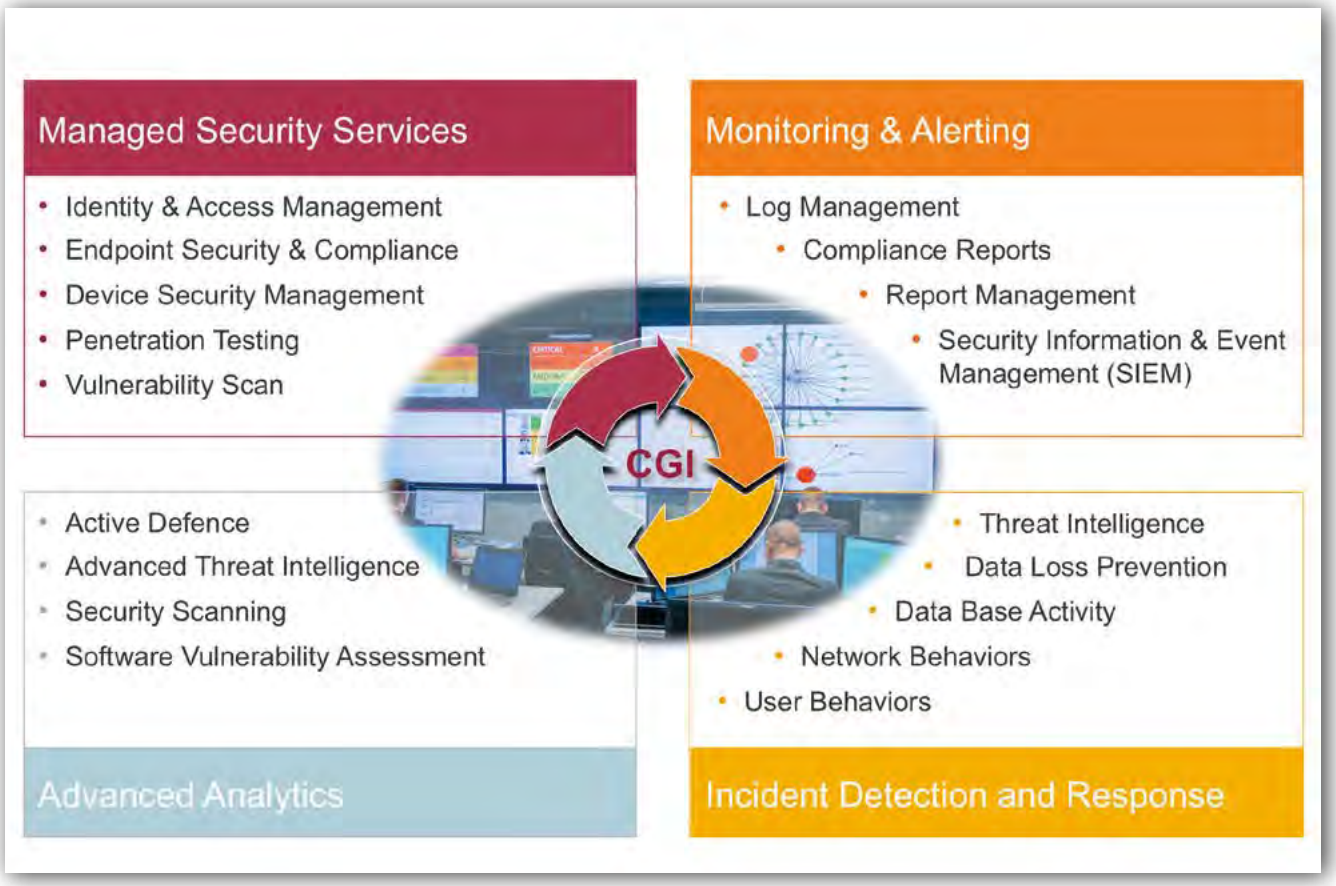
Autor: Frank Reiländer*

Cyber-Attacken stellen Behörden und Unternehmen vor immense Herausforderungen. Öffentliche Institutionen verfügen jedoch nur selten über die erforderlichen personellen Ressourcen, um Cyber-Risiken adäquat zu begegnen. Eine Lösung dafür bieten die Managed Services eines Security Operation Center.

Das Jahr 2017 war gekennzeichnet von einer Vielzahl von Cyber-Attacken durch Angreifergruppen wie DD4BC, Stealth Ravens und XMR Squad, die Erpressungsversuche starteten. Krypto-Trojaner wie beispielsweise Wanna Cry, der Mitte Mai Behörden und Unternehmen paralysierte und weltweit hunderttausende Rechner lahmlegte, verursachten einen immensen materiellen Schaden. Der Hackerangriff im letzten Jahr kostete Schätzungen zufolge alleine die dänische Containerschiff-Reederei Maersk mehrere hunderte Millionen US-Dollar. Hinzu kam der Imageschaden für die betroffen Institutionen.

Ergänzend zu Prävention und Absicherung werden Früherkennung und schnelle Analysen von Sicherheitsrisiken und -bedrohungen immer wichtiger. Gerade in Behörden fehlen aber oft die personellen und technischen Ressourcen und vor allem das umfassende IT-Security-Know-how, um ein eigenes Security Operation Center (SOC) aufzubauen, rund um die Uhr zu betreiben und fortlaufend mit aktuellen Sicherheitstechnologien auszustatten.

Behörden und Einrichtungen des Öffentlichen Sektors müssen heute sicherstellen, dass sie über eine effiziente und zuverlässige Security-Lösung verfügen. Sie sollten ihre spezifischen IT-Sicherheitsbedürfnisse abdecken und müssen vor allem gesetzliche Vorschriften, beispielsweise aus dem IT-Sicherheitsgesetz und der EU-Datenschutzgrundverordnung, und Compliance-Vorgaben erfüllen. Zudem sollte die IT-Sicherheitslösung die personenbezogenen und unternehmenskritischen Daten so schützen, dass ein zuverlässiger und reibungsloser IT-Betrieb gewährleistet ist.



Ein Security Operation Center (SOC) bietet Leistungen in vier großen Bereichen: Monitoring and Alerting, Incident Detection and Response, Advanced Analytics sowie Managed Security Services. Foto: CGI

Umfassendes Spektrum von Sicherheitsservices

Einrichtungen im Öffentlichen Sektor sind mit individuellen, nach dem Baukastenprinzip zusammengestellten Managed Security Services eines lokalen SOC-Spezialisten mit globaler Präsenz wie CGI in der Lage, Sicherheitsrisiken proaktiv und effizient zu managen. Vor allem aber erreichen sie damit einen maximalen Schutz vor Cyber-Bedrohungen.

Managed Security Services decken das gesamte Spektrum von End-to-End-Sicherheitsservices ab. Sie umfassen das Infrastruktur-Management, mit Teilbereichen wie Device-Management, Change-Management und die Sicherheitsanalyse, das Monitoring sowie das Reporting mit daraus abgeleiteten Handlungsempfehlungen. Das Security Information and Event Management (SIEM) as a Service ist ein zentraler Baustein im Rahmen des SOC-as-a-Service-Angebotes von CGI, der die etwa bei der Antivirensoftware, der Intrusion-Lösung oder der Benutzer-Authentifizierung anfallenden Informationen und Events erfasst, analysiert und korreliert. Hinzu kommen weitere Incident-&-Response-Funktionalitäten wie Threat Intelligence, Network and User Behaviors sowie Advanced Analytics und Active-Defence-Mechanismen.

Das Security Operation Center von CGI in Deutschland ist Teil eines weltweiten wachsenden SOC-Netzwerks, in dem monatlich hunderte Millionen Cyber-Angriffe erfasst und analysiert werden. CGI verfügt damit über ein immer aktuelles globales Wissen über die akute Bedrohungslage und kann Behörden und Unternehmen mit vielfach bewährten Praktiken und Sofortmaßnahmen bei verdächtigen Aktivitäten optimal beraten und schützen. Ein SOC-Service unterstützt Organisationen nicht nur durch ein vorausschauendes Risikomanagement sondern es entlastet Behörden und Einrichtungen im Öffentlichen Sektor auch, weil sie keine personal- und kostenintensiven IT-Security-Infrastrukturen aufbauen, betreiben und kontinuierlich auf dem aktuellen Stand halten müssen.

** Frank Reiländer ist Head of Cybersecurity bei CGI.*

Foto: CGI

Entscheidungsunterstützung zur Bewertung von Domänen

Dr. Tobias Albertsson, Abteilung „Cyber Analysis & Defense“, Fraunhofer FKIE

Dr. Tobias Albertsson

Foto: Fraunhofer FKIE

Spam ist ein allgegenwärtiges Ärgernis und wird in der Regel für bösartige Zwecke eingesetzt, u. a. zur Verbreitung von Schadsoftware. Auf diese Weise infizierte Computer, Smartphones oder IoT-Geräte werden für verschiedenartige Zwecke verwendet, wie z. B. für das Ausspähen von Informationen, für sogenannte Denial-of-Service-Angriffe oder wiederum den Versand von Spam. Häufig werden die infizierten Geräte auch zu sogenannten Botnetzen mit teilweise mehreren Millionen infizierter Geräte zusammengeschlossen. Damit unterstützen Cyberkriminelle ihre verschiedenen Geschäftsmodelle wie Spionage, Erpressung, Betrug und Sabotage.

Botnetze sind eine ernste Bedrohung. Häufig werden durch sie auch Geräte beschädigt, die nicht infiziert sind. Ein prominentes Beispiel war ein Mirai-Botnetz, welches dazu führte, dass hunderttausende Telekom-Router nicht mehr richtig funktionierten.

Verschleierung der Botnetze

Botnetze werden üblicherweise von einem oder mehreren sogenannten Botmastern kontrolliert. Dies sind Personen, die mit den infizierten Bots kommunizieren und diesen Befehle übermitteln. Dabei gibt es grob zwei Hauptkategorien für die Art der Kommunikation: Peer2Peer (P2P) und zentralisiert. Bei P2P wird ein dezentrales Netzwerk verwendet, in dem Befehle durch die Bots selber bis zum Empfänger-Bot weitergeleitet werden. Die meisten heutigen Botnetze verwenden jedoch ein zentralisiertes Modell. Die Bots kontaktieren über Internetdomänennamen einen oder mehrere zentrale Server, sogenannte Command-and-Control-Server, von denen sie dann Befehle erhalten. Dabei werden von den Botmastern Techniken wie die Verwendung von Domain Generation Algorithms (DGAs) eingesetzt, um die Erkennung und Störung der Kommunikation zwischen Bots und Servern zu erschweren. DGAs erzeugen Listen mit teilweise mehreren tausend neuen Domänen pro Tag, die von den Bots kontaktiert werden können. Diese Technik zielt darauf ab, es Verteidigern möglichst zu erschweren, Domänennamen in Blocklisten aufzunehmen, damit den Zugriff der Bots auf die C&C-Server und letztlich Schaden bei den Opfern zu verhindern.

An diesem Punkt der Kommunikation zwischen Bots und C&C-Servern über Domänennamen setzt die hier beschriebene Forschung von Fraunhofer FKIE an. Auf Basis von durch die Analyse von Schadsoftware erlangtem Wissen wurde bei Fraunhofer FKIE ein System unter Verwendung von Künstlicher Intelligenz zur Bewertung von Domänen entwickelt.

Domänengenerierung

Mittels Reverse Engineering wurde eine große Anzahl von Schadsoftware analysiert und die DGAs wurden extrahiert sowie reimplementiert [1]. Viele der auf diese Art analysierten DGAs verwenden randomisierte Kombinationen von alphanumerischen Zeichen, einige erzeugen aber auch korrekte oder verstümmelte Worte als Ausgabe. Während randomisierte Domänennamen vergleichsweise einfach zu erkennen sind, ist bei wort-basierten DGAs eine hohe Wahrscheinlichkeit von Kollisionen mit legitimen Domänen gegeben. Dies macht eine Klassifizierung von Domänennamen in „gut“ oder „böse“ schwierig. Darüber hinaus gibt es auch Domänen, die ursprünglich für legitime Zwecke verwendet wurden, mittlerweile aber

Legitim (nicht-DGA)	Wort-basierter DGA	Randomisierte DGAs	
	gozi	ramnit	nymaim
elfagr.org	laterconnection.com	lbnlugbrt.com	zrriupswiz.org
tokopedia.com	exposedlives.ru	orokljeyl.com	uljzuuq.net
redonetype.com	peoplegovernment.pw	pwpcpofiaa.com	lfutxhebnzf.ru
eastday.com	certainmeans.com	rbmtdngjoey.com	zeiqroll.info

Tabelle 1: Beispiele von legitimen Domänennamen und DGA-Domänen

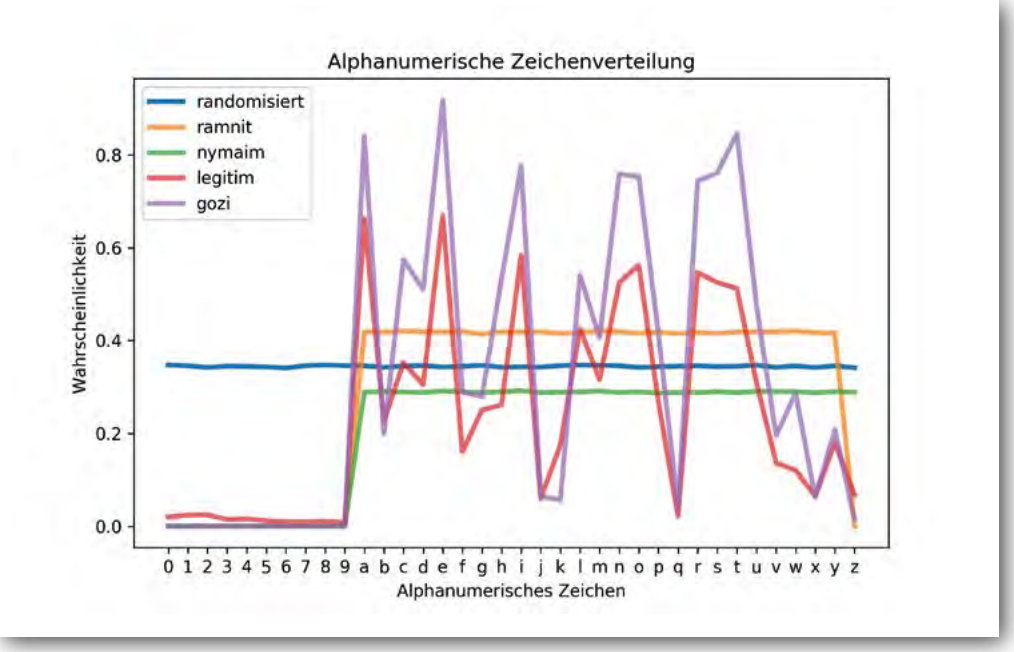
Grafik: Fraunhofer FKIE

kompromittiert wurden und stattdessen für bösartige Zwecke verwendet werden. Basierend allein auf dem Domänennamen kann also nicht definitiv entschieden werden, ob es sich um eine Domäne handelt, die für gutartige oder bösartige Zwecke verwendet wird. Dennoch ist es mit Künstlicher Intelligenz möglich zu unterscheiden, ob der Domänenname mittels eines DGAs generiert wurde oder nicht.

Grundidee ist es dabei, mittels Künstlicher Intelligenz Modelle auf den Daten bekannter DGAs zu trainieren. Dazu werden die von den DGAs erzeugten Domänenlisten zunächst um solche Domänen bereinigt, die durch Kollisionen mit legitimen Domänen entstehen. Hierzu können z. B. Listen von beliebten Domänen wie ALEXA [2] und MAJESTIC [3] verwendet werden. Diese mutmaßlich legitimen Domänen werden aus den Trainingsdaten entfernt.

Merkmale von DGAs

In Tabelle 1 sind Beispiele von DGA- und nicht-DGA-Domänennamen aufgeführt. Um einen robusten Klassifikator entwickeln zu können, ist die Auswahl der betrachteten Merkmale entscheidend. Die meisten DGAs nutzen randomisierte Zeichen.



Verteilung alphanumerischer Zeichen von legitimen Domännamen (ALEXA & MAJESTIC), randomisierten DGAs (ramnit, nymaim), wort-basiertem DGA (gozi) und zufällige alphanumerischen Zeichen.

Grafik: Fraunhofer FKIE

Die Zeichenverteilung unterscheidet sich stark von den meisten legitimen Domänen. Entsprechend erscheint die Zeichenverteilung ein sinnvolles Merkmal zu sein. In Abbildung 1 sind die Verteilungen alphanumerischer Zeichen für verschiedene Quellen zu sehen. Für „ramnit“ und „nymaim“ ist es leicht, den Unterschied zu legitimen Domänennamen zu sehen, für „gozi“ ist es schwieriger. Diese Beispiele verdeutlichen, dass ein einzelnes Merkmal für eine robuste Klassifikation nicht ausreicht.

Daher werden für den Klassifikator mehr als tausend unterschiedliche Merkmale kombiniert, wie z. B. die Häufigkeit des Auftretens einzelner Zeichen und paarweiser Zeichen (Bigramme), die Länge und Entropie der Domänennamen und das Vokal-zu-Konsonanten-Verhältnis. Die Klassifizierung ist dadurch eine mehrdimensionale, komplexe Aufgabe. Genau hier kommen aber die Stärken von Künstlicher Intelligenz bzw. Machine Learning (ML) zum Einsatz. ML zeichnet sich insbesondere bei der Mustererkennung in komplexen Daten aus. Zusätzlich kann ML fast selbstständig auf den bereitgestellten Trainingsdaten lernen. Dennoch bleibt der Mensch wichtig, da der ML-Klassifikator zwar eine sinnvolle Entscheidungsunterstützung darstellt, aber letztlich auf der Wahl der Merkmale und der Trainingsdaten basiert. Eine menschliche Supervision ist letztlich unumgänglich.

Bewertung

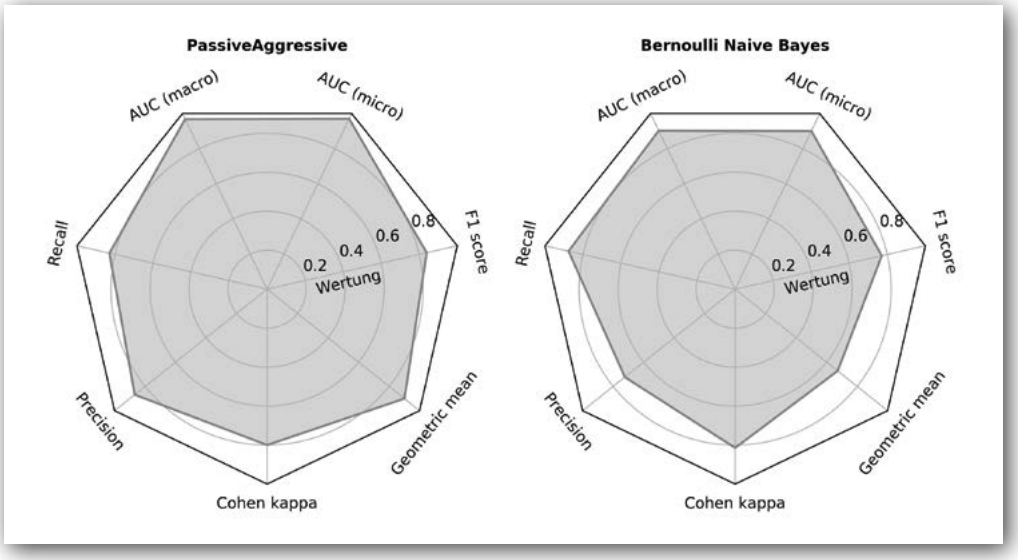
Zu dieser Supervision zählt die Parametrisierung des MLs, durch die angegeben wird, wie stark die verwendeten Modelle neue Daten gewichten. Die Wahl der Parameter ist maßgeblich für die spätere Genauigkeit des Klassifikators. Eine schlechte Wahl der Parameter kann zu sehr allgemeinen oder extrem spezifischen Modellen führen. Beides wird zu einer großen Zahl an Fehlklassifikationen führen.

Darüber hinaus hat die Wahl eines für die Problemstellung geeigneten ML-Algorithmus einen entscheidenden Einfluss auf die Leistungsfähigkeit des Klassifikators. Daher werden derzeit verschiedene Methoden wie z. B. Stochastic Gradient Descent, Perceptron, Multi-layered Perceptron, Passive-Aggressive und Bernoulli Naive Bayes evaluiert.

Die Leistungsfähigkeit der Methoden und Modelle wird mit verschiedenen Metriken bewertet, die die Genauigkeit der Klassifizierung beschreiben. Je näher die Werte an 1.0 heranreichen, desto genauer ist der Klassifikator. Abbildung 2 zeigt, dass der Passive-Aggressive-Algorithmus mit den oben genannten Merkmalen weit besser für eine Bewertung von Domänennamen bzgl. ihrer Zugehörigkeit zu DGAs geeignet ist als ein Bernoulli-Naive-Bayes-Klassifikator. Bei beiden Methoden handelt es sich um vergleichsweise einfache und schnelle Algorithmen. Derzeit werden weitere komplexere Methoden ausgewertet, bei denen eine noch höhere Genauigkeit zu erwarten ist.

Gutes von Schlechtem trennen

Mit den hier vorgestellten Klassifikatoren ist eine Einschätzung möglich, ob eine Domäne von einem DGA erstellt wurde oder nicht. Eine mittels eines DGA erzeugte Domäne ist ein starker Hinweis auf eine bösartige Verwendung der Domäne. Basierend auf dieser Ersteinschätzung kann ein menschlicher Analyst mithilfe weiterer Information, wie z. B. IP-Reputationsdaten oder WHOIS-Daten, entscheiden, ob es sich bei den Domäne tatsächlich um bösartige genutzte Domänen handelt. Nur so ist es möglich, die gewaltige Anzahl potenziell bösartiger Domänen in sinnvoller Zeit zu überprüfen, zu klassifizieren und Schaden zu verhindern.



Vergleich verschiedener Metriken für zwei Klassifikatoren. Werte näher an 1.0 sind besser.

Foto: Fraunhofer FKIE

[1] https://dgarchive.caad.fkie.fraunhofer.de/
[2] https://www.alexa.com/siteinfo
[3] https://majestic.com/

Digitale Transformation mit Atos sicher gestalten

Atos ist ein führender Anbieter für digitale Transformation und vertrauenswürdiger Partner für Sicherheits- und Verteidigungsorganisationen weltweit. Wir entwickeln hoch innovative militärische Informationssysteme und liefern Dienstleistungen sowie Mehrwertdienste, die den hohen, komplexen Anforderungen der Digitalisierung für missionskritische Umgebungen gerecht werden. Als Systemintegrator und Technologieanbieter mit europäischen Wurzeln unterstützt Atos seine Kunden, ihren Auftrag effektiv und effizient erfüllen zu können und damit die Sicherheit zu gewährleisten.

Foto: GettyImages

Die adäquate Informationsversorgung mittels IT-basierter Systeme ist für Verteidigungsorganisationen der kritische Erfolgsfaktor für die Auftragserfüllung. Darüber hinaus gewinnen die Souveränität im Cyberraum sowie die erfolgreiche Abwehr von Cyberbedrohungen zunehmend an Bedeutung. Zuverlässiger Betrieb der IT, Cyber-Sicherheit über alle Fachbereiche hinweg und die Fähigkeiten zur vernetzten Aufklärung und Wirkung auch im Cyber- und Informationsraum sind zunehmend unverzichtbare Grundlagen um Führung, Aufklärung und Wirkung in den „klassischen“ Dimensionen auch zukünftig verlässlich zu ermöglichen. Atos bietet einen wertbringenden Beitrag zum Erfolg, u.a. in den Bereichen Nachrichtengewinnung und Aufklärung, Führungsunterstützung und Logistik.
Atos entwickelt militärische, zukunftssichere Cloud-Lösungen, welche die zweckmäßige und dynamische Bereitstellung und Verarbeitung sensibler Informationen (etwa Verschlusssachen) ermöglichen.
Zudem ist die Fähigkeit zum flexiblen Informationsaustausch, je nach Bedürfnissen der Mission und Lage, zwischen verschiedenen Informations- und Sicherheitsdomänen essentiell. Für den militärischen Einsatz liefert Atos verlässliche, verlegefähige Cloud-Infrastrukturen, die beispielsweise in Containern eingerüstet den weltweiten klimatischen Bedingungen sowohl im Betrieb als auch beim Transport per Flugzeug oder Schiff standhalten.
Atos unterstützt proaktiv die Digitalisierung der Landstreitkräfte durch Konzepte eines durchgängigen Verbundes digitaler Datenverarbeitungs- und Datenübertragungssysteme.
Um sich gegen Bedrohungen im Cyberraum proaktiv zu schützen, Angriffe erkennen und abzuwehren sowie relevante Aktivitäten und Zustände überwachen zu können, vertrauen Organisationen weltweit auf Atos-Lösungen, die in Europa hergestellt werden. Dazu gehören neben den Mission Critical Systems auch Technologien zur Erhöhung der Resilienz, Ermöglichung der Bedrohungserkennung und -abwehr sowie High Performance Computer für echtzeitnahe Analysen von umfangreichen und komplexen Datenvolumina und der Entscheidungsunterstützung.
Atos ist durch das Bundesamt für Sicherheit in der Informationstechnik zertifizierter IT-Sicherheitsdienstleister für die Bereiche Informationssicherheitsberatung, Informationssicherheitsrevision, Penetrationstests sowie Trustcenter. Damit ist Atos in der Lage seine Kunden durch Risikoanalysen, Sicherheitskonzepte, Audits und Revisionen auf Basis anerkannter Standards und hoher Güte zu unterstützen.
Atos ist ein weltweit führender Anbieter von Dienstleistungen und Lösungen zum digitalen Product Life Cycle Management von Spezifikation, Entwicklung, Erprobung, Nutzung bis hin zur Obsoleszenz komplexer Technologieprodukte für Branchen wie z.B. Aerospace, Automotive, Electronics sowie der wehrtechnischen Industrie. Als Mitglied der Industrial Data Space Association e.V. und Digitalisierungs- Partner führender Industrieunternehmen schafft Atos Möglichkeiten zum sicheren Austausch von Daten und deren kontrollierter Nutzung und Verknüpfung zwischen Partnern. Dies ermöglicht Aufbau und Betrieb moderner Geschäftsökosysteme für z.B. Industrie- und Rüstungsgüter im Kontext Internet der Dinge, effizientere Gestaltung von Prozessen und Erschließung neuer Wertschöpfungsketten.
Atos beschäftigt circa 100.000 Mitarbeiter in 72 Ländern mit einem Jahresumsatz von rund 12 Milliarden Euro. Der Konzern ist der weltweite IT-Partner der Olympischen und Paralympischen Spiele. Atos firmiert unter den Marken Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify und Worldline. Atos SE (Societas Europaea) mit Sitz in München und Paris, ist an der Pariser Börse als eine der 40 führenden französischen Aktiengesellschaften (CAC40) notiert.

Atos Deutschland
Hubert Geml
hubert.geml@atos.net
de.atos.net

Anwendungen der Künstlichen Intelligenz in der einsatzbezogenen IT

Dr. Michael Gerz, Forschungsgruppenleiter „Interoperability & Testing“, Abteilung „Informationstechnik für Führungssysteme“, Fraunhofer FKIE

Dr. Michael Gerz

Foto: Fraunhofer FKIE

KI und Deep Learning

Die Künstliche Intelligenz (KI) erlebt derzeit eine Renaissance. Vielfach wird sie gleichgesetzt mit „Deep Learning“, einer Technologie, die auf dem Prinzip der neuronalen Netze beruht. Letztere feierte in den vergangenen Jahren Erfolge in Anwendungsbereichen, die zuvor mit gängigen Methoden nicht in den Griff zu bekommen waren. Der technologische Durchbruch wurde dabei durch drei wesentliche Faktoren erzielt: Neue Architekturen und Trainingsverfahren für neuronale Netze, enorm gesteigerte Rechenleistung durch den Einsatz hocheffizienter Grafik-Prozessoren und die Verfügbarkeit großer Datenmengen (Stichwort: Big Data), die für das Anlernen der neuronalen Netze zwingend notwendig sind.

Deep Learning ist besonders erfolgsversprechend bei klar abgegrenzten Problemen, die sich mit regelbasierten Ansätzen nur schwer erfassen lassen. Aktuelle Forschungsarbeiten widmen sich dabei im Fokus der Analyse und Synthese von Bildern und Videos (z. B. Klassifikation von Objekten, Szenen-Erkennung) sowie der Verarbeitung gesprochener und geschriebener Sprache. Diese Einzellösungen können auch kombiniert werden. So ist es bereits heute möglich, Fotos automatisiert mit einer Bildunterschrift zu versehen. Neuronale Netze werden anhand von Hollywood-Filmen darauf trainiert, einen Dialog mit einer anderen Person zu führen; die Trainingsdaten werden dabei von einem anderen neuronalen Netz erzeugt, welches die gesprochene Sprache aus den Filmen zunächst verschriftlicht. Last but not least ist es möglich, Politikern in aufgezeichneten Videobotschaften neue Reden „unterzujubeln“ – inklusive Synchronisierung der Gestik zur authentisch synthetisierten, gesprochenen Sprache. (Auf das Problem von Fake News sei an dieser Stelle nicht eingegangen.)

KI im militärischen Kontext

Im Bereich der einsatzbezogenen IT können Ansätze aus der KI an vielen Stellen operationelle Vorteile schaffen. Folgt man dem Thesenpapier „Wie kämpfen Landstreitkräfte künftig?“ des Kommandos Heer, so wird das Gefechtsfeld zukünftig vermehrt autonome bzw. teilautonome Systeme (insbesondere Drohnen) umfassen, die ihre Effektivität speziell in Schwärmen entfalten. Für derartige Systeme sind Methoden der KI essenziell. Darüber hinaus können Systeme zur Identifizierung und Klassifikation von Objekten in Bilddaten bei der Aufklärung unterstützen (z. B. bei der Erkennung potenzieller Heckenschützen). Sie sind besonders dann effektiv, wenn sehr große Datenbestände analysiert werden müssen. Ein wesentlicher Vorteil dabei ist, dass KI-Systeme keinen Ermüdungserscheinungen unterworfen sind. KI-Systeme sollten dem Operateur letztlich aber nicht Entscheidungen abnehmen, sondern lediglich unterstützen, indem sie bspw. eine Vorselektion vornehmen oder Priorisierungsvorschläge machen. Dies ist insbesondere vor dem Hintergrund zu sehen, dass bei der Anwendung von neuronalen Netzen die Kausalität unklar ist, d. h. es kann nicht deduziert werden, warum ein System zu einem bestimmten Ergebnis gelangt ist.

Lösungen für die taktische Ebene

Der Einsatz von KI-Methoden wird die Interaktion des Soldaten mit seinem Führungsinformationssystem (FüInfoSys) in den kommenden Jahren maßgeblich verändern und erleichtern. Die größten Veränderungen sind dabei auf der taktischen Ebene zu erwarten. Die folgenden Szenarien sind denkbar:

- Anstatt taktische Zeichen nach APP-6 über komplexe Menüstrukturen auszuwählen, zeichnet der Soldat Symbole per Stift auf die Lagekarte. Diese werden dann mittels KI automatisch in eine formale Repräsentation überführt. Dabei ist das FüInfoSys in der Lage, Vorschläge bereits auf Basis unvollständiger Zeichnungen zu unterbreiten.
- Taktische Funksprüche der Soldaten werden, dank der Fortschritte in der Spracherkennung, in Echtzeit ausgewertet und die daraus extrahierten Informationen in das digitale Lagebild bzw. eine Meldung überführt. Per Sprachsteuerung kann der Richtschütze zudem Parameter für Waffensysteme voreinstellen. Die Anweisung „Feind auf 2 Uhr“ steuert dann z. B. die Turmausrichtung.
- Auch die Fortschritte bei der Bildanalyse lassen sich für militärische Einsätze nutzen. So kann ein Soldat das Foto eines Objekts (z. B. einer Person, eines Gebäudes, eines IEDs, …) aufnehmen. Mithilfe einer Objektklassifikation – an dieser Stelle kommt wieder die KI ins Spiel – sowie verfügbarer Metadaten (Zeit, Ort, Nutzer) wird weitgehend automatisiert ein strukturierter Report erstellt.

- Anhand von Satellitenbildern lassen sich Veränderungen der natürlichen und urbanen Strukturen analysieren und so z. B. Einschätzungen bzgl. der Passierbarkeit des Geländes treffen.

Welche KI-Lösungen sich letztlich im operationellen Einsatz bewähren und welche sich als technische Spielereien erweisen, müssten umfangreiche Feldtests zeigen. In allen Szenarien muss der Soldat stets die Kontrolle über den Prozess behalten und die letzte Entscheidung treffen. Da die Spracherkennung – insbesondere unter den besonderen akustischen Randbedingungen im taktischen Einsatz – auf absehbare Zeit nicht fehlerfrei arbeiten wird, sind besondere technische und organisatorische Vorkehrungen zu treffen, um Fehlentscheidungen aufgrund von Falschinformationen zu verhindern. (Für weitere Aspekte der Sprachsignalverarbeitung sei auf die Beiträge von Prof. Kurth und Herrn von Zeddelmann in diesem Heft verwiesen.)

Strukturierte und unstrukturierte Informationen

Ein Trend, der sich abzeichnet, ist das Zusammenwachsen von unstrukturierten Informationen auf der einen Seite (Funksprüche, Chat-Meldungen, Multimediainhalte, etc.) und strukturierten Informationen (Sensordaten, formatierte Meldungen) auf der anderen Seite. Je mehr unstrukturierte Informationen der taktischen Ebene in das digitale Lagebild einfließen, umso besser sind die Möglichkeiten zur Informationsauswertung, was wiederum neue Anwendungen der KI „befeuern“ wird. Durch die Nutzung von KI-Lösungen ist es möglich, mehr Informationen mit kürzerem Zeitverzug bereitzustellen; durch Überführung unstrukturierter Information in ein digitales Lagebild wird zudem der Austausch mit internationalen Partnern erleichtert.

Intelligente Systeme durch Ontologien

Auch jenseits von Deep Learning bieten sich zahlreiche Möglichkeiten, Führungsinformationssysteme „intelligenter zu machen“. Durch die Nutzung von domänenspezifischen Ontologien ist es z. B. möglich, die Suche nach Informationen deutlich zu verbessern. Sucht der Nutzer z. B. nach „Hindernissen“ in seinem Operationsraum, sollten auch alle Meldungen erscheinen, in denen der Begriff „Minenfeld“ auftaucht. Das Einbeziehen von taxonomischen Beziehungen bietet insbesondere bei unstrukturierten Meldungen einen großen Mehrwert. Mit dem MIP Information Model (MIM; https://www.mimworld.org), an dem das Fraunhofer FKIE maßgeblich mitgewirkt hat, existiert ein international anerkannter Standard, der eine derartige Ontologie für Command & Control (C2) definiert. Die damit verbundenen Potenziale sind durch heutige FüInfoSys bei weitem nicht ausgeschöpft.

Fazit

Auch jenseits der großen Themen wie „autonome Systeme“ bietet die KI vielfältige Möglichkeiten, um bestehende einsatzbezogene IT benutzerfreundlicher, interoperabler und effizienter zu gestalten. Die KI wird den Soldaten nicht ersetzen, ihn aber in spezifischen Situationen unterstützen – etwa bei der Informationssuche und -analyse. Zweifelsohne wird der Bereich „Aufklärung“ hiervon besonders profitieren.

Lösungen auf Basis von neuronalen Netzen liefern bei eng umrissenen Aufgaben bereits heute in vielen Fällen nachweislich bessere Ergebnisse als ihre menschlichen Counterparts. Die Entwicklungen auf dem zivilen Markt zeigen, dass Lösungen aus dem KI-Umfeld in viele Anwendungen Einzug finden; deren Integration erfolgt aber häufig „lautlos“ und subtil und wird durch den Nutzer allenfalls durch eine höhere „Erwartungskonformität“ realisiert. Nur wenige hinterfragen, aufgrund welcher technischer Verfahren Google zum Ranking seiner Suchergebnisse gelangt, obgleich darauf weitreichende Entscheidungen basieren können. In militärischen Anwendungen hingegen liegt es gleichsam in der Verantwortung der Systementwickler als auch der Nutzer, den Einsatz von KI hinsichtlich ihres Nutzens, aber auch ihrer Risiken kritisch zu bewerten bzw. einzuschätzen.

Sprachsignalverarbeitung für den Einsatz: Aktuelle Möglichkeiten und Grenzen von KI-Methoden

TORR Dirk von Zeddelmann, M.A., J6, Kommando Strategische Aufklärung,
Prof. Dr. Frank Kurth, Forschungsgruppenleiter „Aufklärung und Störung“,
Abteilung „Kommunikationssysteme“, Fraunhofer FKIE

TORR Dirk von Zeddelmann

Foto: privat

Prof. Dr. Frank Kurth

Foto: Fraunhofer FKIE

Im Aufgabenbereich der signalerfassenden Aufklärung fallen aufgrund neuer, leistungsfähiger Methoden zur Signalerfassung und -vorauswertung in erheblichem Umfang Signaldaten an, die im Weiteren analysiert und ausgewertet werden müssen. Demgegenüber steht eine geringe Kapazität verfügbarer Bearbeiter und Auswerter, insbesondere vor dem Hintergrund wechselnder Einsätze und einsatzrelevanter, oft exotischer Sprachen. Um diese Herausforderungen auftragsgerecht bewältigen zu können, werden dringend Mechanismen zur automatischen Sprachverarbeitung benötigt, die den Bearbeiter zielführend entlasten und helfen, alle potenziell relevanten Signalmassendaten zu bearbeiten. Verbesserte Methoden aus dem Bereich der KI – insbesondere Methoden zum Maschinellen Lernen – bieten sich an dieser Stelle besonders an.
In diesem Beitrag werden zunächst die zahlreichen Einsatzmöglichkeiten der Sprachverarbeitung innerhalb der signalerfassenden Aufklärung skizziert und die besonderen Herausforderungen in diesem Umfeld aufgezeigt. Danach werden das Potenzial neuer KI-Methoden beleuchtet, aber auch aktuelle Grenzen aufgezeigt.

Einsatzmöglichkeiten von Methoden der Sprachsignalverarbeitung

Eine breite Palette von Methoden der automatischen Sprachverarbeitung ist in der signalbasierten Aufklärung gewinnbringend anwendbar. Zunächst kann eine automatische Sprachsignaldetektion genutzt werden, um entweder Sprachübertragungen im breitbandigen Funksignalspektrum aufzufinden oder, beim Vorliegen von Schmalbandsignalen, Sprachanteile innerhalb langer zeitlicher Aufzeichnungen zu lokalisieren. Vielversprechende Ansätze hierzu wurden in der Vergangenheit bei Fraunhofer FKIE entwickelt und von Seiten der Bw erfolgreich erprobt.
Nach dieser sensornahen Signaldetektion ist eine gezielte Sichtung und Reduktion der hierbei massenhaft anfallenden Sprachsignale notwendig. Hierzu bietet es sich an, je nach Auftrag, gezielt bestimmte Sprachverarbeitungstechniken zu verwenden. Sucht man explizit Sendungen bestimmter Personen, können Methoden der Sprechererkennung eingesetzt werden. Sind Sendungen zu bestimmten, vorab bekannten Themen interessant, können gezielt themenspezifische Schlüsselworte gesucht werden. Ebenso lassen sich spezifische Wortfolgen, beispielsweise Rufkennungen, oder bekannte Rufnamen detektieren. Auch das Ausfiltern gesprochener Landessprachen aus Signalaufzeichnungen stellt eine wichtige Technologie dar. Nach erfolgter Reduktion auf die relevanten Sprachanteile einer Signalaufzeichnung ist eine weitere Analyse, möglichst mit einer Verschriftung oder sogar einer automatischen Übersetzung aus der Zielsprache ins Deutsche, wünschenswert.
Neben den hier aufgeführten Anwendungen innerhalb eines klassischen signalbasierten Aufklärungsablaufs, bietet die automatische Sprachverarbeitung auch Lösungen für spezialisierte Aufgaben wie etwa die Detektion und Decodierung spezieller Sendungsformen.

Herausforderungen

Die größten Herausforderungen beim Einsatz automatisierter Sprachverarbeitung in diesem Umfeld sind ein Mangel an verschiedensten Ressourcen sowie die heterogene und oft schlechte Qualität der anfallenden Daten. Hierbei fehlen nicht nur für neue Einsatzgebiete und somit neue Zielsprachen verfügbare sprachenkundige Bearbeiter, sondern auch verfügbares Audiomaterial. Problematisch ist hier beispielsweise, dass State-of-the-art-Methoden zur automatischen Verschriftung oder auch „nur“ zur Schlüsselworterkennung (automatische Verschriftung eines eingeschränkten Wortschatzes) aufgrund des vorab nötigen Trainingsschrittes gerade auf das Vorliegen einer beträchtlichen Menge an annotierten Sprachaufnahmen angewiesen sind. Der personelle Aufwand zum Anfertigen geeigneter Annotationen ist hierbei nicht zu unterschätzen.
Für eine signifikante Verschlechterung der angepriesenen Leistungsfähigkeit von Methoden auf dem Stand der Technik sorgen die meist sehr schlechten Signalqualitäten, die im Aufklärungsumfeld vorliegen. Diese sind die Summe des

nicht-kooperativen Erfassungsszenarios, möglicher Umwelteinflüsse wie Windgeräusche, diverser Übertragungsfehler und nicht zuletzt der stark variierenden Aussprache seitens der Zielpersonen. Erschwerend hinzukommt, dass der Erfolg von Methoden wie etwa Sprecher- oder Schlüsselworterkennung stark abhängig vom jeweils betrachteten Übertragungskanal und dessen zur Verfügung stehenden Bandbreite sind. So wird ein speziell für HF-Funkübertragungen konfigurierter Schlüsselworterkenner nicht ohne weiteres für Satellitenübertragungen nutzbar sein, selbst wenn dieselben Sprecher aktiv sind. Somit ist ein aufwendiges separates Training für jeden Übertragungskanal nötig.

vollautomatisch durchgeführt werden können. Man spricht hier von Ende-zu-Ende-Verarbeitung: Idealerweise erhält das neuronale Netz zum Zwecke des Trainings eine umfängliche Menge von Beispielen für ein korrektes Eingabe-Ausgabe-Verhalten, wie etwa Paare von Sprachsignal und zugehöriger Verschriftung. Nach dem Trainingsschritt ist das Netz dann so konfiguriert, dass bei Eingabe eines Sprachsignals die wahrscheinlichste Verschriftung ausgegeben wird.
Aber auch bei fast allen anderen obigen Aufgaben der Sprachverarbeitung können neuronale Netze gewinnbringend und zielgerichtet eingesetzt werden. So steigen die Möglichkeiten zum Transfer von bereits Gelerntem auf neue Problemfelder,

Potenziale und Grenzen von KI-Methoden

Neue KI-Trends betreffen insbesondere große Fortschritte auf dem Gebiet der künstlichen Neuronalen Netze. Hier konnten signifikante Fortschritte bei Standardaufgaben der Mustererkennung und des Maschinellen Lernens erzielt werden, wie etwa in der Bilderkennung oder der Entwicklung von dem Menschen überlegenen Computerprogrammen für das Schach- und Go-Spiel. Auf die Sprachverarbeitung haben KI-Methoden die positive Auswirkung, dass wesentlich komplexere Sprach- und Sprechermodelle effektiv genutzt werden können. Im Bereich der automatischen Verschriftung konnte so mittels neuronaler Netze seit langem wieder ein Quantensprung bei der Reduktion der Fehlerrate erzielt werden.
Eine besondere Stärke der sogenannten Deep-Learning-Methoden ist, grob gesprochen, dass die „Black Box“, also die Einheit, die vollautomatisch Daten analysiert und klassifiziert, größer gemacht wird. Größer bedeutet dabei, dass viele Vor- und Nachverarbeitungsschritte, die sonst noch manuell realisiert oder problemangepasst entwickelt werden mussten, nun wie etwa bei der Übertragung der Spracherkennung von einer bereits vom Erkenner beherrschten Sprache auf eine neue, oder bei der Verwendung von für die Bildverarbeitung vortrainierten Netzen auf die Schlüsselworterkennung.
Das zum Training benötigte Datenmaterial ist bei der Sprachverarbeitung in Einsatzszenarien jedoch nach wie vor eine der größten Herausforderungen. Hier hilft die gesteigerte Leistungsfähigkeit der KI-Methoden nicht unmittelbar, da bei diesen Methoden die Anforderungen an den Umfang benötigter Daten eher noch gestiegen sind. Es gibt aber auch an dieser Stelle bereits Ansätze, bei denen der Umfang des vorhandenen Trainingsmaterials automatisiert vergrößert werden kann, etwa durch verschiedenste Modifikationen vorhandenen Trainingsmaterials. Trotz dieser Herausforderungen hat der Einsatz von KI-Methoden im Bereich der Sprachsignalverarbeitung in den letzten Jahren für signifikante Leistungssteigerungen gesorgt. Erste umfangreichere am Fraunhofer FKIE durchgeführte Versuche im Bereich der Sprecherklassifikation belegen klar, dass KI-Methoden auch weitere Bereiche der signalerfassenden Aufklärung vorantreiben können.

Die Zukunft taktischer Gefechtsfeld-Kommunikation: in Realzeit und in Bewegung

Hintergrund

In den letzten Jahren ging es insbesondere darum, das erforderliche Leistungsvermögen taktischer Kommunikationssysteme zu ermitteln – insbesondere bei Funklösungen – um die Erfordernisse auf dem Gefechtsfeld der Zukunft optimal zu erfüllen. Im Mittelpunkt der Diskussion stand dabei ganz einfach das Ziel, mehr Daten pro Zeiteinheit zwischen den Funkteilnehmern austauschen zu können. Also standen Themen wie größerer Netzwerkdurchsatz und Applikationen wie Full Motion Video im Mittelpunkt des Interesses.

Zeitkritisch: Die neue Normalität

Klar ist, dass zum Übertragen großer Informationsmengen ein hoher Datendurchsatz erforderlich ist, doch es ist auch wichtig herauszustellen, dass die Kommunikation auf den Gefechtsfeldern der Zukunft viel mehr als das ermöglichen muss, und Hochgeschwindigkeit ist nur ein Teil. Tatsächlich wird es wahrscheinlich die Geschwindigkeit sein, mit der Informationen erfasst, kommuniziert, analysiert und in Handlungen überführt werden können, welche die Ergebnisse zukünftiger Gefechte entscheidet.
Zum Beispiel kann die Geschwindigkeit, in der eine Nachricht (d. h. ein „packet“) gefechtsfeldübergreifend von der Quelle zum Ziel überbracht werden kann, über Tod und Leben entscheiden. In der Vergangenheit war die Übermittlung von Informationen über das Gefechtsfeld hinweg begrenzt auf Sprachverbindungen und solche Datenanwendungen für Landkarten, Bilder und Zeichnungen, die nicht als besonders zeitkritisch erachtet wurden, weil es keine wirklichem taktischen Konsequenzen hatte, wenn die Inhalte die kämpfende Truppe innerhalb von Minuten erreichten statt in Sekunden. Das Gefechtsfeld der Zukunft wird aber zu einem taktischen Internet der Dinge (TIoT – Tactical Internet of Things) werden, mit immer mehr zeitkritischen Anwendungen, die bei der Informationsverteilung keine Verzögerungen dulden. Auf Basis neuer und spannender Technologien, die das Gesicht des modernen Gefechtsfeldes verändern werden, wird der Erfolg von Operationen davon abhängig sein, dass Verzögerungen auf ein Minimum reduziert werden. Ein Beispiel dafür ist die Nachfolgegeneration von Systemen zum Schließen von Sensor-zu-Effektor-Zyklen. Ein solches System beinhaltet mehrere Sensoren, die an verschiedenen geographischen Standorten operieren und Informationen über mehrere sich bewegende Ziele erfassen und diese dann an viele sich bewegende „Shooters“ an unterschiedlichen Orten weitergeben, die dann diese Informationen nutzen, um Bedrohungen zu eliminieren – und das alles innerhalb von Sekunden.

Konnektivität für die Mobilität von Einheiten sicherstellen

Auch Geschwindigkeit und Sicherheit des Verbindungsaufbaus werden beträchtliche Folgen für das Gefechtsfeld der Zukunft haben. Die Natur des Kampfgeschehens bringt es mit sich, dass Soldaten, Einheiten und Waffen – mit ihren Funkgeräten – in ein bestimmtes Gebiet kommen, sich dort bewegen oder bewegt werden und es wieder verlassen. Diese willkürlichen Bewegungsmuster der Netzknoten bewirken schnelle Veränderungen bei der Netzwerk-Struktur, die in feindlicher Umgebung ohne Infrastruktur auf raffinierte Weise angepasst werden muss. Manchmal können Einheiten so abgesetzt positioniert sein, dass über lange Zeiträume Kommunikationsversuche erfolglos bleiben. In anderen Fällen dringen Soldaten möglicherweise tief in städtische Gebiete ein und „verschwinden“ dabei aus

Die taktische Funkkommunikation mit BNET ermöglicht den Kämpfern, sich frei zu bewegen und dabei in Verbindung zu bleiben

Foto: Rafael

dem Funknetz, nur um irgendwann später irgendwo plötzlich „wieder aufzutauchen“, aber ohne die Möglichkeit zu haben, schnell genug zu kommunizieren und Eigenbeschuss-Situationen zu verhindern. Damit unter den rasch sich ändernden Bedingungen moderner Gefechtsfelder das Funknetz hinreichend funktioniert, muss es in der Lage sein, in Realzeit auf Veränderungen der Topologie zu reagieren. Anders ausgedrückt, das Netz muss innerhalb von Sekunden „sich bilden und heilen“, nicht in Minuten.

Radio MANET Technologie: Eine Teillösung

Diese dringenden Erfordernisse haben die Branche gezwungen zu reagieren, und das Ergebnis der letzten Jahre ist die Einführung der Radio MANET Technologie. Radio MANET (MANET – Mobile Ad-hoc Networks) basiert auf Software-basierten Funkgeräten (SDRs – Software Defined Radio Units). Diese bilden zusammen infrastrukurlose, vollständig verteilte, sich selbst bildende und heilende mobile Funknetze. In MANET-Netzen werden Informationen zwischen Benutzern über andere Funkgeräte geroutet, die somit Meshed Networks (vermaschte Netze), bilden. Der militärische Einsatz von MANET ist am anspruchsvollsten in Szenarien mit hoher Mobilität, leistungsschwachen Funksendern, einer infrastrukturlosen Umgebung und ungleichmäßigen Ausbreitungsbedingungen z. B. auf Grund des Geländes.

Die Mängel bei MANET-Netzen

Unter bestimmten Bedingungen sind diese Möglichkeiten ausreichend. In vielen Kampfsituationen von heute können die Bedingungen aber zunehmend schwieriger werden, ja sogar zu schwierig, um von den meisten konventionellen handelsüblichen MANET-Netzen bewältigt zu werden.
Der Grund, warum handelsübliche MANET-Einheiten durch die Bedingungen auf modernen Gefechtsfeldern überfordert werden, ist einfach: Konventionelle MANET-Netze arbeiten mit 1-Kanal-Empfangsgeräten. Das bedeutet, dass Funkgeräte, die auf den vom MANET-Netz benutzen Frequenzkanal abgestimmt sind, nur dann die Signale anderer Funkgeräte empfangen können, wenn diese auf demselben Frequenzkanal senden. Diese Abhängigkeit vom 1-Kanal-Empfang bringt viele kritische Einschränkungen mit sich, die verheerende Folgen für den jeweiligen Auftrag und die militärischen Kräfte haben können.
Einer der Mängel bei einem konventionellen MANET-Netz besteht in der Netzzuteilung, bei dem „ein Frequenzkanal einem Sub-Netz entspricht“. Dadurch sind Funkgeräte nicht in der Lage, als Relaisstationen für in der Nähe befindliche Funkgeräte zu fungieren, wenn diese auf einem anderen Frequenzkanal senden. Dadurch entsteht die Notwendigkeit, dass das Netz zahlreiche „Gateways“ mit mehreren Sende-/Empfangseinheiten haben muss. Diese Begrenzung schafft eine Skalierbarkeitsobergrenze, denn jedes Sub-Netz ist typischerweise begrenzt auf wenige Dutzend Benutzer (höchstens ±40-50). Das wiederum macht es zunehmend schwierig, große, wachsende

BNET garantiert höchste QoS bei anspruchsvollen Anwendungen wie Video und BMS *Foto: Rafael*

Netze zu unterstützen, ohne bei Durchsatz und QoS (Quality of Service) Kompromisse machen zu müssen. Neben diesen Engpässen und Einbußen bei der Datenübertragungsrate müssen bei konventionellen MANET-Netzen die Frequenzkanäle gegebenenfalls manuell verwaltet werden, etwa wenn während einer Mission Frequenzkanäle geändert werden müssen, um hinreichend Bandbreite zu gewährleisten – ein Alptraum für jeden Fernmeldeoffizier an der Front, eine beträchtliche Quelle für menschliches Versagen und Grund für ineffiziente Nutzung des verfügbaren Frequenzbandes.
Ein weiterer Nachteil konventioneller MANET-Netze ist ihre Bremswirkung in Bezug auf Datendurchsatz, die vom Netzsteuerungs-Overhead und ausgedehnten Verzögerungen herrührt.
Und schließlich sind konventionelle MANET-Netze beim Zusammenführen und Heilen von Netzen gefährlich langsam. Bei einem konventionellen MANET-Netz ist es nicht ungewöhnlich, dass es dazu mehrerer Minuten bedarf, was unter bestimmten Bedingungen tödlich sein kann (z. B. durch das Entstehen von „Eigenbeschuss“-Situationen).
Im Großen und Ganzen sind die erwähnten Nachteile der heutigen handelsüblichen konventionellen MANET-Netze bedingt durch ihre Unfähigkeit, zu einem gegebenen Zeitpunkt mehr als nur einen einzigen Frequenzkanal empfangen zu können – ein Beschränkung, welche die Ergebnisse selbst bester Netzwerk-Dynamik und Auto-Routing-Algorithmen schmälern oder unwirksam machen.

Rafaels Antwort: BNET SDR als taktische Kommunikationslösung

Im Wissen um diese Defizite und auf Basis jahrzehntelanger Expertise in der Entwicklung von C4I-Lösungen hat Rafael die BNET-Familie entwickelt – eine in unterschiedlichsten Einsätzen erprobte erweiterte Breitband IP MANET SDR (Software Defined Radio) Lösung für taktische Einsätze, erweitert durch Mehrkanalempfang (MCR – Multi-Channel Reception). BNET liefert Hochgeschwindigkeits-Breitbandkommunikation von Daten, Sprache und Video für mobile Einheiten.
Aufgrund seiner MCR-Funktionen kann der BNET-Empfänger Informationen, die über zahlreiche Frequenzkanäle übertragen werden, unter Nutzung einer einzigen Sende-/Empfangseinheit

gleichzeitig empfangen. Das schafft die Möglichkeit, ein „flat“ Netzwerk zu bilden, das auf Größen von bis zu Hunderten von Benutzern skaliert werden kann. Tatsächlich ist ein BNET skalierbar auf über 400 Benutzer in einem einzigen Netzwerk. Bei BNET gibt es keine Engpässe, da das System eine einzige vereinheitlichte logische Gruppe bildet, ohne dass dazu Gateways erforderlich sind. Zu den zusätzlichen Vorteilen zählen automatische und dynamische Frequenzzuweisung, was bedeutet, dass der Fernmeldeoffizier des Bataillons nicht manuell eingreifen muss und dass die verfügbaren Frequenzen (die immer eine Begrenzung darstellen) in höchstem Maß ausgenutzt werden.

Der erweiterte Datendurchsatz von BNET unterstützt zeitkritische und anspruchsvolle Anwendungen, einschließlich solcher mit vielen verschiedenen Video- und Sensorsignalen – und das gleichzeitig. Das ist wichtig für die Digitalisierung von Landoperationen und ist eines der größten Herausforderungen, wenn es um Fähigkeiten geht, Sensor-zu-Effektor-Zyklen zum richtigen Zeitpunkt aufzubauen. Rafael ist in dieser Hinsicht einmalig positioniert: Das Unternehmen verfügt über das weltweit ausgereifteste System zum Schließen von Sensor-zu-Effektor-Zyklen.

Durch die ulta-schnellen BNET-Funktionen zum Zusammenführen und Heilen von Netzen bleiben alle Einheiten ständig in Kommunikation Foto: Rafael

Außerdem verfügt das BNET über ultra-schnelle Funktionen zum Zusammenführen und Heilen von Netzen (in Sekunden reagierend statt in Minuten), was die Risiken durch Totalausfall der Kommunikation weitgehend ausschließt (z. B. das Risiko unter „Eigenbeschuss“ zu geraten).

Schlussfolgerung

Zusammenfassend ist festzustellen, dass es auf den Gefechtsfeldern von heute weit reichende Veränderungen gibt, welche die Herausforderungen betreffen, denen sich Land-, Luft- und Seestreitkräfte bei ihren Operationen gegenüber sehen. Lösungen müssen sowohl den Anforderungen kleiner Truppenverbände entsprechen, die in dicht bebauten, oft von Zivilbevölkerung bewohnten Stadtvierteln kämpfen, und auch genauso den Bedarf von Kämpfern erfüllen, die im offenen Gefechtsfeld einer massiven Streitmacht frontal gegenüber stehen. Die Zeiten sind vorüber, als es genug war, neben Sprachverbindungen statische Dateien und Bilder zu haben, die Minuten brauchten, um über das Gefechtsfeld hinweg übertragen zu werden. Heutzutage ist ein neues taktisches Internet der Dinge für das Gefechtsfeld im Kommen (Battlefield TIoT – Tactical Internet of Things), das auf in Realzeit arbeitenden Anwendungen basiert, z. B. Systeme zum Schließen von Sensor-zu-Effektor-Zyklen. Kommunikationssysteme sind essentielle Wegbereiter, sie müssen in jeder Hinsicht beweglicher werden, um rasch eingesetzt werden zu können, um skalierbar zu sein und um im Chaos eines Gefechts robust und stabil zu funktionieren.

Erfahren Sie mehr darüber, wie die neue MCR-Technologie bei BNET-Systemen die taktische Funkkommunikation revolutioniert. Sehen Sie die ausgereifteste verfügbare Technologie zum Schließen von Sensor-zu-Effektor-Zyklen. Besuchen Sie uns bei der AFCEA 2018 in Bonn, Saal MARITIM, M28.

RAFAEL
SMART AND TO THE POINT

rola.
SECURITY SOLUTIONS

AFCEA Fachausstellung 2018
Stand B11

Zusammenarbeit stärken, Sicherheit schaffen.

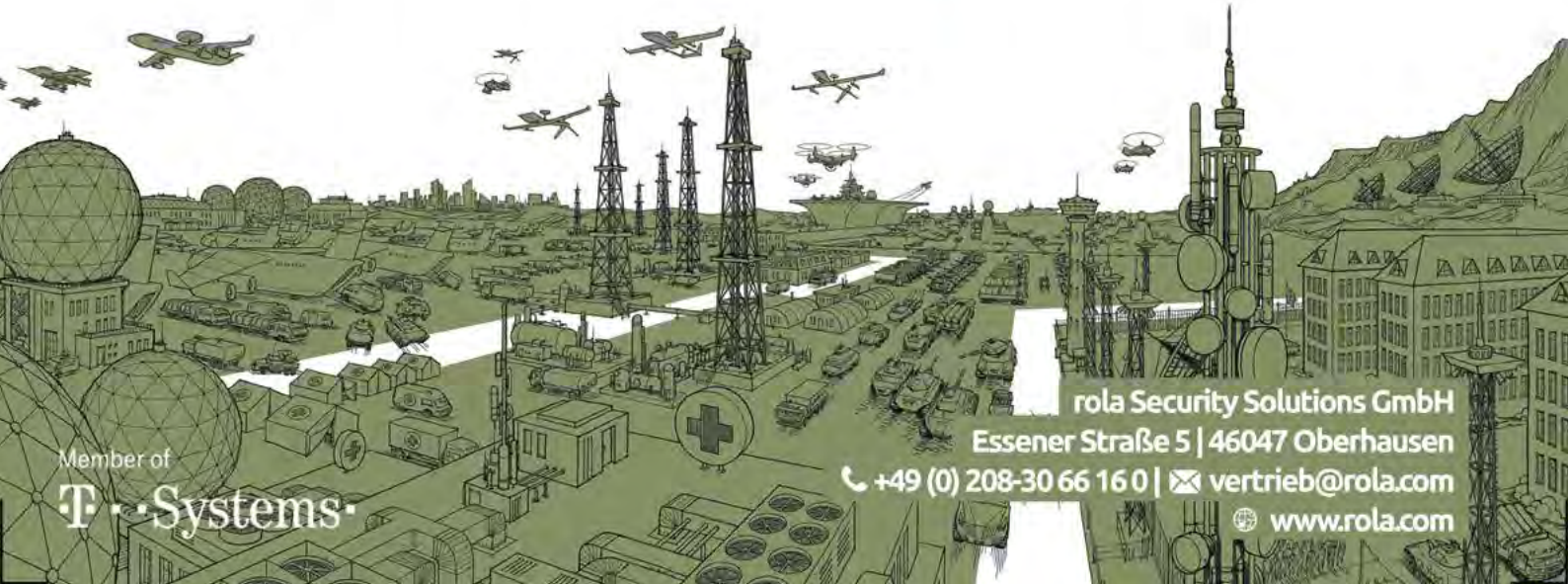
Jederzeit von jedem Ort auf die relevanten Informationen zugreifen zu können: Was vor wenigen Jahren noch als Wunschtraum in der Kriminalitätsbekämpfung galt, wird durch rola Securtiy Solutions zur Realität.

Im Rahmen komplexer Ermittlungen, Gefährdungsanalysen oder der Auswertung von Angriffen, kommt es darauf an, relevante Informationen zeitnah zu erkennen, zusammenzuführen und zu analysieren. Ohne diese Möglichkeiten trägt die reine Information im Zeitalter des Datenüberflusses kaum noch zur Problemlösung bei.

rola entwickelt, vertreibt und integriert seit 1983 IT-Verbundlösungen für die Innere und Äußere Sicherheit. Nationale und internationale Sicherheits- und Ermittlungsbehörden vertrauen unserer Kompetenz. Wir versorgen unsere Kunden mit intelligenten IT-Systemen, die auf den einzelnen Anwender zugeschnitten sind.

- Militärische Lagebilderstellung
- Analyse von Massendaten
- Auswertung Sozialer Medien
- Cyber Threat Intelligence

rsIntCent®
rsExTract®
rsNetMAn®
rsCyInt®



Member of
T · · Systems ·

rola Security Solutions GmbH
Essener Straße 5 | 46047 Oberhausen
+49 (0) 208-30 66 16 0 | vertrieb@rola.com
www.rola.com

Künstliche Intelligenz im wehrtechnischen Umfeld – eine kritische Reflexion

Dr. Felix Govaers, Stv. Abteilungsleiter „Sensordaten- und Informationsfusion“, Fraunhofer FKIE

Dr. Felix Govaers

Foto: Fraunhofer FKIE

Unüberhörbar machte im Jahr 2017 das Kommando Heer mit zwei Thesenpapieren zur Digitalisierung der Streitkräfte [1, 2] auf sich aufmerksam, die aufzeigen, wo aus Sicht der Autoren Schwerpunkte bei der Planung von Ressourcen liegen sollten. Die Hinweise auf die Notwendigkeit eines durchgreifenden digitalen Wandels in den Streitkräften dürfen als wichtiger Beitrag zur Diskussion über die zukünftige Ausrichtung der Bundeswehr aufgefasst werden. „Digitalisierung“ ist eine Aufgabe, die nicht neu ist, sich aber heute besonders drängend stellt. Es kann nicht mehr allein darum gehen, die computergestützte Datenverarbeitung in die deutschen Kasernen zu bringen. Vielmehr geht es darum, modernste Technologien der Kommunikation, der Informationsverarbeitung und -darstellung für „combat centric“, sprich auf den Kampfeinsatz fokussierte, Anwendungen zu erschließen. Diese Forderung ist jedoch weniger im Sinne eines „nice to have“ sondern mehr als ein „must have“ zu verstehen, da zunehmend offensichtlich wird, wie die Streitkräfte der Bundeswehr technologisch von den außereuropäischen Großmächten abgehängt werden. Während Russland seine traditionell starke wehrtechnische Entwicklung unter der aktuellen Regierung im Kreml weiter aufwertet, führen die USA und China im Wettkampf um die besten und neuesten Methoden von Künstlicher Intelligenz (KI).

Das Schlagwort KI wird oftmals synonym für Künstliche Neuronale Netze (KNN) verwendet, was nicht zuletzt daher rührt, dass letztere an die Funktionsweise der menschlichen Gehirnzellen angelegt sind. Doch sollte zunächst klargestellt werden, dass KI als Überbegriff für komplexe Informationsverarbeitung weit mehr abdeckt: So gehören neben KNN auch Methoden wie Entscheidungsbäume, Support Vector Machines, Bayes Netze, Bayes’sche Schätzer und Algorithmen der Sensordatenfusion dazu. Weiterhin sind erfolgreiche Systeme oftmals Hybride, also ein heterogener Mix, in Hinblick auf ihre grundlegende Methode, was dann in publizistischen oder populärwissenschaftlichen Darstellungen gerne auf KNN vereinfacht und reduziert wird. Im Folgenden soll ein Überblick gegeben werden, welche Strömungen sich in den unterschiedlichen Forschungs-Communities herauskristallisieren und welche Potenziale sich daraus erschließen lassen.

KI ist in bestimmten Aufgaben der Kognition (wie in der Bild- und Spracherkennung), der Strategie (wie im Schach und im Go) und der Interpretation (z. B. automatisierte Diagnosen des Zustands komplexer Systeme) dem Menschen überlegen. Doch die öffentlich wahrnehmbare Freude über diese technischen Errungenschaften ist nicht ungetrübt. So warnten beispielsweise im Jahr 2015 prominente Experten in einem „Digitalen Manifest“ vor den Folgen der zunehmenden Integration von KI in den Alltag. Elon Musk hat die Debatte 2017 erneut durch einen Tweet befeuert, indem er den Wettkampf um die beste KI als Ursache eines Dritten Weltkrieges vorhersagt. Auch der prominente Physiker Stephen Hawking macht regelmäßig mit apokalyptischen Warnungen vor der Entwicklung und dem Einsatz von KI auf sich aufmerksam. Insbesondere der Einsatz von KI für wehrtechnische Anwendungen schürt Kontroll- und Existenzängste, was die Bewegung „Ban Lethal Autonomous Weapons“ [3] verdeutlicht, an deren stetig wachsende Anhängerschaft in sozialen Medien makabre Dystopien verbreitet werden. Die Diskussion wurde auch durch die Medien weitläufig aufgenommen, wobei die kritische Seite sichtlich dominierte – viele Kommentatoren fragen sich: „Geht das nicht zu weit?“

Die Abteilung „Sensordaten- und Informationsfusion“ des Fraunhofer FKIE ist der Meinung, dass es wichtig ist, die kritischen Aspekte von KI im Detail zu beleuchten, gerade weil sie dem Ansatz grundsätzlich positiv gegenüber steht. Nur so können Entwickler und Anwender sich der damit einhergehenden Risiken bewusst werden und zu einem verantwortungsvollen Umgang kommen. Umso wichtiger ist es, auf Spekulationen, was KI in Zukunft alles machen wird, zu verzichten, und auf die Möglichkeiten existierender Algorithmen und Anwendungen zu beschränken.

Entscheidend für die Bundeswehr ist, dass die Friktion, sprich die Behinderung im operativen Aufgabenbereich, bei taktischen Szenarien trotz hohem Technologiegrad enorm hoch ist, was schwere Implikationen nicht nur für eigene und verbündete Soldaten nach sich zieht. Daher muss auch der Einsatz moderner Methoden wie KI für wehrtechnische Systeme systematisch untersucht werden. Insbesondere vor dem Hintergrund, dass das Zeitalter von „Machine Learning“ (ML) bzw. „Deep Learning“ gerade erst angefangen hat und die Potenziale sich nur schwer ausloten lassen. Ein verantwortlicher Umgang mit der sich entfaltenden Technologie setzt dabei zwingend eine Auseinandersetzung mit den Schwächen und Risiken voraus, die zwar durchaus vorhanden, jedoch nicht unkontrollierbar sind.

Die Leistungsfähigkeit im Sinne der Präzision und der Generalisierung von ML hängt maßgeblich von zwei Faktoren ab: dem Trainingsdatensatz und der Architektur. Während es für relativ einfach strukturierte Probleme einen großen Fundus an verfügbaren Daten gibt, gilt dies für komplexe Entscheidungsprozesse

in einer militärischen Lage kaum. Zudem ist nicht allein die Quantität entscheidend, sondern auch die Qualität. Werden die ML-Algorithmen mit ungeeigneten Daten gespeist, so werden sie in der Anwendung entsprechend auf die Realität reagieren. Weiter können KNN den Menschen durch datenbasierte Entscheidungen unterstützen, der Weg der Entscheidungsfindung bleibt im Nachhinein jedoch selbst den Spezialisten verborgen. Während dies bei trivialen Problemstellungen noch verschmerzbar ist, wird die Erklärbarkeit für die Verarbeitung von Daten im öffentlichen Bereich zunehmend gesetzlich vorgeschrieben. So tritt am 25. Mai 2018 die „General Data Protection Regulation“ (GDPR) [4] der Europäischen Union in Kraft, die zur Prävention von Vorurteilen basierend auf Rasse, politischer Orientierung oder Gesundheitsparameter das „Tell-me-why“ der getroffenen Entscheidung uneingeschränkt fordert und deren Auswirkungen noch schwer abzuschätzen sind. Insbesondere im militärischen Kontext spielt die Nachvollziehbarkeit von Situationsbewertungen eine maßgebliche Rolle für die Kontrolle von KI-Systemen durch den Menschen.

In der Konsequenz werden vermutlich auch zukünftig modellbasierte sowie selbstlernende Methoden für Systeme der Entscheidungsunterstützung im militärischen Kontext eingesetzt und weiterentwickelt werden, die immer neue und zunehmend komplexere Aufgaben lösen können. Jedoch ist abzusehen, dass bei höherem Abstraktionsgrad der Problemstellung selbstlernende Methoden stets nur untergeordnete Funktionen übernehmen können und „Intelligenz“ modell- und regelbasiert gesteuert werden muss. Die stetig wachsende Mächtigkeit von KNN ist trotz alledem ein Umbruch in großen Bereichen der Forschungslandschaft, der nicht missachtet werden darf. Dabei profitieren die Methoden nicht zuletzt von der Verfügbarkeit riesiger Rechenzentren beispielsweise von Google oder Amazon. Ersterer hat inzwischen beispielsweise seinen eigens konzipierten Chip, die „Tensor Processing Unit“ (TPU) [5], eingeführt, der durch die Zusammenfassung von über 100.000 Operationen in einem einzigen Zyklus die Berechnungsgeschwindigkeit und Effizienz von GPUs noch übertrumpfen soll. Dieses Potenzial der sich abzeichnenden Hardwareentwicklung muss auch für wehrtechnische Probleme nutzbar gemacht werden. Bei Fraunhofer FKIE wird bereits an Hybridlösungen geforscht, die die Stärken der KNN mit den hochentwickelten Modellen der stochastischen Zielverfolgung aus der Theorie des Target Tracking vereinen und dabei die Vorteile von moderner Hardware ausnutzen. Ein weiterer Hinweis, wie vielfältig und komplex die neueste Generation von Algorithmen in der Informationsverarbeitung sein wird.

[1] Autorenteam Kommando Heer II 1, „Thesenpapier – wie kämpfen Landstreitkräfte künftig?“ 2017.
[2] Autorenteam Kommando Heer II 1, „Digitalisierung von Landoperationen“, 2017.
[3] http://autonomousweapons.org, 30.11.17.
[4] https://www.eugdpr.org, 30.11.17.
[5] https://cloud.google.com/blog/big-data/2017/05/an-in-depth-look-at-googles-first-tensor-processing-unit-tpu, 30.11.17

Kognitive Modelle für die Gestaltung und Entwicklung von Benutzungsschnittstellen

Dr. Carsten Winkelholz, Forschungsgruppenleiter „Informationsvisualisierung und Interaktion“, Abteilung „Mensch-Maschine-Systeme“, Fraunhofer FKIE

Dr. Carsten Winkelholz

Foto: Fraunhofer FKIE

Kognitive Modelle versuchen die kognitiven Vorgänge auf wissenschaftliche Weise zu beschreiben und berücksichtigen die für einen Menschen gegebenen Restriktionen, wie bspw. Gedächtniskapazität oder die Fähigkeit, verschiedene Informationen gleichzeitig zu verarbeiten. Das Ziel kognitiver Modelle ist, das Verhalten und die Leistung von Menschen in bestimmten Situationen vorauszusagen oder zu simulieren.

Damit unterscheidet sich der Fokus der Forschung von dem vieler aktuell aus dem Bereich der Künstlichen Intelligenz diskutierter Anwendungen. In dem Forschungsfeld der Künstlichen Intelligenz liegt der Fokus in der Entwicklung von Algorithmen, die intelligentes Verhalten zeigen und in der Lage sind, Prozesse zu automatisieren oder zu teilautomatisieren, in denen bislang das Mitwirken eines Menschen notwendig ist, um diesen zu ersetzen oder zumindest in seinen Aufgaben zu entlasten. Hier hat man in der Regel konkrete Aufgaben im Auge, die man mit intelligentem Verhalten lösen/bearbeiten will und möchte Schwächen der menschlichen Intelligenz vermeiden, wie die eingangs Erwähnten oder auch irrationales Handeln. Das Ziel kognitiver Modelle dagegen ist, das Verhalten von intelligenten Systemen, insbesondere die Kognition des Menschen, zu verstehen. Dieses Wissen kann in den Entwicklungsprozess von Systemen, in denen Mensch und Computer zusammenarbeiten, eingebracht werden. Die Restriktionen und Randbedingungen, denen die informationsverarbeitenden Prozesse des kognitiven Systems unterworfen sind, werden in einer kognitiven Architektur definiert, in der dann ein kognitives Modell für eine bestimmte Aufgabe formuliert werden kann.

Kognitive Architekturen entstammen der Kognitionswissenschaft und haben das Ziel, die Ergebnisse verschiedener psychologischer Untersuchungen in eine Art Theorie zu beschreiben. Es gibt hier verschiedene konkurrierende Architekturen, mit denen die kognitiven Prozesse von Menschen beschrieben werden. Das Konzept der kognitiven Architekturen kann allgemein auf kognitive Systeme angewendet werden, auch auf Systeme Künstlicher Intelligenz. Hier stellt sich die Frage, ob eine perfekte kognitive Architektur existiert oder ob man – wie bei jedem komplexen System – mit Kompromissen leben muss. So ist häufig das Vergessen von unwichtigen Dingen auch Teil der Intelligenz.

Kognitive Architekturen werden häufig in Form einer Programmiersprache formuliert, die es entsprechend eines Computerprogramms erlauben, bestimmte kognitive Abläufe zu beschreiben. Anders als bei generellen Programmiersprachen soll aber nicht eine möglichst große Vielfalt von Verhalten gewährleistet werden, sondern nur ein in Bezug auf das betrachtete kognitive System valides, das heißt beobachtbares Verhalten. Zwei populäre kognitive Architekturen sind ACT-R (Adaptive Control of Thoughts – Rational) und SOAR (State, Operator, Apply, Result). Beide basieren auf Erzeugungssystemen, die Wissen in Form von Objekten für Fakten und Produktionsregeln für Handlungsabläufe darstellen. Produktionsregeln sind lose Regeln, aus denen das kognitive System eine passende basierend auf seinem Zustand oder externen Einflüssen auswählt und seine mit ihr definierten Aktionen ausführt, was das Erzeugen neuer Objekte intern oder auch Aktionen nach außen bedeuten kann. Durch die unabhängigen Regeln kann sich das System verschiedenen Situationen flexibel anpassen und auch dadurch lernen, dass der Erfolg der Anwendung einer Regel für das Erreichen eines Ziels nach der Methode des „Reinforcement Learning“ bewertet wird. SOAR ist spezialisiert für die Modellierung des Verhaltens von Menschen beim Problemlösen. ACT-R simuliert auch, wie erfolgreich sich an eine Gedächtniseinheit erinnert werden kann, und berücksichtigt dafür zeitliche Aspekte und Assoziationen zu aktuellen Zielen und anderen Gedächtniseinheiten.

ACT-R wurde Ende der 90er und Anfang 2000 in vielen Arbeiten für die Simulation von Operateuren im Zusammenhang mit Benutzungsschnittstellen eingesetzt. Die Arbeiten wurden stark von der DARPA gefördert und hatten entsprechend auch meistens einen militärischen Kontext. Für die Bewertung von Benutzungsschnittstellen wird auch häufig GOMS (Goals, Operators, Methods and Selection rules) verwendet. GOMS ist ein einfacheres Erzeugungssystem, das darauf spezialisiert ist, Zeiten von Bearbeitungsvorgängen über seine verschiedenen möglichen Variationen abzuschätzen. In KLM-GOMS (Key-Stroke Level) sind entsprechende empirische Zeiten für fundamentale Bearbeitungsschritte wie das Bewegen einer Maus zu einem Ziel oder das Betätigen eines Tasters hinterlegt. ACT-R/PM enthält auch entsprechende Module und kann daher ebenso verwendet werden, wobei dann auch kognitive Aspekte wie Lernen, Gedächtnis und mögliche Fehler durch den Nutzer berücksichtigt werden können.

Das Ziel von ACT-R war stets die Formulierung allgemein gültiger Modelle, die sich für verschiedene Aufgaben generalisieren lassen. In den meisten Fällen wurden aber Modelle den Beobachtungen angepasst und nur selten wurde der Nach-

weis erbracht, dass sich ein an einer Aufgabe parametrisiertes Modell ohne weiteres auf andere Aufgaben übertragen lässt. Dennoch erfordert der Versuch der Modellierung einer Aufgabe eines Operateurs in einer kognitiven Architektur eine detaillierte Auseinandersetzung mit möglichen kognitiven Aspekten und es können so wertvolle qualitative Hinweise für die adäquate Gestaltung einer Benutzungsschnittstelle gewonnen werden, die mögliche Engpässe in der Informationsverarbeitung beim Operateur betreffen.

Das Fraunhofer FKIE hat in seinen Forschungsarbeiten zur Mensch-Computer-Interaktion diese Modelle immer wieder berücksichtigt und eigene Methoden zur modellgestützten Bewertung von Benutzungsschnittstellen entwickelt, unter anderem eine Erweiterung von ACT-R für die Verarbeitung von visuell räumlichen Informationen, die bei der Bewertung von Layouts wichtig sind. Zudem wurden Werkzeuge entwickelt, mit denen die Interaktion von Nutzern mit grafischen Benutzungsoberflächen modellbasiert analysiert werden können. Hierzu werden die beobachteten Benutzerinteraktionen und auch Blickbewegungen durch Algorithmen in einen stochastischen Zustandsautomaten überführt, dessen Zustände auf einzelne Zeitabschnitte abgebildet werden können und dem Analysten so helfen, Muster im Nutzerverhalten zu erkennen oder auch mit kognitiven Modellen abzugleichen.

Künstliche Intelligenz und der Faktor Mensch

Dr. Thomas Alexander, Abteilungsleiter „Human Factors“, Fraunhofer FKIE

Dr. Thomas Alexander

Foto: Fraunhofer FKIE

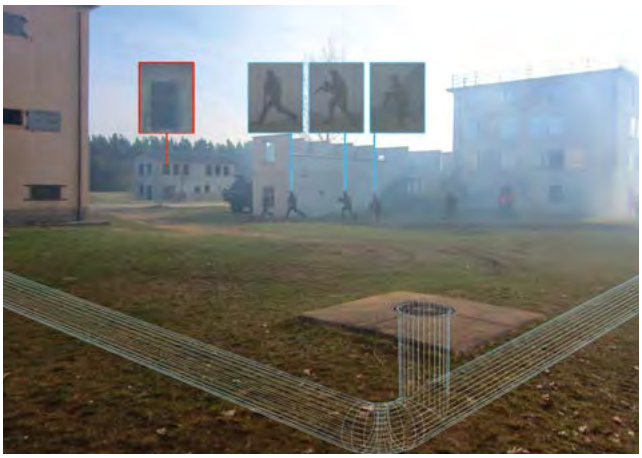
Der Begriff der Intelligenz war und ist eng mit dem Menschen als vernunftbegabtem Wesen verbunden. So wird unter „Intelligenz“ die Fähigkeit des Menschen verstanden, „abstrakt und vernünftig zu denken und daraus zweckvolles Handeln abzuleiten“ (Duden, 2017). Waren Aktivitäten zur Intelligenz ursprünglich in den Geisteswissenschaften beheimatet, so beschäftigen sich heute zunehmend die Naturwissenschaften unter dem Begriff der Künstlichen Intelligenz (KI) mit der Nachbildung (und Automatisierung) intelligenten Verhaltens. Durch die Vernetzung mit intelligenten Systemen wird angestrebt, den Menschen auf unterschiedlichen Ebenen bei seinen Aufgaben zu unterstützen und die Leistungsfähigkeit zu steigern. Dies gilt für den Industriearbeiter in der zukünftigen „Industrie 4.0“ ebenso wie für den Soldaten bei seinen zukünftigen, diversitären Einsätzen und Missionen. Hier ist eine intelligente Unterstützung besonders wichtig, denn diese Einsätze werden durch eine zunehmende Komplexität, Dynamik und Geschwindigkeit des Geschehens charakterisiert. Neue Aufklärungstechnologien und eine komplexe Ausrüstung des Soldaten werden die Informationsflut und Informationsbelastung weiter steigern.

Umso wichtiger ist es, den Soldaten situations- und einsatzbezogen durch intelligente Systeme zu unterstützen. Verfahren der KI bieten hierzu Potenzial. Allerding darf sich dabei nicht ausschließlich auf technologische Verfahren und Möglichkeiten beschränkt werden, sondern vielmehr ist stets das Gesamtsystem aus Soldat, unterstützender Technik und militärischem Auftrag zu berücksichtigen. Dies erfordert die Einbeziehung des Soldaten, insbesondere seiner perzeptiven, kognitiven und motorischen Eigenschaften und Fähigkeiten. Die Interaktion mit dem komplexen System ist aus ergonomischer Sicht einfach und verständlich zu gestalten, um den Soldaten zu unterstützen und nicht noch stärker zu belasten.

Verfahren der KI sind daher nicht isoliert, sondern als Element des oben geschilderten Gesamtsystems zu betrachten. Vor Festlegung eines möglichen Einsatzbereiches sind deshalb die Charakteristiken des militärischen Einsatzes sowie der Bedarf an Assistenz zu ermitteln. Hierzu werden Prozesse bei typischen militärischen Einsätzen erfasst und analysiert. In der Folge können Ressourcenengpässe identifiziert werden. Erst dann kann eine Unterstützung durch passende KI-Verfahren ausgewählt werden. So werden beispielsweise Orts- und Häuserkampf durch eine sehr hohe Dynamik und ein hohes Belastungsniveau der Soldaten geprägt. Eine Unterstützung während des ablaufenden Einsatzes ist hier, wenn überhaupt, nur sehr eingeschränkt sinnvoll. Dagegen besteht bei der Einsatzplanung und vorbereitung vielfältiger Bedarf an Assistenz und Unterstützung. Sie wird im Bereich des Operations Research (OR) sowohl bei der Situationseinschätzung als auch bei der Planung und Optimierung des Einsatzes eingesetzt. Hierunter fallen auch kognitive Verhaltensmodelle des Menschen, die landläufig ebenfalls als KI bezeichnet werden. Allerdings handelt es sich bei genauerer Betrachtung eher um einfache, regelbasierte Systeme, welche menschliche Eigenschaften und Fähigkeiten rudimentär modellieren.

In zeitunkritischen Phasen während eines Einsatzes können KI-Verfahren beispielsweise die Aufmerksamkeit des Soldaten lenken, ohne zu stören. Jedoch ist die menschliche Fähigkeit zur Informationsaufnahme bereits in alltäglichen Situationen eingeschränkt. Umso wichtiger ist es, in kritischen Situationen die richtigen Informationen wahrzunehmen und die Aufmerksamkeit nicht abzulenken. KI-Verfahren der Bildanalyse und der Informationsvorverarbeitung besitzen ein hohes Potenzial, eine Auswahl der situationsspezifisch relevanten Informationen zu treffen, die dann dem Soldaten zur Verfügung gestellt werden. Aus ergonomischer Sicht erfolgt dadurch eine Verschiebung von kognitiven Aufgaben zu perzeptiven Aufgaben. Der Soldat wird also kognitiv entlastet und kann die freiwerdenden Ressourcen anderweitig einsetzen.

Dabei darf der Soldat durch die KI nicht von der Hauptaufgabe abgelenkt werden. Deshalb erfolgt eine konsistente Integration der Information in die reale Umgebungswahrnehmung. Zur Darstellung räumlich bezogener Lösungen bieten sich heute beispielsweise Verfahren der Augmented Reality (AR) an. Dabei werden diese Informationen räumlich und perspektivisch in die Realsicht eingefügt. Damit wird der Soldat nicht abgelenkt. Gleiches gilt für eine akustische Aufmerksamkeitslenkung. Auch hier können intelligente Verfahren aus dem Um-



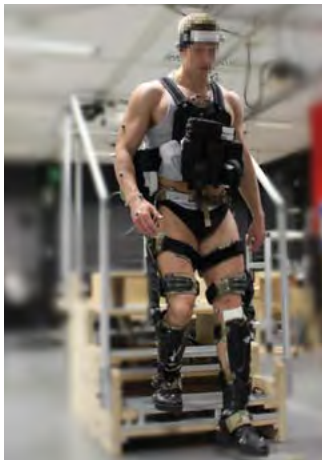
Augmented Reality zur Aufmerksamkeitslenkung.

Foto: Fraunhofer FKIE

gebungsrauschen und Stimmengewirr relevante Informationen herausfiltern. Diese werden dem Soldaten gezielt dargeboten. Durch eine multimodale Anzeige, welche gleichermaßen visuelle, akustische und haptische Verfahren einsetzt, wird ein höheres Gefahrenbewusstsein beispielsweise bei der Schützendetektion erreicht.

Auch zur Unterstützung der physischen Leistungsfähigkeit (sog. „Exoskelette“) werden KI-Verfahren eingesetzt. So wird durch die Verwendung von Robotern eine Leistungssteigerung hinsichtlich Maximalkraft und Ausdauer möglich. Herkömmliche, traditionelle robotische Systeme reagieren dabei jedoch erst auf Aktionen und Bewegungen des Benutzers; dieser Ansatz ist aufgrund der Latenzzeiten für soldatische Aufgaben nicht zielführend. Dort ist hohe Dynamik und Flexibilität erforderlich. Aus diesem Grund gilt es, die Unterstützung adaptiv an die individuellen Erfordernisse anzupassen. KI-Verfahren lernen hier den Bewegungsablauf des Benutzers und unterstützen fallweise und adaptiv. Die Unterstützung wird dann subjektiv als unterstützend wahrgenommen und akzeptiert.

Diese Beispiele aus laufenden und geplanten Forschungs- und Technologiestudien zeigen, dass eine intelligente Assistenzlösung durch KI stets eine umfassende Gesamtbetrachtung erforderlich macht. Sie umfasst den Nutzungskontext, die sich daraus ergebenen Anforderungen an die Unterstützung, die Implementierung und schließlich die Evaluation des Gesamtsystems aus Soldat, Technik und Auftrag. Geschieht keine Gesamtbetrachtung, so können KI-Verfahren und entsprechende intelligente Assistenzsysteme allerdings auch dazu führen, dass sie vom Menschen nicht als Unterstützung, sondern als Störung wahrgenommen werden. Durch eine geeignete Auslegung und intelligente Verwendung der Verfahren wird dem entgegengewirkt und die Leistung des Soldaten bei seinen Einsätzen und Missionen erhöht.



Einsatz intelligenter Verfahren zur physischen Leistungssteigerung. Foto: Fraunhofer FKIE

Click & Grasp: Assistiertes Greifen beliebiger Objekte mittels Robot Vision

Dr. Dirk Schulz, Abteilungsleiter „Kognitive Mobile Systeme“, Fraunhofer FKIE

Dr. Dirk Schulz

Foto: Fraunhofer FKIE

Immer dann, wenn wegen einer besonderen Gefährdungslage der unmittelbare Einsatz von Personal vor Ort nicht in Betracht kommt, bietet sich der Gebrauch mobiler UGVs an. Solche Roboter können mit vielfältiger Ausrüstung bestückt werden, um spezielle Bedrohungen zu bewältigen. Denkbar sind u. a. Sensoren und Wirkmittel zur CBRNE-Aufklärung, -Entschärfung oder -Räumung. Viele solcher Einsatzszenarien erfordern die entfernte, mobile Manipulation von Objekten. Die direkte Fernsteuerung eines UGVs mit Greifarm erforderte jedoch bisher eine langwierige Ausbildung des Bedienpersonals. Es braucht viel Erfahrung, selbst kleine Aufgaben zu bewältigen, wenn Antriebe und Armgelenke nur mittels Joysticks oder Knöpfen bewegt und koordiniert werden können. Trotz regelmäßiger Übung bleiben solche Einsätze zeitaufwändig und anstrengend für einen Operateur. Unterstützt von der Bundeswehr erforscht und entwickelt das Fraunhofer FKIE daher die nächste Generation intelligenter Assistenzfunktionen, welche eine entfernte Steuerung solcher Roboter deutlich einfacher und intuitiver gestalten oder Teilaufgaben sogar vollständig automatisiert erledigen können. Dank immer leistungsfähigerer mobiler Rechner und moderner KI-Algorithmen nimmt die Fähigkeit zur Echtzeit-Verarbeitung detailreicher Videodatenströme, sogenannte „Robot Vision“, stetig zu. Deren Bedeutung für autonome High-Level-Anwendungen wächst rasant. Das Bedienpersonal kann hierdurch spürbar entlastet und es können umfangreichere Einsätze in kürzerer Zeit durchgeführt werden.

Neue KI wird Robotik revolutionieren

Jüngstes Werkzeug im Arsenal intelligenter Methoden der Abteilung „Kognitive Mobile Systeme“ ist ein „Click & Grasp“-System, mit dessen Hilfe auf einfachste Weise beliebige Gegenstände mit einem Greifarm aufgenommen und an anderer Stelle, z. B. in einem Sammelbehälter, wieder abgelegt werden können. Der Demonstrator ist dazu mit einer Farb-Tiefen-Kamera ausgestattet. Der Operateur sieht in seiner Bedienoberfläche live übertragene Videobilder aus dem Einsatzgebiet des Roboters. Möchte er ein Objekt aufnehmen, kann er dieses mit einem simplen Mausklick (für mobile Geräte ist auch eine Touch-Geste möglich) oder durch Ziehen eines Begrenzungsrahmens auswählen. Dazu analysiert der Algorithmus in Sekundenbruchteilen die aktuelle Szene und generiert ein hierarchisches Strukturmodell ihrer Elemente, d. h. die Bilddaten werden in zusammenhängende Flächen, Objekte und deren Teilstücke gegliedert. Gleichzeitig imitiert das Verfahren den neurobiologischen Mechanismus der visuellen, menschlichen Aufmerksamkeit zur Bewertung aller Bestandteile der Szene nach Wichtigkeit. Der zur Nutzereingabe am besten passende Bereich wird ausgewählt und sofort auf der Anzeige hervorgehoben. Sollte der Anwender diese Selektion noch verfeinern wollen, kann er dieses mittels der digitalen Werkzeuge „vergrößern“, „verkleinern“, „hinzufügen“ oder „abziehen“ von Elementen leicht umsetzen. In den allermeisten Fällen ist dies aber gar nicht mehr nötig und es kann sofort ein Greifpunkt auf dem ausgewählten Gegenstand ausgesucht werden.
Aus den Tiefendaten (Abstandsmessungen) der Kamera wird

Das UGV sammelt mittels „Click & Grasp“-System beliebige Gegenstände im Labor ein. *Foto: Fraunhofer FKIE*

die dreidimensionale Geometrie der Szene bestimmt. Vollautomatisch und kollisionsfrei bewegt der Greifarm sich in die Aufnahmeposition, packt das selektierte Objekt rund um den Greifpunkt und hebt es an. Die Bedienoberfläche wechselt in den Ablege-Modus. Ebenfalls mit nur einem Klick ins Bild kann der Operateur nun einen Zielort bestimmen. Wieder schwirrt der Greifarm von selbst durch die Luft und setzt den Gegenstand an der gewünschten Stelle ab. Das Erlernen dieses Steuerungsverfahrens dauert in der Regel keine fünf Minuten.

Praxisnahe Wettbewerbe ermöglichen bedarfsgerechte Forschung

Die Wissenschaftler haben die Funktionalität und Effizienz des intelligenten Assistenzverfahrens nicht nur wissenschaftlich unter Laborbedingungen bewiesen, sondern mit dem Demonstrator auch mit Erfolg am „European Robotics Hackathon“ (EnRicH) teilgenommen. Dieser Wettbewerb fand in Kooperation mit dem Amt für Rüstung und Wehrtechnik (ARWT) des österreichischen Bundesheers im Juni 2017 im stillgelegten Atomkraftwerk Zwentendorf statt. Ziel war es, die derzeitigen Fähigkeiten mobiler Roboter zur Reaktion auf nukleare Katastrophen zu prüfen und voranzubringen. Als einziges Team konnten die FKIE-Wissenschaftler dabei autonom nach auf dem Boden verstreuten Zylindern mit teils radioaktivem Inhalt greifen, sie zum Strahlungsdetektor führen, die strahlenden Proben in einer Box an Bord des Roboters sammeln und schließlich die gesamte Box in einem dafür vorgesehenen Sicherheitsbehälter ablegen. So konnten innerhalb der vorgegebenen 40 Minuten aus einer Vielzahl von Zylindern vier von fünf Strahlenquellen identifiziert und geborgen werden. Diese Leistung wurde von einer Jury aus unabhängigen Experten auch mit dem Preis „Best Manipulation“ ausgezeichnet.

AKW Zwentendorf: Das UGV sichert radioaktives Material.

Foto: Fraunhofer FKIE

Voranschreitende Entwicklung der Robot Vision birgt enormes Potenzial

Für das „Click & Grasp“-System wurde bewusst ein ganzheitlicher Ansatz zur Bildauswertung für universell einsetzbare Roboter gewählt. Die Abteilung „Kognitive Mobile Systeme“ wird in den nächsten Jahren auf dieser Grundlage noch viele weitere Funktionen realisieren. Robot Vision als Basis für geometrische und semantische Umgebungserfassung greift einen Trend auf, der in der zivilen Industrie auch durch die Entwicklung autonomer Autos mittlerweile die notwendige Einsatzreife erreicht hat. Leistungsfähige Sensoren und miniaturisierte Rechner stehen zur Verfügung. Das Aufkommen ausgereifter Virtual-Reality-Brillen und Steuergeräte im zivilen Unterhaltungssektor ist ebenfalls eine Triebfeder für den weiteren Aufschwung der Robot Vision. Durch gezielte Förderung dieses Bereichs könnten auch militärische Technologien profitieren und ganz neue Bedienkonzepte und Anwendungsfelder erschlossen werden.

Assistenzsystem zu Ähnlichkeiten in Programmen zur Unterstützung von Täterattribution bei Malware

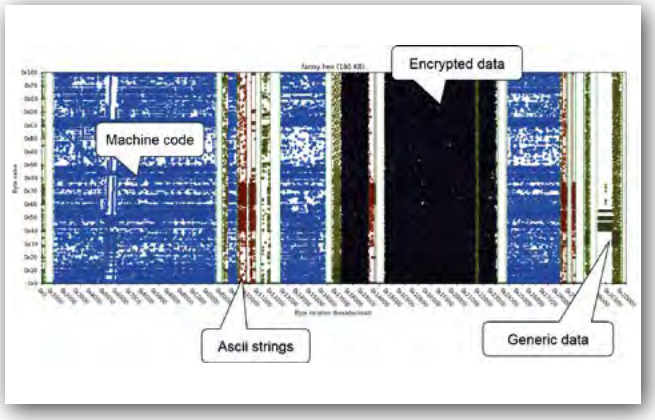
Viviane Zwanger, Abteilung „Cyber Analysis & Defense“, Fraunhofer FKIE

Viviane Zwanger

Foto: Fraunhofer FKIE

Bereits seit mehreren Jahren werden organisierte, zielgerichtete Angriffe auf Unternehmens- und Behördennetze beobachtet und untersucht. Dabei konnten wiederkehrende Vorgehensmuster und Angriffswerkzeuge identifiziert werden, die den Schluss nahe legen, dass es sich um feste Tätergruppen handelt. Die Attribuierung von Angriffen zu Tätern ist meist nicht gerichtsfest nachzuweisen, da die Spuren durch Angreifer bewusst manipuliert werden können. Dennoch bietet auch die nicht gerichtsfeste Attribuierung wertvolle Informationen über Fähigkeiten, Kapazitäten, Zielsektoren und Schwächen von Tätergruppen, die genutzt werden können, um defensive Maßnahmen zu verbessern und deren Ziele und Methodik vorherzusagen.

Im Rahmen der Arbeiten der Abteilung „Cyber Analysis & Defense“ des Fraunhofer FKIE wird daher an Methoden geforscht, um die Attribuierung von Angriffen zu verbessern. Dabei wird Maschinencode entdeckter Schadsoftware (Malware) gesammelt, analysiert und mit bekanntem Code verglichen, der bei anderen Angriffen gefunden wurde. Hieraus ergeben sich verwandtschaftliche Beziehungen zwischen den einzelnen Funden. Ähnlich wie in der kommerziellen Software-Entwicklung stellt der Schadsoftware-Code für die Tätergruppen ihr „Intellectual Property“ dar und wird möglichst geheim gehalten. Erkenntnisse über verwandtschaftliche Beziehungen von Schadsoftware-Code sind daher äußerst wirksam, um Rückschlüsse auf Tätergruppen zu ziehen.



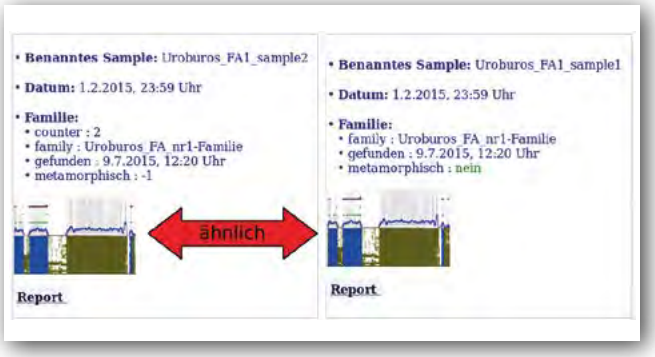
Eine vom Codescanner zerlegte Datei, der NSA Fanny Wurm. Zu sehen sind mehrere Maschinencode-Regionen (blau), die verschiedenen Komponenten entsprechen, darunter sogar ein sog. Kernel Rootkit. Außerdem Text (rot), verschlüsselte Komponenten (schwarz), und sonstige Daten (gold).

Foto: Fraunhofer FKIE

Funktionsweise der Attribuierung

Die Attribuierung nutzt drei bei Fraunhofer FKIE erforschte Methoden. Mithilfe des Codescanner wird die Schadsoftware zunächst „zerlegt“ (s. Bild 1). Dieser Schritt trennt in erster Linie den Maschinencode von Daten, um in den späteren Schritten den reinen Maschinencode betrachten zu können. Diese Zerlegung ist sinnvoll, weil Daten einfach geändert werden können und einer konstanten Veränderung unterliegen, während die Funktionalität der Malware nicht so leicht änderbar ist. Eine Besonderheit ist, dass der Codescanner nicht nur auf ausführbare Dateien angewendet wird, sondern auch auf Memory Dumps, aus dem Arbeitsspeicher ausgeschnittene Fragmente.

Dies ist deswegen wichtig, weil Malware-Entwickler sehr häufig Verschlüsselungs- und Obfuszierungs-Techniken anwenden und nur der im Arbeitsspeicher geladene Code im entschlüsselten Zustand vorliegt. Darüber hinaus ist das Verfahren nicht nur für weit verbreitete Prozessorarchitekturen von Intel/AMD anwendbar, sondern funktioniert ebenfalls auf ARM, MIPS, Power-PC und weiteren. Somit kann das Verfahren auch bei nicht-klassischen IT-Geräten, so z. B. im Bereich von Embedded Devices, militärischen Geräten und dem Internet of Things (IoT) eingesetzt werden.



Zwei Malware-Dateien, die aufgrund von Maschinencode-Ähnlichkeit zusammen gruppiert wurden. Blau: Maschinencode, golden: Daten. Die Byteplots dienen der optischen Kontrolle.

Foto: Fraunhofer FKIE

Die vom Codescanner gewonnenen Maschinencode-Bestandteile können an die dafür entwickelte Code-Datenbank übergeben werden. Mithilfe spezieller Clustering-Algorithmen wird dort ähnliche Malware zu Gruppen zusammengefasst. An dieser Stelle ist auch ein Einsatzfeld der Künstlichen Intelligenz zu finden, denn es gilt charakteristische Merkmale für verschiedene Malwaregruppen zu finden. Hier eignen sich Methoden des Machine Learning besonders gut. Die Zuordnung von Malware zu Gruppen geschieht auf Basis der Ähnlichkeit von Maschinencode (s. Bild 2). Anfänglich weisen solcherart gefundene Gruppen in der Code-Datenbank noch keine Labels auf, da der Algorithmus ohne menschliche Beihilfe nach Maschinencode-Verwandtschaft sortiert. Das heißt, dass zwar Beziehungen zwischen den Samples aufgedeckt werden können, aber für die Gruppe noch kein gebräuchlicher Name existiert. Als dritte Komponente kommt daher die Malpedia zum Einsatz. Bei der Malpedia handelt es sich um eine bei Fraunhofer FKIE entwickelte Malware-Systematik-Bibliothek, die von Experten kuratiert wird. Anhand der Beispiele aus der Malpedia können den Verwandtschaftsgruppen der Code-Datenbank gebräuchliche Namen („APT28“, „Regin“) zugeordnet werden. Aktuell geschieht diese „Namensbestimmung“ noch durch Analysten. Derzeitige Forschungsarbeit ist es daher, dies unter Verwendung von Methoden der Künstlichen Intelligenz automatisiert durchführen zu lassen.

Wird bei einem Sicherheitsvorfall Malware entdeckt, kann diese in die Code-Datenbank eingegeben und analysiert werden. Handelt es sich um bekannten oder modifizierten Schadcode, kann neben der Familien-Zugehörigkeit auch die (vermutete) Tätergruppe angegeben werden. Theoretisch könnten Tätergruppen natürlich für jedes Ziel von Grund auf neue Schadsoftware entwickeln, jedoch sind Neuentwicklungen „from Scratch“ extrem zeitaufwendig und teuer, und können daher nicht beliebig stattfinden.

Metamorphischer Maschinencode

Im Gegensatz zu zielgerichteten Angriffen, bei welchen mitunter großer Aufwand für die Entwicklung spezialisierter Schadsoftware getrieben wird, wird bei typischer Cybercrime versucht, die gleiche Schadsoftware ohne Aufwand möglichst breit und schnell zu verbreiten. Um der Erkennung durch Antivirus-Software zu entgehen, wird in diesem Umfeld metamorphischer Maschinencode eingesetzt. Für jede einzelne Datei wird der Maschinencode durch spezielle Methoden geringfügig verändert, ohne die eigentliche Schadcode-Funktion zu verändern. Signatur-basierte Antivirus-Tools können solche Malware nicht mehr erkennen. Die oben beschriebenen Methoden abstrahieren jedoch so weit vom „Äußeren“ des Maschinencodes und fokussieren auf die Funktionen, dass auch hier die Attribuierung in der Regel funktioniert, allerdings nur bis zu einem gewissen Grad. Ein weiteres, sehr häufiges Hindernis im Cybercrime-Umfeld ist Malware, die im „gepackten“ Zustand vorliegt. Der Maschinencode der Schadsoftware verbirgt sich hinter einer Art „Verschlüsselungsschicht“, die zunächst entfernt werden muss. In solchen Fällen greifen jedoch die oben angesprochenen Memory Dumps bzw. weitere dafür entwickelte Komponenten, die das automatisierte entpacken von Malware-Dateien realisieren.

Ausblick

Für die Zukunft sind erweiterte Such- und Vergleichsmöglichkeiten in Planung. Vor allem soll es möglich sein, spezifische Maschinencode-Sequenzen schnell und einfach gegen den Code-Datenbank Bestand zu testen, so dass Sequenzen aus hochspezifischen Kryptografie- und Obfuszierungsroutinen direkt gesucht werden können.

Von KI zum teilautomatisierten, hochautomatisierten oder autonomen Fahren?

Prof. Dr.-Ing. Frank Flemisch, Abteilungsleiter „Human Systems Integration“, Fraunhofer FKIE, RWTH Aachen, Forschungs- und Lehrgebiet Systemergonomie,
Marcel Baltzer, Abteilung „Human Systems Integration“, Fraunhofer FKIE

Prof. Dr.-Ing. Frank Flemisch
Foto: Fraunhofer FKIE

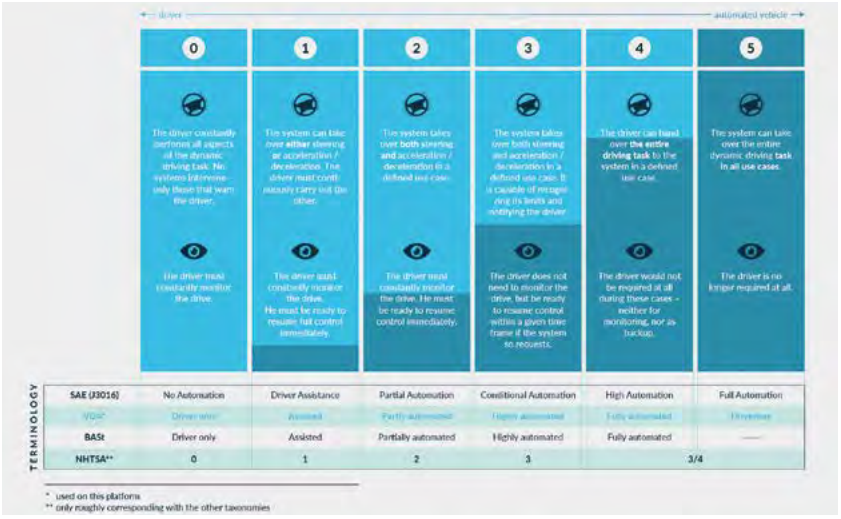
Marcel Baltzer
Foto: privat

Einführung: Ist KI und autonomes Fahren nur ein Hype?

Künstliche Intelligenz (KI, engl. Artificial Intelligence = AI) und das autonome Fahren, oft in einem Zusammenhang genannt, sind zurzeit in den Medien präsent wie kaum zwei andere technische Themen. Durchbrüche auf dem bereits Jahrzehnte alten Forschungsgebiet der KI wie mehrschichtige Neuronale Netze (Deep Learning) wecken Hoffnungen, dass damit eine Reihe von Problemen des autonomen Fahrens, z. B. das schnelle Lernen neuer Umweltsituationen, umfassend gelöst werden kann und damit dem autonomen Fahren zum Durchbruch verholfen werden kann. Gleichzeitig gibt es eine Reihe von ethischen Diskussionen um KI und Autonomie sowie wissenschaftliche Diskussionen, ob und wie Maschinelle Intelligenz deutlich mehr sein kann als Deep Learning. Namhafte Beratungsfirmen wie Gartner stufen sowohl das autonome Fahren als auch das Deep Learning als Hypes ein, die gerade den „Berg der inflationären Erwartungen“ überschritten haben und dabei sind, in das Tal der Desillusionierung abzurutschen, bevor dann in einem längeren Prozess ein Plateau der Produktivität erreicht werden kann.Das bedeutet nicht, dass man diese Forschungsrichtungen aufgeben sollte, im Gegenteil: Auch wenn sich nicht alle ursprünglichen Hoffnungen erfüllen werden, so lohnt sich auch hier der Blick ins Detail, um Chancen und Risiken fundiert abwägen zu können.

Automatisiertes oder autonomes Fahren?

In der Fachgemeinschaft spricht man mittlerweile weniger vom autonomen als vielmehr vom „Automatisierten und Vernetzten Fahren“, so auch der Titel einer Fachtagung des BMWi und BMBF Ende November 2017 in Berlin. Aus einer Situation der 1990er, als nur von Fahrerassistenzsystemen und autonomen Fahrzeugen gesprochen wurde, ist man über eine Reihe von DFG-, BMBF-, BMWi und EU-Projekten, sowie Arbeitsgruppen der BASt, der NHTSA und SAE zu einem Spektrum oder einer Skala von Assistenz- und Automationsstufen gekommen, die sich auch als Evolutionspfad hin zu höherautomatisiertem Fahren begreifen lassen (vgl. Abbildung 2). Teilautomatisierte Fahrzeuge (SAE Level 2), bei denen die Automation zwar weitgehend steuert, der Fahrer sowohl aufmerksam bleiben muss als auch volle Verantwortung behält, sind bereits in der Serie, z. B. als Stau- oder Autobahnpilot. Technische Systeme mit höheren Automationsstufen, bei denen der Fahrer unter bestimmten Bedingungen (SAE Level 3) oder immer (SAE Level 4) fahrfremde Dinge tun darf, sind von vielen größeren Fahrzeugherstellern und Zulieferern in der Serienentwicklung. So hat Audi vor kurzem angekündigt, mit dem „Audi-AI-Staupilot“ im neuen A8 das erste Serienautomobil der Welt für hochautomatisiertes Fahren in Serie zu bringen [1], bewusst mit „AI“ als Bezeichner für die Automation.



Assistenz- und Automationsgrade für das automatisierte Fahren. *Foto: 2025ad.com*

Rechtliche, ethische und ergonomische Aspekte der Automation

Wir sind mittlerweile an einem Stand der Entwicklung, bei dem ein beindruckend großer Teil der technologischen Fragen gelöst ist oder sich Lösungen bereits klar abzeichnet. Sehr früh schon wurde klar, dass die rechtliche und ethische Seite der Automation für die weitere Entwicklung bestimmend sein könnte. In einer Arbeitsgruppe der BASt sowie einem sog. „Runden Tisch Automatisiertes Fahren“, an denen der Autor mitbeteiligt war, wurden wesentliche rechtliche Rahmenbedingungen und die notwendige Begleitforschung ausgelotet [2]. Ausgehend davon wurde in einem langwierigen Prozess das Wiener Weltabkommen mit einem Zusatz versehen [3, 4, 5] sowie das Straßenverkehrsgesetz bereits dahingehend geändert, dass teil- und unter Bedingungen auch hochautomatisiertes Fahren zulässig ist, weitere Änderungen für hochautomatisiertes Fahren sind in Abstimmung. Inzwischen hat eine vom BMVI eingesetzte Ethik-Kommission zum automatisierten Fahren ihren Bericht vorgelegt und vergleichsweise klare Hinweise gegeben. Entscheidend an dieser Stelle ist, dass das autonome Fahren, also das Fahren ohne Fahrer, auf öffentlichen Straßen noch etwa ein Jahrzehnt rechtlich problematisch bleiben wird, während sich für das hochautomatisierte Fahren eine Zulassungsfähigkeit bereits in den nächsten zwei Jahren abzeichnet. Sehr gemischt, oft auch misstrauisch wird zurzeit noch das Thema KI gesehen: Das langfristige technische Potenzial wird zwar hoch, die Zulassungsfähigkeit aber als sehr kritisch eingeschätzt. Die Gründe hierfür liegen etwa in Schwierigkeiten der Nachvollziehbarkeit von selbstlernenden Algorithmen begründet sowie in der damit verbundenen schwierigen Risikoabschätzung. So werden auch beim Audi A8 Staupiloten keine selbstlernenden Algorithmen in sicherheitskritischen Fahrfunktionen eingesetzt, sondern AI wird eher als genereller Begriff für nicht-menschliche Fahrintelligenz verstanden.

Automatisiertes Fahren bei der Bundeswehr: Beispiel TULF und StrAsRob

Auch die Bundeswehr forscht zusammen mit Partnern aus Industrie und Forschung an automatisierten Fahrzeugen. So kann der TULF („Technologieträger unbemanntes Landfahrzeug“) in bestimmten Umgebungen sowohl fahrerlos fahren als auch aus anderen Fahrzeugen heraus ferngesteuert werden. In dem vom BAAINBw geförderten Projekt StrAsRob (Straßentransport mit Assistenzfunktionen von Robotern) wurde mit den Partnern Diehl, Rheinmetall, Universität der Bundeswehr München, Logistik-Schule der Bundeswehr sowie Fraunhofer FKIE ein Lkw und ein Simulationsdemonstrator aufgebaut, der u. a. zusammen mit dem TULF das automatisierte Fahren in Konvois demonstrierte (s. Abb. 3) [6]. Dabei wurde von Anfang an der amtlich anerkannte Sachverständige für Zulassungsfragen sowie zukünftige Nutzer mit einbezogen, um in Workshops wesentliche rechtliche, technische und ergonomische Fragen bereits früh beantworten zu können. Um einen frühen Einsatz dieser Technik bei gleichzeitiger Anschlussfähigkeit zu höheren Automationsgraden zu gewährleisten, wurde das Konzept so ausgelegt, dass es mit einem Sicherheitsfahrer bereits teil- und hochautomatisiert einsetzbar ist, aber auch vollautomatisiert ausgebaut werden kann. Methoden der KI wurden nur soweit eingesetzt, dass die Automation weiterhin deterministisch arbeitet und damit die Zulassungsfähigkeit nicht unnötig eingeschränkt wird.

Automatisiertes Konvoifahren mit TULF im Projekt StrAsRob.

Foto: Fraunhofer FKIE

Fazit

Versteht man KI eng als Deep Learning, so ist der Einsatz beim automatisierten Fahren aufgrund von Zulassungsfragen noch Zukunftsmusik. Versteht man KI allgemeiner als maschinelle Fähigkeit und Intelligenz zum Fahren, dann ist KI notwendige Voraussetzung zum automatisierten Fahren. Auch wenn das autonome, also fahrerlose Fahren noch etwas weiter in der Zukunft liegt, ist das teil- und hochautomatisierte Fahren im zivilen Bereich bereits kurz vor der großflächigeren Einführung, die zeitversetzt auch Auswirkungen auf den militärischen Bereich haben wird. Forschungs- und Entwicklungsbedarf liegt vor allen Dingen darin, der maschinellen Intelligenz mehr beizubringen als reine Reiz-Reaktionsschemata, sondern basierend auf zum Menschen kompatiblen Werten erfolgreich mit Menschen und anderen Maschinen zu kooperieren.

[1] Audi, 2017. „Automatisiertes Fahren auf neuem Level: der Audi AI Staupilot“. Pressemitteilung vom 7.9.2017. URL: https://www.audi-mediacenter.com/de/pressemitteilungen/automatisiertes-fahren-auf-neuem-level-der-audi-ai-staupilot-9300.

[2] Gasser, T. M.; Arzt, C.; Ayoubi, M.; Bartels, A.; Bürkle, L.; Eier, J.; Flemisch, F.; Häcker, D.; Hesse, T.; Huber, W.; Lotz, C.; Maurer, M.; Ruth-Schumacher, S.; Schwarz, J. & Vogt, W.: Rechtsfolgen zunehmender Fahrzeugautomatisierung - Gemeinsamer Schlussbericht der Projektgruppe, Bundesanstalt für Straßenwesen (bast), Bundesanstalt für Straßenwesen (bast), 2012.

[3] United Nations, „19th convention on road traffic“ Final Act, Art 8 §5, Vienna, November 1968.

[4] United Nations, „Report of 68th session of the working party on road traffic safety“ Geneva, March 2014.

[5] United Nations, „Acceptance of amendments to articles 8 and 39 of the convention“ New York, October 2015.

[6] Flemisch, F.; Baltzer, M.; Rudolph, C.; Heesen, M.; Krasni, A.; Boehmsdorff, P. & Linder, T.: Abschlussbericht FKIE. Straßentransport mit Assistenzfunktionen von Robotern (StrAsRob), Anteil Ergonomie und Use Cases, BAAINBw, BAAINBw, 2015.

Bedeutung von KI und Big Data für die NATO Science & Technology Organization

Dr.-Ing. Michael Wunder, Chairman NATO IST-Panel, Abteilungsleiter „Informationstechnik für Führungssysteme“, Fraunhofer FKIE

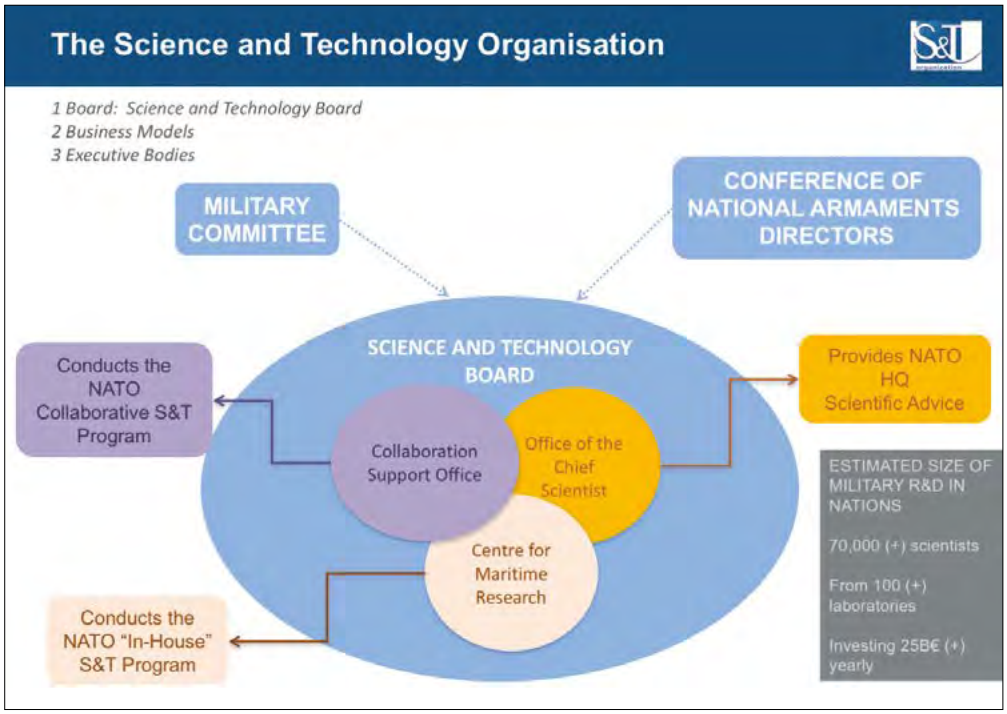
Dr.-Ing. Michael Wunder

Foto: Fraunhofer FKIE

Nicht überraschend, sind KI und auch Big Data für die NATO wesentliche Themen, die in zahlreichen Forschungsaktivitäten bearbeitet werden.

Dies geschieht u. a. innerhalb der NATO-eigenen Science & Technology Organisation (STO, www.sto.nato.int), die wissenschaftlich-technische Lösungskompetenz mit operativem Bedarf verbindet und auf diese Weise zielgerichtet innovative Ergebnisse hervorbringt. Die STO hat denselben rechtlichen Status, wie die NATO selbst und wurde zeitgleich in 1949 gegründet. Orientierung erhält die STO vom Science & Technology Board (STB), in dem sich die F&T-Direktoren aller beteiligten Nationen treffen. Den Vorsitz im STB hat ein hochrangiger Chief-Scientist, der die NATO Führung aus wissenschaftlich technischer Sicht berät. Das komplette, wehrwissenschaftliche Spektrum wird in sieben unterschiedlich fokussierten Panels im Rahmen eines bemerkenswert effizient funktionierenden, partnerschaftlich organisierten Geschäftsmodells bearbeitet. Über 5.000 Wissenschaftler, Techniker und Operateure aus den in der NATO engagierten Nationen beteiligten sich aktuell an über 280 multinationalen Forschungsaktivitäten – ein durchaus beeindruckender Think-Tank. Unter den NATO Nationen gehört Deutschland zu den aktivsten Nutzern der STO und damit den Profiteuren dieses Modells.

Mit Blick auf den bei Militärs üblichen Entscheidungszyklus (OODA-Loop) wird klar, dass alle Teilschritte ganz wesentlich von der Bewältigung von Massendaten und intelligenter Entscheidungsunterstützung profitieren. Im ersten Schritt „Observe“ geht es um die Beschaffung von Daten und Informationen. Die Erfassung und Verarbeitung von Signalen und von natürlicher Sprachen sowie deren Aufbereitung und dezentrale Vorverarbeitung, die semantische Integration heterogener Erfassungssysteme und vieles mehr bieten ein riesiges Feld für den Einsatz intelligenter Methoden und Verfahren. Beim nächsten Schritt („Orient“) geht es um Schlussfolgerungen. Auswertungen sozialer Medien, die Fusion von Daten und Informationen, die Erkennung von Anomalie, aber auch die Unterscheidung relevanter Informationen von irrelevanten oder verfälschten Informationen („Fake Data“) bieten ein enormes Potenzial für Maschinelles Lernen. Gleiches gilt für den Schritt „Decide“, bei dem augmented und virtual reality, predictive analytics und viele weitere Technologien und Methoden die Meinungsbildung unterstützen können. Ein komplexes Schlachtfeld und High-Speed-Operationen erfordern intelligente Komponenten und Geräte sowie deren Fähigkeit, mit einem gewissen Maß an Autonomie zu agieren („Act“). In allen Schritten ist also der Einsatz von KI-Technologien relevant. Insofern widmen sich zahlreiche, im IST-Panel (und anderen Panels) gestartete Aktivitäten und Veranstaltungen dem zentralen Thema der künst-



Übersicht über die Organisationsstruktur der NATO Science and Technology Organization.

Foto: NATO STO

lichen Intelligenz, das man ja stets in Verbindung mit dem zweiten Mega-Thema Massendaten (Big Data) sehen muss.
KI und Big Data sind klassische IT-Themen. Insofern ist insbesondere das Information Systems & Technology (IST) – Panel federführend bei zahlreichen Aktivitäten. Aber auch andere Panels, wie bspw. das Human Factors & Medicine (HFM) -Panel oder die Modeling & Simulation Group (MSG) bearbeiten diese Themen und nutzen dazu ihre speziellen Kernkompetenzen. Von aktuell 30 durch das IST-Panel koordinierten F&T-Aktivitäten spielen die Themen KI und Big Data bei etwa der Hälfte eine Rolle.
Es gibt keine eindeutige Definition, ab wann man bei rechnerbasierter Entscheidungsunterstützung von Künstlicher Intelligenz spricht. Scharfsinn, Genialität oder Auffassungsgabe sind keine für die Leistung von Maschinen anwendbare Bemessungsgrößen. Bei der Verwendung moderner Deep-Machine-Learning-Verfahren herrscht Einigkeit in der einschlägigen Community, dass es zutreffend ist. In einer weitergehenden Auslegung spricht man dann schon von Künstlicher Intelligenz, wenn die entwickelten Algorithmen besonders komplex und Ergebnisse für den Menschen nicht einfach nachvollziehbar sind. Insofern dürfte die Anzahl an F&T-Aktivitäten, mit KI-Anteil deutlich höher sein.
Beispielsweise werden im IST-Panel in der Research & Technology Group (RTG) mit dem Titel „Deep Machine Learning For Cyber Defense“ u. a. maschinelle Lernverfahren eingesetzt, um Angriffsvektoren für Cyberangriffe frühzeitig zu detektieren. Die RTG mit dem Titel „Autonomous Cyber Defense Agents“ untersucht die Möglichkeit, selbstständig agierende Cyber Agents zur Aufklärung von Cyberangriffen zu etablieren. So sollen im Falle eines Cyberangriffs zeitverzugslos Gegenmaßnahmen getroffen werden. In der RTG „High-level Fusion Of Hard And Soft Information For Intelligence“ werden Fusionsalgorithmen für die Kombination von technischen Daten mit von Menschen gewonnenen Informationen entwickelt, um ein insgesamt umfassenderes Lagebild zu unterfüttern.
Reizvolle Fragestellungen und neue Geschäftsmodelle versetzen Wissenschaft und Industrie derzeit in Entzücken. In einigen Fällen, wie bspw. in der Krebsdiagnostik, bringen KI und Big Data bereits wichtige Verbesserungen. Weitere Anwendungen wie autonome Mobilität werden sich mehr und mehr durchsetzen. Im Zuge der allgemeinen Hochstimmung und dem damit verbundenen Drang, KI möglichst zügig bei der Entscheidungsunterstützung einzusetzen, darf nicht vergessen werden, dass wir vergleichsweise wenig Erfahrung damit haben. Was bedeutet es für operative Gesamtprozesse, wenn Entscheidungen auf maschinellem Lernen basieren? Was passiert, wenn ein Algorithmus zur Entscheidungsunterstützung, der als Produkt erworben oder lizensiert wurde, in eine Plattform integriert wird und dann plötzlich wesentliche Veränderungen im Umfeld auftreten (bspw. wird aus einem Feind ein Verbündeter)? Lernen, auch maschinelles, erfordert Zeit. Softwareanpassungen und Integration lassen sich wohl kaum immer online und ohne Zeitverzug durchführen. Wie geht man also mit einer unsicheren Qualität der auf KI basierenden Ergebnisse um? Ein anderes Problem ist, dass in den mit Massendaten trainierten Algorithmen unerkannte Tendenzen zu zweifelhaften Ergebnissen führen können. Bei Big Data lassen sich die in den enormen Datenmengen verborgenen Zusammenhänge schließlich nicht ohne weiteres erkennen. Wie kann man sicher sein, dass Computer das aus menschlicher Sicht Richtige erlernen?
Solange ein Computer mit Blick auf das von ihm gewonnene Ergebnis nicht über die menschliche Fähigkeit verfügt, selbst in Skepsis zu verfallen, sollten wir bei künstlicher „Intelligenz“ vorsichtig sein. Über die reinen technischen Fragestellungen hinausgehend gibt es also Fragen zur Handhabung der KI und natürlich auch solche der Ethik. Es besteht erhöhter Bedarf an Diskussion sowie an Aufklärung. Angesichts der Euphorie wird auch eine nüchterne Betrachtung der Risiken wichtig sein.
Die NATO widmet sich in einer drei-tägigen Konferenz mit dem Thema „Big Data and Artificial Intelligence for Military Decision Making“ (30. Mai/1. Juni 2018, Bordeaux) diesen und weiteren Fragestellungen: http://www.fkie.fraunhofer.de/de/Veranstaltungen/NATO_IST-160_Specialists_Meeting.html

Einladungsflyer zum IST-160 Specialists' Meeting „Big Data and Artificial Intelligence for Military Decision Making“.

Foto: NATO STO

ÖA AFCEA Messe 2018

Bechtle AG: starker IT-Partner öffentlicher Auftraggeber

Ob klassische IT-Infrastruktur, Digitalisierung, Cloud, Mobility, Security oder IT als Service – Bechtle agiert bei allen Themen vernetzt, professionell und ist flexibel aufgestellt. Mit dem eigenen Geschäftsbereich Public Sector Business richtet das IT-Unternehmen gezielt seinen Blick auf die besonderen Anforderungen öffentlicher Auftraggeber. Seit vielen Jahren schon stattet Bechtle die Bundeswehr über Rahmenverträge mit Informationstechnologie aus und erbringt als starker Partner Dienstleistungen für zukunftsfähige IT-Architekturen.

Im Juni 2017 hat das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) Bechtle zum dritten Mal in Folge den Zuschlag für einen Rahmenvertrag über IT-Komponenten und Dienstleistungen erteilt. Abrufberechtigte Einrichtungen können über standardisierte Prozesse verschiedene Produkte und Dienstleistungen ausschreibungsfrei beziehen. Die Laufzeit des aktuellen Rahmenvertrags „IT-Plattform – 2./3. Rechnerebene R1112“ reicht bis 2021. Er schließt nahtlos an die bereits 2009 und 2013 geschlossenen Rahmenverträge an. Bechtle setzt damit die etablierte Partnerschaft fort und stattet auch in den kommenden Jahren die Bundeswehr mit Informationstechnologie und Dienstleistung aus. Das Kerngeschäft umfasst dabei die Bereiche Handelsware mit mobilen Endgeräten, PCs, Peripherie, Drucker, Server, Speichersysteme, USV-Anlagen, sowie hardwarenahe Softwareprodukte. Neben Lieferung von Informationstechnik plant, installiert und konfiguriert Bechtle auch IT-Umgebungen und Netzwerke. Kontinuierlich vertiefen die Partner ihre Zusammenarbeit außerdem rund um Dienstleistungen zu aktuellen Themenbereichen wie IT-unterstütztes Controlling (IT-U), IT-Sicherheitskonzepte, Service- und Systemsteckbriefe und Enterprise Architecture nach NATO Architecture Framework (NAF). Leistungen des Fachbereichs Teilekennzeichnung (TKZ) von Geräten, Gütern und Behältern mit grafischen Codierungen und Nummernkreisen runden das Dienstleistungsportfolio ab.

Wir für die Bundeswehr.

Die Bechtle AG realisiert den Vertrag als Hauptauftragnehmer unter anderem mit seinen langjährigen Herstellerpartnern HP, Dell EMC sowie den Dienstleistungsunternehmen CONET Solutions und GBS Tempest. Die modulare, an den Kundenanforderungen ausgerichtete Organisationsform ist mit lokaler Nähe und der zentralen Stärke eines internationalen IT-Konzerns optimal an die Rahmenverträge angepasst.

Die im IT-Systemhaus Bonn ansässige zentrale Projektleitstelle (ZPLS) dient der Bundeswehr als direkte Koordinierungsstelle für die Bereiche Vertrieb, technische Beratung und Validierung, Warenkorbmanagement sowie dem Projekt- und Servicemanagement.

Das Auftragsmanagement und die gesamte Lieferlogistik erfolgen gebündelt aus der Konzernzentrale der Bechtle AG in Neckarsulm.

Viele Spezialisten, zentrale Serviceeinheiten, 43 Competence Center – für Bechtle arbeiten derzeit rund 8.400 engagierte Mitarbeiter in 70 lokalen Standorten und IT-E-Commerce Gesellschaften in 14 Ländern. Ein flächendeckendes Netz, das kurze Servicewege zu den einzelnen Standorten der Bundeswehr garantiert.

Mit dieser konsequent auf die Anforderungen der Kunden ausgerichteten Aufstellung hat sich Bechtle zu Deutschlands größtem konzernunabhängigen IT-Systemhaus und zum führenden IT-E-Commerce-Anbieter in Europa entwickelt.

Bechtle AG Konzernzentrale *Foto: Bechtle AG*

Kontakt:

Bechtle AG
Zentrales Team Bundeswehr
Telefon: 0228 6888 400
Email: zpls-r1112@bechtle.com

AFCEA Bonn e.V.

Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

32. AFCEA-Fachausstellung

Informations- und Kommunikationstechnik

„Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher."

11./12. April 2017 • Maritim Hotel Bonn

11. April 2017

09:00 – 18:00 Uhr	**Ausstellung • Vorträge im Saal REGER** *Moderation:* Oberst i.G. Armin Fleischmann, stv. Vorsitzender AFCEA Bonn e.V.
10:00 Uhr	**Begrüßung / Eröffnung der 32. AFCEA-Fachausstellung** Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V.
10:10 Uhr	**Keynote: „Digitalisierung Bundeswehr"** Klaus-Hardy Mühleck, Abteilungsleiter Cyber- und Informationstechnik und CIO im BMVg
11:00 Uhr	**„Digitalisierung Bund"** Ministeraldirigent Andreas Könen, Leiter der Stabsstelle „IT- und Cybersicherheit; sichere Informationstechnik" im Bundesinnenministerium
14:00 Uhr	**„Blackout, Zero – Empfehlungen für die Digitalisierung"** Marc Elsberg, Bestsellerautor, u.a. „Blackout" (Stromausfall) und „ZERO" (Big Data/Datenschutz)
16:00 – 17:45 Uhr	**Young AFCEANs Leadership Forum im Saal REGER** Das Young AFCEANs Leadership Forum ist eine Gesprächsrunde für junge Führungskräfte mit Spitzenvertretern aus Bundeswehr, Verwaltung, Wissenschaft und Industrie, die Einblicke in ihren Lebenslauf gewähren und Karrieretipps geben. Im Mittelpunkt steht der Erfahrungsaustausch. Leitung: Frau Sandra Pfetzing-Huber, IBM
18:00 – 21:00 Uhr	**Get-together AFCEA Fachausstellung** AFCEA Bonn e.V. lädt Besucher und Aussteller der AFCEA Fachausstellung 2018 ein zu Kölsch mit Snacks im Ausstellungsbereich Foyer I/II der Fachausstellung

12. April 2017

09:00 – 17:00 Uhr	**Ausstellung • Vorträge im Saal REGER** Moderation: Oberst i.G. Armin Fleischmann, stv. Vorsitzender AFCEA Bonn e.V.
10:00 Uhr	**„Sachstand Agentur für disruptive Innovationen in Cybersicherheit"** Oberst i.G. Frank Werner Trettin, Leiter Aufbaustab ADIC
14:00 Uhr	**„Digitalisierung Gesundheitswesen Bundeswehr"** Generalarzt Dr. Michael Zallet, Abteilungsleiter B im Kommando Sanitätsdienst der Bundeswehr
Abschluss	Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V. und General Manager AFCEA Europe

Ausstellerliste AFCEA-Fachausstellung 2018

	Ausstellende Firma/Organisation	Stand
1	A. WEIDELT Systemtechnik GmbH & Co. KG	F 30
2	ACT	F 05
3	AD2V Industries GmbH	S 02
4	Airbus	M 09
5	aiso-lab Gmbh	F 46
6	Allianz	ME 21
7	AOC Red Baron Roost	ME 07
8	Aruba, a Hewlett Packard Enterprise company	S 06
9	ATM ComputerSysteme GmbH	M 06
10	Atos Information Technology GmbH	M 02
11	Avitech GmbH	S 09
12	AVS Systeme GmbH	ME 19
13	Bechtle AG	F 12
14	Behörden Spiegel/ProPress Verlagsgesellschaft mbH	F 20
15	blackned gmbh	M 01
16	Broadcast Solutions GmbH	ME 16
17	BRUGG KABEL AG	B 02
18	BWI GmbH	M 16
19	CANCOM on line GmbH	B 05
20	Carl-Cranz-Gesellschaft e.V.	ME 06
21	Carmenta AB	F 21
22	Cellebrite GmbH	S 02
23	CeoTronics AG	M 31
24	CGI Deutschland Ltd. & Co. KG	F 08
25	Cisco Systems GmbH	B 13
26	Citrix Systems GmbH	B 07
27	CMV Hoven GmbH	B 06
28	Computacenter	M 23
29	Comrod Communications AS	F 24
30	Condok GmbH	S 04
31	CONET	F 06
32	conpal Information Security Systems GmbH	S 08
33	Cordsen Engineering GmbH	F 10
34	cpm communication presse marketing GmbH	ME 04
35	crisis prevention	ME 05
36	Cubic Mission Solutions	S 02
37	dainox GmbH	M 24
38	DEKOM AG	ME 12
39	Dell EMC	F 45
40	Deutsche Gesellschaft für Wehrtechnik e.V. (DWT)	F 49
41	DIGITTRADE GmbH	F 53
42	DSI Datensicherheit GmbH	B 01
43	DXC Deutschland GmbH	M 03
44	ECOS Technology GmbH	F 29
45	EGL Elektronik Vertrieb GmbH	M 29
46	ELE.SI.A S.p.A.	S 02
47	ELNO GmbH	B 02
48	Epson Deutschland GmbH	ME 09
49	ESG Elektroniksystem- und Logistik-GmbH	M 04
50	Esri Deutschland GmbH	M 26
51	FFG Flensburger Fahrzeugbau Gesellschaft mbH	S 02
52	Forcepoint Deutschland GmbH	ME 17
53	Fraunhofer FKIE	M 25
54	Fraunhofer IOSB	B 12 + S 02
55	Frequentis Comsoft GmbH	B 09
56	FREQUENTIS Deutschland GmbH	B 09
57	GAF AG	ME 18
58	GBS TEMPEST & Service GmbH	S 03
59	Gebr. Friedrich Industrie- und Elektrotechnik GmbH	S 04
60	genua gmbh	M 19
61	griffity defense GmbH	S 02
62	Hagenuk Marinekommunikation GmbH	S 07
63	Haivision Network Video	F 28
64	Harris Geospatial Solutions	S 02
65	Hexagon Safety & Infrastructure – c/o HxGN Safety & Infrastructure GmbH	F 15
66	Hitachi Vantara	M 21
67	IABG mbH	M 27
68	IBM Deutschland GmbH	M 17
69	iesy GmbH & Co. KG	F 42
70	Indra Sistemas S.A.	S 09
71	INFODAS GmbH	M 20
72	interface projects GmbH	F 43
73	ISEC7 Group AG	ME 20
74	IT-Standort Bonn	F 04
75	itWatch GmbH	F 26 + ME 13
76	JK Defence & Security Products GmbH	F 41
77	Kommando Cyber- und Informationsraum der Bundeswehr	ME 22
78	K&K Medienverlag-Hardthöhe GmbH/ Hardthöhenkurier	ME 01
79	Lachen helfen	ME 14
80	Leonardo, vertreten durch Selex ES GmbH	B 04
81	Luciad	S 05
82	Materna GmbH	F 14
83	Media Broadcast Satellite GmbH	F 27
84	Mellanox Technologies	M 13
85	Microsoft Deutschland GmbH	F 09
86	Mittler Report Verlag	ME 03
87	Mönch Verlagsgesellschaft mbH	ME 02
88	Motorola Solutions	M 30
89	MSAB	S 10
90	ND SatCom GmbH	F 07
91	NSSLGlobal GmbH	F 48
92	NVIDIA GmbH	F 45
93	NYNEX satellite OHG	F 27
94	Oblong Industries	ME 12
95	OHB System AG	F 01
96	ORACLE Deutschland B.V. & Co. KG	F 11
97	Panasonic Computer Product Solution	F 02
98	PASS-Medientechnik GmbH	F 50
99	PELI HARDIGG	S 01
100	promegis GmbH	B 08
101	PWA Electronic Service- und Vertriebs-GmbH	F 02
102	QGroup GmbH	F 51
103	Rafael Advanced Defense Systems Ltd.	M 28

Ausstellerliste AFCEA-Fachausstellung 2018

Ausstellende Firma/Organisation		Stand
104	Rheinmetall Defence	M 05
105	roda computer GmbH	F 03
106	Rohde & Schwarz	M 08
107	rola Security Solutions GmbH	B 11
108	RUAG Defence	F 07
109	Saab Deutschland GmbH	S 02
110	Saab Medav Technologies GmbH	S 02
111	SAF Tehnika JSC	F 44
112	Samsung Electronics GmbH	M 17
113	SAP Deutschland SE & Co. KG	M 15
114	SCHNEIDER DIGITAL	F 22
115	Schönhofer Sales and Engineering GmbH	F 25
116	SciEngines GmbH	B 03
117	secunet Security Networks AG	M 13
118	Secusmart GmbH	M 11
119	SELECTRIC Nachrichten-Systeme GmbH	ME 10
120	Selex ES GmbH, a Leonardo company	B 04
121	Sennheiser Vertrieb und Service GmbH & Co. KG	F 32
122	SES Networks	F 47
123	SFC Energy AG	S 02
124	SINUS Electronic GmbH	F 31

Ausstellende Firma/Organisation		Stand
125	Software AG	M 14
126	Sophos	S 08
127	Sopra Steria Consulting	M 12
138	SQS Software Quality Systems AG	F 52
129	steep GmbH	M 07
130	SVA System Vertrieb Alexander GmbH	F 23
131	SYKO Gesellschaft für Leistungselektronik mbH	M 22
132	Systematic GmbH	M 18
133	systerra computer GmbH	ME 15
134	TELEFUNKEN Radio Communication Systems GmbH & Co. KG	M 10
135	Textron Systems	B 08
136	Thales Deutschland	F 13
137	T-Systems International GmbH	B 10
138	tukom GmbH	ME 11
139	Utimaco	S 08
140	Verband der Reservisten der deutschen Bundeswehr e.V.	ME 08
141	VITES GmbH	S 02
142	ZARGES GmbH	B 14

WLAN Fachausstellung 2018

gesponsort von

aruba

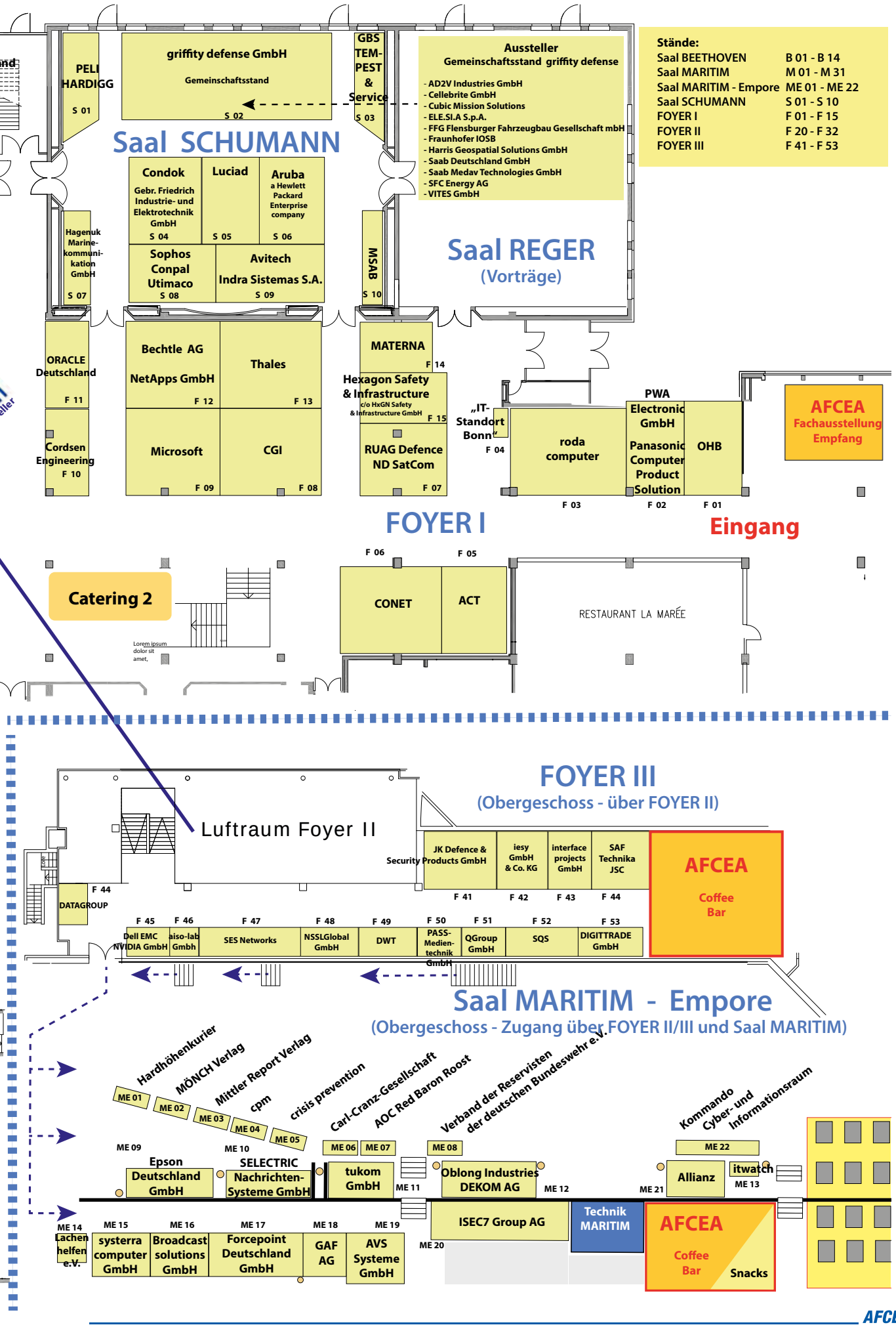
a Hewlett Packard Enterprise company

Unsere Aussteller bei der AFCEA Fachausstellung 2018

AFCEA Fachausstellung 2018

11./12. April 2018

Standplan


PELI HARDIGG
S 01
griffity defense GmbH
Gemeinschaftsstand
S 02
GBS TEM-PEST & Service
S 03
Aussteller
Gemeinschaftsstand griffity defense
- AD2V Industries GmbH
- Cellebrite GmbH
- Cubic Mission Solutions
- ELE.SI.A S.p.A.
- FFG Flensburger Fahrzeugbau Gesellschaft mbH
- Fraunhofer IOSB
- Harris Geospatial Solutions GmbH
- Saab Deutschland GmbH
- Saab Medav Technologies GmbH
- SFC Energy AG
- VITES GmbH
Stände:
Saal BEETHOVEN B 01 - B 14
Saal MARITIM M 01 - M 31
Saal MARITIM - Empore ME 01 - ME 22
Saal SCHUMANN S 01 - S 10
FOYER I F 01 - F 15
FOYER II F 20 - F 32
FOYER III F 41 - F 53
Saal SCHUMANN
Condok
Gebr. Friedrich Industrie- und Elektrotechnik GmbH
S 04
Luciad
S 05
Aruba
a Hewlett Packard Enterprise company
S 06
Hagenuk Marine-kommuni-kation GmbH
S 07
Sophos Conpal Utimaco
S 08
Avitech
Indra Sistemas S.A.
S 09
MSAB
S 10
Saal REGER
(Vorträge)
ORACLE Deutschland
F 11
Bechtle AG
NetApps GmbH
F 12
Thales
F 13
MATERNA
F 14
Hexagon Safety & Infrastructure
c/o HxGN Safety & Infrastructure GmbH
F 15
Cordsen Engineering
F 10
Microsoft
F 09
CGI
F 08
RUAG Defence ND SatCom
F 07
„IT-Standort Bonn"
F 04
roda computer
F 03
PWA Electronic GmbH
Panasonic Computer Product Solution
F 02
OHB
F 01
AFCEA
Fachausstellung
Empfang
FOYER I
Eingang
Catering 2
Lorem ipsum dolor sit amet,
F 06
F 05
CONET
ACT
RESTAURANT LA MARÉE
FOYER III
(Obergeschoss - über FOYER II)
Luftraum Foyer II
Security Products GmbH
JK Defence & Security Products GmbH
iesy GmbH & Co. KG
interface projects GmbH
SAF Technika JSC
F 41
F 42
F 43
F 44
AFCEA
Coffee Bar
F 44
DATAGROUP
F 45
Dell EMC NVIDIA GmbH
F 46
aiso-lab Gmbh
F 47
SES Networks
F 48
NSSLGlobal GmbH
F 49
DWT
F 50
PASS-Medien-technik GmbH
F 51
QGroup GmbH
F 52
SQS
F 53
DIGITTRADE GmbH
Saal MARITIM - Empore
(Obergeschoss - Zugang über FOYER II/III und Saal MARITIM)
Hardhöhenkurier
MÖNCH Verlag
Mittler Report Verlag
cpm
crisis prevention
Carl-Cranz-Gesellschaft
AOC Red Baron Roost
Verband der Reservisten der deutschen Bundeswehr e.V.
Kommando Cyber- und Informationsraum
ME 01
ME 02
ME 03
ME 04
ME 05
ME 06
ME 07
ME 08
ME 09
ME 10
ME 11
ME 12
ME 13
ME 21
ME 22
Epson Deutschland GmbH
SELECTRIC Nachrichten-Systeme GmbH
tukom GmbH
Oblong Industries DEKOM AG
Allianz
itwatch
ME 14
Lachen helfen e.V.
ME 15
systerra computer GmbH
ME 16
Broadcast solutions GmbH
ME 17
Forcepoint Deutschland GmbH
ME 18
GAF AG
ME 19
AVS Systeme GmbH
ME 20
ISEC7 Group AG
Technik MARITIM
AFCEA
Coffee Bar
Snacks

Aussteller AFCEA-Fachausstellung 2018

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

Stände:			
FOYER I	F 01 – F 15	Saal BEETHOVEN	B 01 – B 14
FOYER II	F 20 – F 32	Saal MARITIM	M 01 – M 31
FOYER III	F 41 – F 53	Saal MARITIM – Empore	ME 01 – ME 21
		Saal SCHUMANN	S 01 – S 10

A. WEIDELT Systemtechnik GmbH & Co. KG F 30

Die A. Weidelt Systemtechnik ist ein seit Jahrzehnten führender Systemintegrator und unverzichtbarer zuverlässiger Partner der Bundeswehr und ziviler Kunden. Durch langjährige Erfahrung in der Realisierung mobiler und stationärer Systeme, sowie

- ein hohes Maß an Kompetenz und Erfahrung spezialisierter Mitarbeiter,
- fachkompetente Projektleitung, Konstruktion und Integration,
- Systemschulung und Dokumentation,
- ständige Weiterentwicklung von Systemen und Neukonzipierungen,
- einen bundesweiten Vor-Ort-Service,
- umfangreiche Erfahrungen in der Durchführung von militärischen Beschaffungsvorhaben und Projekten, liefern wir Lösungen zugeschnitten auf die individuellen Problemstellungen des Kunden.

ACT F 05

Seit über 36 Jahren unterstützen wir Unternehmen und Organisationen als IT-Dienstleister bei der Optimierung und dem reibungslosen Betrieb ihrer IT. Wir planen, richten ein und überwachen Infrastrukturen und entwickeln individuelle Customer Communication Management-Lösungen, analysieren Geschäftsprozesse und unterstützen die Betriebsorganisationen durch qualifizierte Dienstleistungen. Wir gestalten die Zukunft unserer Kunden und schaffen durch Anwendung neuster Technologien Vorteile. Entwicklungen vorantreiben und dem Wettbewerb immer eine Nase voraus sein, dies ist unser Ziel! Denn damit heben wir uns nicht nur ab vom klassischen IT-Dienstleister – sondern bringen Bewegung ins Business. Indem wir bei allem, was wir tun, immer einen Schritt weiterdenken.

AD2V Industries GmbH S 02

Die AD2V Industries GmbH ist ein hoch innovatives österreichisches Unternehmen, welches weltweit im Fachbereich von lichtempfindlichen optronischen Sensoren und Systemen für professionelle und behördliche sowie militärische Anwendungsgebiete tätig ist. Das Kerngeschäft des Unternehmens ist die Entwicklung, die Produktion und der Vertrieb von patentierten digitalen optoelektronischen Geräten und Systemen, insbesondere von digitalen Nachtsichtsystemen.
Die Produktpalette reicht von Tag- und Nachtsichtsystemen über externes Zubehör bis hin zu individualisiertem Project Engineering, um spezielle Kundenbedürfnisse erfüllen zu können bzw. die Produkte optimal in die bestehende Infrastruktur integrieren zu können.

Airbus M 09

Airbus ist ein weltweit führendes Unternehmen im Bereich Luft- und Raumfahrt sowie den dazugehörigen Dienstleistungen. Airbus bietet die umfangreichste Verkehrsflugzeugpalette mit 100 bis über 600 Sitzen sowie Produkte für den Geschäftsflugverkehr. Das Unternehmen ist europäischer Marktführer bei Tank-, Kampf-, Transport- und Missionsflugzeugen und eines der größten Raumfahrtunternehmen der Welt. Die zivilen und militärischen Hubschrauber von Airbus zeichnen sich durch hohe Effizienz aus und sind weltweit gefragt.

aiso-lab Gmbh F 46

Die aiso-lab Gmbh bietet Bilderkennungssysteme auf Basis von Künstlicher Intelligenz an. Das Produkt Raypack Face Detection ist eine weltweit führende Technologie zur Gesichtserkennung und – Identifikation. Hunderte Personen können in Real-Time Kamera-Videostreams erkannt und verfolgt werden. Revolutionär ist die Möglichkeit, neue Gesichtsprofile im laufenden Betrieb hinzuzufügen und bei Bedarf auch wieder zu entfernen.
Raypack Drone Detection ist eine Software, um Dronen aus Live-Kamerabildern (im sichtbaren und Infrarot-Bereich) zu entdecken und nachzuverfolgen und kritische Infrastrukturen vor Angriffen aus der Luft zu schützen. Raypack AICam ist eine intelligente Kamera für individuelle, flexible Überwachungssysteme.
Kontakt: Joerg Bienert, aiso-lab GmbH,CEO & Founder, Tel.: +49 177 7940463, E-Mail: joerg.bienert@aiso-lab.com, www.aiso-lab.com

Allianz ME 21

CyberSchutzKonzepte
Von der Sensibilisierung Ihrer Mitarbeiter über die Sicherheits-Analyse, die Sicherheitsberatung bis hin zur Assistance-Leistung. Im Angriffsfall erhalten Sie bei uns die von Ihnen benötigte Hilfestellung aus einer Hand. Im Ernstfall brauchen Sie Experten aus den Bereichen Krisenmanagement, Recht, IT-Forensik und Öffentlichkeitsarbeit um kurzfristig auf den nächsten Cyber-Angriff reagieren zu können.
Ferner kann Sie unser Netzwerk aktiv bei der Umsetzung der neuen Europäischen Datenschutz-Grundverordnung unterstützen. Dies gilt unter anderem durch die Risiko-Absicherung im Rahmen eines Versicherungskonzeptes.
Kontakt: Dipl.-Volkswirt Christos Pechlivanidis, Dipl.-Kaufmann Michael Jung
Besuchen Sie uns gerne am Stand ME 21 im Obergeschoß neben der Coffee-Bar oder auf www.cyber-schutz-netwerk.de.

AOC Red Baron Roost ME 07

Der AOC Red Baron Roost ist das deutsche Chapter der internationalen Fachinteressengemeinschaft für den Elektronischen Kampf, der in den 1960'ziger Jahren gegründeten Association of Old Crows. Wir bieten unseren Mitgliedern aus den Streitkräften, den wehrwissenschaftlichen und wehrtechnischen Instituten und der Rüstungsindustrie ein anerkanntes Forum zum fachlichen Erfahrungs- und Interessenaustausch. Neben dem für unsere Mitglieder kostenfreien monatlich erscheinenden Fachmagazin "Journal of Electronic Defence (JED)" bieten wir regelmäßige Informationsveranstaltungen und Themenabende zu aktuellen Themen rund um die Bereiche EW, IO, EMSO und CEMA an. Sie finden weitere Informationen unter www.aoc-redbaronroost.de und www.crows.org

Aruba S 06

Aruba, a Hewlett Packard Enterprise company, ist ein führender Anbieter von Next-Generation-Netzwerklösungen für Unternehmen jeder Größe weltweit. Das Unternehmen liefert IT-Lösungen, mit denen Organisationen die neueste Generation von technikversierten Nutzern, die sich sowohl bei der Arbeit als auch im Privatleben

voll und ganz auf Cloud-basierte Geschäftsanwendungen verlassen, unterstützen. Weitere Informationen und aktuelle Nachrichten zu Aruba erhalten Sie auf http://www.arubanetworks.com, Twitter und Facebook. Um mehr über die neusten technischen Diskussionen zu Mobility und Produkten von Aruba zu erfahren, besuchen sie Airheads Social unter http://community.arubanetworks.com.

ATM ComputerSysteme GmbH — M 06

Die ATM ComputerSysteme GmbH ist ein international aktives Systemhaus für gehärtete IT-Hardware und Software. Als langjähriger Partner der Bundeswehr ist die ATM seit mehr als drei Jahrzehnten erfolgreich. Fokus der Entwicklungen sind Computer- und Displaysysteme, Panel-PCs, mobile wie stationäre Kommunikationsanwendungen sowie die Erstellung leistungsfähiger und passgenauer Software. Die IT-Systeme trotzen härtesten Umweltbedingungen, wie sie zu Land, zu Luft und zu Wasser herrschen. Wer im internationalen Markt bestehen will, muss maßgeschneiderte Produkte präsentieren. Die ATM verwirklicht dies mit ihren innovativen Lösungen. Dienstleistungen und Beratung rund um das Produkt charakterisieren die Unternehmens- und Produktphilosophie.

Kontakt: ATM ComputerSysteme GmbH, Max-Stromeyer-Str. 116, 78467 Konstanz, Tel.: +49 75 31 808 44 62, info@atm-computer.de, www.atm-computer.de

Atos Information Technology GmbH — M 02

Atos ist ein weltweit führender Anbieter für die digitale Transformation mit Sitz in Bézons/Paris und München. Mit rund 100.000 Mitarbeitern erzielte die Atos Gruppe 2016 circa 12 Milliarden Euro Umsatz. Als europäischer Marktführer für Big Data, Cybersecurity, High Performance Computing und Digital Workplace unterstützt Atos Unternehmen weltweit und begleitet die digitale Transformation von Kunden aus allen Branchen. Atos präsentiert auf der AFCEA seine Lösungskompetenz bei der Entwicklung und Betriebsunterstützung von einsatzfähigen IT-Plattformen (insbesondere Führungsinformationssystemen) und bietet Informationen zu Technologietrends.

Kontakt: Atos Information Technology GmbH ; Franz-Geuer-Str. 10; D-50823 Köln; Hubert Geml (Leiter Defense); Tel.: +49 (173) 9793 804; hubert.geml@atos.net

Avitech GmbH — S 09

Avitech GmbH, eine Tochtergesellschaft der Indra Sistemas S.A., ist seit über 20 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfoSysBw und InfoDADBw. Unsere Kompetenzen liegen im Bereich der Aero-nautischen und Hindernis Datenbank, Luftfahrtkarten, sowie Flugplan- und Pilotenbriefingssysteme inklusive Schnittstelle zur zivilen Flugsicherung und zu Euro-control. Darüber hinaus sind Meldungsvermittlungs- und Kommunikationssysteme sowie SWIM Lösungen bei der Bw im Einsatz. Avitech Produkte werden bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an ca. 100 Standorten genutzt. Auf der AFCEA 2018 ist Interoperabilität, Datenversorgung für Missionsplanung und Datenvisualisierung unser Schwerpunkt.

Kontakt: Thomas Mattick, Programm Manager Bundeswehr, Bahnhofplatz 3, 88045 Friedrichshafen, Tel.: +49(0)7541 / 282-0, www.avitech.aero

AVS Systeme GmbH — ME 19

Der lebenswichtige Notruf, die entscheidenden Informationen oder die visuelle Unterstützung von Entscheidungsträgern in spezifischen Situation – in jeder Branche gibt es Momente, die nicht unterbrochen, gestört, oder vorzeitig beendet werden dürfen. Die AVS Systeme GmbH hat sich auf die Planung und Realisierung von hoch technisierten audiovisuellen Visualisierungssystemen und Systemanlagen in Leitstellen und Führungsräumen spezialisiert – deutschlandweit, europaweit und über zahlreiche Märkte und Branchen hinweg. Dank 20 jähriger Unternehmenserfahrung mit eigener Forschung und Entwicklung, kann AVS Technologien und Lösungen garantieren, die zukunftsweisend, faszinierend und zuverlässig sind.

Kontakt: AVS Systeme GmbH, Steinhäuserstraße 12, 76135 Karlsruhe, Tel.: +49 (0)721 96470 0, Direkt: +49 (0)721 96470 11, Fax: +49 (0)721 96470 10, E-Mail: Tobias.Baader@avs-systeme.com, Web: www.avs-systeme.com

Bechtle AG — F 12

Starker IT-Partner öffentlicher Auftraggeber

Für Bechtle arbeiten derzeit rund 8.400 Mitarbeiter in 70 Standorten und E-Commerce Gesellschaften in 14 Ländern. Mit dem Bereich Public Sector Business richtet Bechtle sich gezielt an die Bedürfnisse öffentlicher Auftraggeber. Das Kerngeschäft umfasst dabei die Bereiche Handelsware mit Hardware, sowie hardwarenahe Software. Daneben zählt die Planung, Installation und Konfiguration von IT-Umgebungen und Netzwerken ebenso zum Portfolio. Der Ausbau von Dienstleistungen wie IT unterstütztes Controlling (IT-U), IT Sicherheitskonzepte, Cyber Resilience, Service- & Systemsteckbriefe, Enterprise Architecture nach NAF und Teilekennzeichnung (TKZ) von Geräten, Gütern und Behältern mit grafischen Codierungen und Nummernkreisen runden das Dienstleistungsportfolio ab.

Kontakt: Gabor Jeszenöi, Zentrales Team Bundeswehr, Key Account Manager, Bechtle AG

Tel.: +49 228 6888-400, ZPLS-R6717@bechtle.com, www.bechtle.com

Behörden Spiegel / ProPress Verlagsgesellschaft mbH — F 20

Der Behörden Spiegel ist mit einer Druckauflage von 114.000 Exemplaren monatlich, die auflagenstärkste unabhängige Zeitung für den Öffentlichen Dienst in Deutschland. Neben der Bundeshauptstadt Berlin sind 16 Landeshauptstädte, der Standort Bonn und letztlich jede Kommune und jeder Landkreis Ziele des Vertriebs. Neben den Beziehern aus dem Öffentlichen Dienst gehören aber auch die Parlamente, die Wirtschaftsverbände, die ausländischen Missionen, Berufsverbände und Gewerkschaften des Öffentlichen Dienstes sowie Industrievertretungen zu den regelmäßigen Lesern. Zahlreiche Städte haben eine verdichtete Verbreitung des Behörden Spiegel, nämlich dort, wo obere Bundes- und Landesbehörden oder zentrale behördliche Einrichtungen sitzen. www.behoerdenspiegel.de

blackned gmbh — M 01

blackned – critical command and control solutions. anywhere.

Die blackned gmbh ist ein Beratungsunternehmen für moderne Kommunikations- und Datenübertragungslösungen mit Sitz in Süddeutschland. Mit ihrem Beratungs- und Lösungsportfolio stellt die blackned gmbh Ihren Kunden ganzheitliche Systemlösungen für Kommando-, Kontroll- und Kommunikationsanwendungen für unterschiedlichste Branchen und Industriesegmente zur Verfügung.

Im Rahmen der AFCEA 2018 stellt die blackned den derzeitgen Planungsstand einer möglichen Systemarchitektur für das Programm MOTAKO / Digitalisierung Landbasierte Operationen vor. Die Architektur wird in Zusammenarbeit mit einer Vielzahl von Partner im Auftrag des BAAINBw entwickelt und soll bereits in 2018 in einem ersten Versuch funktional getestet werden.

blackned gmbh • +49 (0) 8331 9959 – 600 • info@blackned.de • www.blackned.de

Broadcast Solutions GmbH — ME 16

Mit mehr als 120 Mitarbeitern weltweit und Dependancen in Europa, Asien und Middle East ist die Broadcast Solutions GmbH einer der größten Systemintegratoren Europas im Bereich Broadcast-Technik. Mit jahrelanger Erfahrung im Broadcast-Bereich bietet das Unternehmen das nötige Know-how und die technischen Möglichkeiten, um dem BOS-Bereich komplett neue und innovative Produkte und Komplettlösungen für den taktischen und strategischen Einsatz anzubieten. Wir stellen unseren Kunden neuartige Lösungen zur Verfügung, die für Up- und Downlink im Bereich der Satellitenkommunikation (VSAT), moderner COFDM Übertragungstechnologie oder drahtloser Kommunikation mit Mesh-Netzwerken zur Übertragung von Daten, Audio und hochauflösendem Video-Material entscheidende Vorteile bieten.

Kontakt: Broadcast Solutions GmbH, Sebastian Schlusnus, Head of Marketing
Alfred-Nobel-Str. 5, 55411 Bingen am Rhein,
s.schlusnus@broadcast-solutions.de
Tel.: +49 (0) 6721/4008-298, +49 (0) 171/265 16 34,
www.broadcast-solutions.de

BRUGG KABEL AG — B 02

Brugg Cables ist für Signal- und Energiekabel weltweit bekannt. In der Wehrtechnik besticht Brugg Cables durch besonders robuste taktische fiberoptische Feldkabel, konfektioniert mit verschiedensten Militärsteckertypen. Diese Stecker sind zu tausenden seit über 10 Jahren im harten Feldeinsatz. Die breite Zubehörpalette, zur Feldverlegung, die Test-, Unterhalts- und Reparaturkits werden von anspruchsvollen Militärkunden gefordert. Die angebotenen Lösungen sind in der Schweizer Armee, der Bundeswehr, bei weiteren NATO-Mitgliedern und Streitkräften weltweit beliebt. Der große Erfahrungsschatz in Design und Systemintegration fließt in die Lösungspalette, sowie in Kundenschulungen ein. Am Stand B02 im Saal Beethoven präsentieren wir als Hauptthema unsere patentierten Blitzschutzlösungen für Camp- und Ausseneinsatz.
Kontakt: Brugg Kabel AG, Klosterzelgstrasse 28, CH-5201 Brugg, Vertrieb Deutschland, Edi Lützenkirchen Tel.: +49 170 188 20 71

BWI GmbH — M 16

Die BWI GmbH gehört zu den Top-10-IT-Service-Unternehmen in Deutschland. Seit dem 28. Dezember 2016 ist die BWI eine 100%ige Bundesbeteiligung. Seit dem 1. August 2017 sind die BWI-Gesellschaften zu einem Unternehmen verschmolzen, das seitdem unter dem Namen „BWI GmbH“ firmiert. Neben dem verlässlichen und sicheren Betrieb von Teilen des IT-Systems der Bundeswehr entwickelt die BWI die IT-Infrastruktur der Bundeswehr weiter und bietet dieser zukunftsweisende und sichere Services. Zusätzlich zu IT-Dienstleistungen für die Bundeswehr bietet die BWI als IT-Dienstleistungszentrum des Bundes ihre Lösungen auch anderen Ressorts der Bundesregierung an und spielt eine wichtige Rolle in der „IT-Konsolidierung Bund“. Die BWI präsentiert sich bei der AFCEA Fachausstellung 2018 als kundenorientiertes IT-Systemhaus mit innovativen IT-Entwicklungen für die Bundeswehr. **www.bwi.de**

CANCOM on line GmbH — B 05

Die CANCOM on line GmbH ist aufgrund seiner mehrjährigen Erfahrung im Public-Sektor optimal darauf eingestellt, die dedizierten Anforderungen von Bund, Ländern und Kommunen zu erfüllen. Darüber hinaus unterstützen wir seit Jahren Sicherheitsbehörden sowie die Bundeswehr. Unser bundesweit agierendes Team erfasst Ihre speziellen Ansprüche und bietet maßgeschneiderte Lösungen und Dienstleistungen für diesen Bereich an.
Seit 2016 hält die CANCOM den Rahmenvertrag für Virenschutz der Bundesverwaltung, durch den auch die Bundeswehr als Bedarfsträger beschaffen kann.
Mit CANCOM Public Solutions betreuen wir Sie umfassend in verschiedenen Bereichen des Öffentlichen Sektors:

- Gewährleistung einer sicheren und störungsfreien IT Infrastruktur
- Umfassender Schutz personenbezogener Daten
- Individuelle Beratung und Konzeptionierung einer IT Architektur für Ihre Bedürfnisse
- Branchenspezifische Lösungen und umfassendes Know-How im Public Bereich, seit 25 Jahren

Carl-Cranz-Gesellschaft e.V. — ME 06

Gesellschaft für technisch-wissenschaftliche Weiterbildung
Technisch-wissenschaftliche Weiterbildung für Ingenieure und Naturwissenschaftler auf höchstem Niveau – Dieser Aufgabe widmet sich die Carl-Cranz-Gesellschaft e.V. (CCG) als gemeinnützige Einrichtung seit mehr als 50 Jahren. Gemeinsam mit führenden Experten aus Forschung & Entwicklung sowie Industrie erarbeiten wir das Potenzial zukunftsträchtiger Technologien und stellen bedarfsgerechte, praxisorientierte Fort- und Weiterbildungen in unserem Seminarzentrum in Oberpfaffenhofen, an weiteren Standorten in Deutschland, Frankreich, Österreich, der Schweiz sowie bei Bedarf auch Inhouse zur Verfügung. Kleine Lerngruppen und renommierte Dozenten aus Hochschule, Forschung und Industrie garantieren den Lernerfolg. Zu unseren Kernkompetenzen zählen die Fachgebiete Informations- und Kommunikationstechnologie, Führungs- und Aufklärungssysteme, Mobilität / Transport- und Verkehrssysteme, Sensorik, Verteidigung- und Sicherheitstechnik, Werkstoffkunde und Werkstofftechnologie sowie fachgebietsübergreifende Querschnittsthemen.
Kontakt: Jutta Ries, Marketing, Argelsrieder Feld 11, 82234 Weßling/Obb., Tel.: +49 8153 88119813, Fax +49 8153 88119819, petra.walter@ccg-ev.de, www.ccg-ev.de

Carmenta AB — F 21

Seit mehr als 30 Jahren entwickelt Carmenta erstklassige Software für missionskritische Systeme wie Anwendungen für Verteidigung und Public Safety, bei denen Superior Situational Awareness unerlässlich ist. Carmenta hat ein umfassendes Portfolio leistungsstarker Softwareprodukte zur Missionsoptimierung mit Geodaten in Echtzeit entwickelt. Unsere Produkte und Lösungen werden derzeit von mehreren Streitkräften in allen drei Bereichen eingesetzt: Luft, Land und See. Eine enge Zusammenarbeit mit unseren Anwendern ermöglicht es uns, unsere Lösungen so zu optimieren, dass sie alle neuen oder zukünftigen Anforderungen erfüllen.
Kontakt: Carmenta Germany GmbH, www.carmenta.com, Patrick Franz, An der Haltestelle 9, D-88069 Tettnang, Tel.: +49 176 22664121, Patrick.Franz@carmenta.com

Cellebrite GmbH — S 02

Digitale Datengewinnung für eine sicherere Welt.
Digitale Daten spielen zunehmend eine wichtige Rolle bei Ermittlungen und Operationen aller Art. Diese Daten macht Cellebrite verfügbar, gemeinsam nutzbar und verwertbar. Als weltweit führendes Unternehmen für die digitale Datengewinnung mit mehr als 60.000 Lizenzen, die in 150 Ländern genutzt werden, bieten wir Strafverfolgungsbehörden, Militär, Geheimdiensten und Unternehmen die umfangreichsten bewährten Lösungen für die digitale Forensik, Sichtung und Analyse.
Die Produkte, Lösungen, Service- und Schulungsangebote von Cellebrite unterstützen unsere Kunden dabei, ihre komplexesten Fälle schnell zu lösen, indem wir ihnen das Abrufen, die gemeinsame Nutzung und die Analyse der digitalen Daten von mobilen Endgeräten, den sozialen Medien, Cloud-Diensten, Computern, Mobilfunkbetreibern und anderen Quellen ermöglichen. Deshalb ist Cellebrite der beliebteste Komplettanbieter von Lösungen für die digitale Datengewinnung und macht die Welt jeden Tag etwas sicherer.

CeoTronics AG — M 31

Innovative Produkte „Made in Germany“
Seit über 30 Jahren vertrauen die Spezialkräfte von Polizei und Militär auf die Zuverlässigkeit der Kommunikationssysteme von CeoTronics. Die kundenindividuellen Lösungen werden in enger Zusammenarbeit mit den Anwendern entwickelt. Hierbei schätzen unsere Kunden den kurzen Weg zum Ingenieurs-Know-how.
Der Konzern umfasst derzeit drei Tochterunternehmen in drei Ländern, Vertriebsmitarbeiter im In- und Ausland sowie Vertriebspartner, die die in Deutschland entwickelten und produzierten Produkte in über 40 Ländern der Erde verkaufen. Zahlreiche Premium-Hersteller von Schutzhelmen, Funkgeräten, Spezialfahrzeugen und Flugzeugen vertrauen auf die Produkte der CeoTronics AG und ihrer Tochterunternehmen.
CeoTronics AG, Audio • Video • Data Communication, Adam-Opel-Str. 6, 63322 Rödermark (Germany), Tel.: +49 6074 8751-0, Fax +49 6074 8751-265, verkauf@ceotronics.com, www.ceotronics.com

CGI Deutschland Ltd. & Co. KG — F 08

CGI, gegründet 1976, ist ein globaler Dienstleister für IT und Geschäftsprozesse, der mit 70.000 Mitarbeitern Business- und IT-Beratung, Systemintegration und Outsourcing-Services auf Top-Niveau anbietet. Unsere langjährige Erfahrung in der Zusammenarbeit mit Auftraggebern aus Militär und BOS ist der Garant für höchste Qualität, Innovation und Einsatzorientierung unseres Portfolios an marktverfügbaren Produkten und Dienstleistungen. Wir präsentieren Lösungen für den Einsatz (HaFIS) sowie für die Herausforderungen im Bereich der Cyber-Sicherheit. Mit DokMBw demonstrieren wir die Zukunft für die Stabs- und Verwaltungsarbeit. Wir freuen uns auf spannende Gespräche und den Erfahrungsaustausch im Kontext von strategischer Ausrichtung, Outsourcing und Cloud für die Bundeswehr und BWI.
Kontakt: CGI Deutschland Ltd. & Co. KG, Andreas Pankratz, Tel.: +49 22036993-0, andreas.pankratz@cgi.com, de.cgi.com

Cisco Systems GmbH B 13

Netzwerke sind heute wichtiger Teil der Infrastruktur im Bereich der Verteidigung. Die von Cisco entwickelten Produkte auf Basis des Internet-Protokolls sind Grundlage dieser Netzwerke und machen Cisco zum weltweit führenden Anbieter.
Für Institutionen im Bereich der Verteidigung eröffnet die Vernetzung über die Domänen Heimatland, verlegefähige Systeme, mobile Infrastrukturen und abgesessene Einheiten sowie mit Koalitionspartnern zahlreiche Möglichkeiten: Durch intelligentes Zusammenspiel von Personen, Prozessen, Daten und Dingen können Prozesse optimiert, Ressourcen effizienter und sicher genutzt und Vorteile in allen Domänen für Aufklärung, Gefecht, Logistik und Sanitätswesen realisiert werden. Im Geschäftsjahr 2016/17 erzielte Cisco einen Umsatz von 48,0 Milliarden $ mit weltweit ca. 70.500 Mitarbeitern.

Citrix Systems GmbH B 07

Citrix entwickelt Lösungen für eine Welt, in der Menschen, Organisationen und Dinge sicher miteinander vernetzt sind, um das Außergewöhnliche zu erreichen. Citrix unterstützt seine Kunden dabei, die Zukunft der Arbeit neu zu denken, indem das Unternehmen den umfassendsten sicheren digitalen Arbeitsplatz anbietet. Dieser vereint Anwendungen, Daten und Services, die Menschen brauchen, um produktiv zu sein und hilft der IT-Abteilung, komplexe Cloud-Umgebungen einfacher einzuführen und zu verwalten.
Mehr als 400.000 Organisationen, inklusive 99 Prozent der Fortune 100 und 98 Prozent der Fortune 500, setzen weltweit auf Lösungen von Citrix. Weitere Informationen unter http://www.citrix.de.

CMV Hoven GmbH B 06

VERTRIEB. Der Vertrieb von messtechnischen Produkten und Systemlösungen zählt zu unseren Leistungsschwerpunkten. Die Umsetzung unterschiedlichster Applikationsanforderungen und individueller Komplettlösungen für unsere Kunden aus unterschiedlichsten Bereichen der Industrie, Automotive, Luft-/Raumfahrt und Militär zählen zu unseren Hauptaufgabengebieten.
ENGINEERING. Mit individuellen Machbarkeitsstudien versuchen wir gemeinsam mit Ihnen den richtigen Schritt in Richtung Problemlösung zu gehen. Unsere Ingenieure und Techniker bringen Ihr gesamtes Know-how in Ihre Vorüberlegungen und entwickeln ganzheitliche Lösungen.
CONSULTING. Unter betriebswirtschaftlichen Aspekten führen wir in den Bereichen der Messtechnik professionelle Beratungen und Unterstützung zu den individuellen Lösungsansätzen unserer Klienten durch. Konzepte mit umfassenden, gedanklichen Entwürfen sind die bewussten Inhalte einer Problemlösung.

Computacenter M 23

Computacenter ist Europas führender herstellerübergreifender Dienstleister für Informationstechnologie. Kundennähe bedeutet für uns, Geschäftsanforderungen zu verstehen und präzise darauf einzugehen. Auf dieser Basis entwickeln, implementieren und betreiben wir für unsere Kunden maßgeschneiderte IT-Lösungen.
Darüber hinaus hält Computacenter diverse Rahmenverträge mit Landesministerien und Dienstleistungszentren verschiedener Länder und Kommunen, sowie dem Bund.
Weitere Informationen erhalten Sie gerne an unserem Stand oder über Patrick Pensel, Direktor Geschäftsfeldentwicklung für den Bereich Öffentliche Auftraggeber (Patrick.Pensel@computacenter.com) .

Comrod Communications AS F 24

Comrod Communications AS have their corporate headquarters in Stavanger, Norway with manufacturing facilities in Norway, France, Hungary and the USA. Comrod designs and manufactures manpack, vehicle, remote and shipboard antennas in the HF/VHF/UHF/SHF frequency bands. Sophisticated multiband versions are available to overcome co-site or space constraints. Support masts are available to elevate top loads at heights ranging from 5 to 34 metres (16 to 110 ft). Aluminium telescopic, composite telescopic, sectional tripod and manpack sectional models are available. Comrod ComPact series power supplies and battery chargers provide the best power to size density available on the market today.
For all product enquiries please email sales@comrod.com

Condok GmbH S 04

Die CONDOK GmbH ist ein Systemhaus für technische Dienstleistungen, System-Entwicklung und Realisierung.
Neben der Spezialisierung auf die Erstellung von IETD nach S1000D/ S2000M werden vielfältige und umfangreiche Technische Dokumentationen, Bebilderte Teilekataloge, Technische Übersetzungen und Computer Based Trainings erstellt.
Als Systemhaus entwickelt und realisiert CONDOK Einrüstungs- und Umrüstungsmaßnahmen in Kabinen und Fahrzeugen und führt Instandsetzungsleistungen durch. Das Portfolio wird durch die Bereiche der Produkt- und Betriebssicherheit sowie Themen des Integrated-Logistic-Support abgerundet.
Mit mehr als 120 Mitarbeitern in Kiel, Hamburg und Koblenz unterstützt die CONDOK mit umfangreichen technischen und logistischen Dienstleistungen die Bundeswehr sowie eine große Anzahl von Unternehmen der Wehrtechnik und der zivilen Industrie.
Kontakt: www.condok.de

CONET F 06

„Erfolg. Unsere Leidenschaft.“ CONET ist das kompetente IT-System- und Beratungshaus für SAP, Infrastructure, Communications, Software und Consulting in den Schwerpunktbereichen Cyber Security, Cloud, Mobility und Big Data. Seit mehr als 30 Jahren unterstützt CONET als IT-System- und Beratungspartner die Bundeswehr und begleitet sie zuverlässig auf dem Weg zur digitalisierten Streitkraft.
Durch partnerschaftliche Zusammenarbeit, Innovationsfähigkeit und hohe Dienstleistungsqualität entstehen erfolgreiche Implementierungen für Fach- und Führungsinformationssysteme, SAP, Kommunikationsarchitekturen und IT-Infrastrukturen. An seiner Plan-Bar (Stand F 06) präsentiert CONET aktuelle Lösungen etwa für Cyber Security, strategisches IT-Management mit EAM und Entwicklungsansätze für schnellere und gleichzeitig einfachere Prozesse mit SAP HANA.
Kontakt: www.conet.de | info@conet.de

conpal Information Security Systems GmbH S 08

Die conpal Information Security Systems GmbH ist ein Anbieter von Lösungen im Bereich IT-Sicherheit mit Fokus auf den Themen Endgeräte-Sicherheit, Authentisierung, sowie Identity und Access Management. Grundlage des Angebotes sind eigenentwickelte Standard-Software-Lösungen und Technologien sorgfältig ausgewählter Partnerunternehmen. Durch kontinuierliche Analyse von Markt- und Technologieentwicklungen erreichen wir in unserem Portfolio einen optimalen Mix zukunftssicherer Technologien in Verbindung mit praxisorientierter Umsetzung. Die Lösungen von conpal sind konsequent an den Bedürfnissen der Kundenumgebungen ausgerichtet, einfach einzuführen und verhalten sich robust im Betrieb.

Cordsen Engineering GmbH F 10

CORDSEN Engineering GmbH entwickelt und fertigt eine breite Palette an militärisch gehärteten (Ruggedized) Workstations und Peripheriegeräten nach MIL-STD-810F / MIL-STD-461E für mobilen und stationären Einsatz, sowie abstrahlsichere (TEMPEST) Produkte nach SDIP 27 Level A , wie Workstations, Server, TFT-Displays bis 70″, FO-Hubs, Drucker und Scanner.
Wir verfügen über zwei TEMPEST/EMV-Labore: Für Zulassungsmessungen nach SDIP 27 Level A/B/C, sowie für Zulassungsmessungen und Kurzmessungen nach dem Zonenmodell. Als Dienstleistungen bieten wir u. a. Platform-Testing an.
Mit der Firma Twinhead, einem der führenden Hersteller von rugged Equipment, wurde ein Kooperationsvertrag abgeschlossen.
Kontakt: Cordsen Engineering GmbH, Am Klinggraben 1A, D-63500 Seligenstadt Tel. 06182-9294-0, Fax 06182-9294-45, www.cordsen.com

cpm communication presse marketing GmbH ME 04

cpm communication presse marketing GmbH wurde 1989 als Dienstleistungsgesellschaft für Publikationen, Tagungen und Studien in ausgewählten Marktsegmenten gegründet. In enger Zusammenarbeit mit vornehmlich militärischen Stellen und der Wirtschaft veranstaltet cpm nationale und internationale Fachtagungen (z.T. mit begleitender Ausstellung).
Zu unseren Veröffentlichungen gehören:

- cpm forum – Das Magazin für Wehrtechnik und Logistik als themenorientierte wehrtechnische Dokumentationen mit jährlich 6 Publikationen
- Taschenbuch „Deutsche Bundeswehr – Folge 5 (2015)“ als aktuelles Nachschlagewerk über die deutschen Streitkräfte
- Taschenbuch „Die Ausrüstung der Bundeswehr“ – Folge 2 (2013).
- Die Internetplattform „German Defence Industry“

Kontakt: info@cpm-st-augustin.de / www.german-defence-industry.com

crisis prevention / BETA Verlag & Marketinggesellschaft mbH ME 05

CRISIS PREVENTION (CP) ist das behördliche Fachmagazin für Gefahrenabwehr, Innere Sicherheit und Katastrophenhilfe und deckt das breite Spektrum an redaktionellen Inhalten ab, was fach- und ressortübergreifend notwendig ist, um die Leserschaft umfassend auf dem aktuellen Stand zu halten und eine Hilfestellung zur täglichen Aufgabenbewältigung und Einsatzoptimierung zu leisten.
Der Leserkreis sind Dienststellenleiter, Multiplikatoren und Sicherheitsbeauftragte aus den Behörden und Organisationen mit Sicherheitsaufgaben (BOS), der Bundeswehr, Hilfsorganisationen, Betreiber Kritischer Infrastrukturen sowie Bundesämtern und Verbänden, Ministerien und Verwaltungen. Dieser Leserkreis erhält die CP quartalsweise (personalisiert) deutschlandweit direkt in die jeweilige Dienststelle.

Cubic Mission Solutions S 02

Cubic Mission Solutions (CMS) bietet vernetzte Führungs-, Kontroll-, Kommunikations-, sowie Überwachungs- und Aufklärungsfunktionen (C4ISR) für militärische und BOS-Einsätze. Unsere C4ISR-Lösungen bieten Informationserfassung, -bewertung, -nutzung und -verteilung in einer sicheren, netzzentrierten Umgebung. Unsere Technologie ermöglicht die Übertragung von Push-to-Talk-Funk, Telefon, Video und Daten über eine breite Palette von Technologien, einschließlich Mobilfunk-, Wi-Fi- und Satellitennetzwerken.
Unsere 60-jährige Erfahrung und unser Engagement für kontinuierliche Innovation, stellen sicher, dass unsere Kunden auf ihre nächste Mission vorbereitet sind.
Kontakt: Cubic Mission Solutions, Ronnie J. Rinaldi, Sr. Dirctor C4ISR Solutions, Ronnie.Rinaldi@cubic.com, www.cubic.com/Mission-Solutions

dainox GmbH M 24

dainox ist ein Hersteller **verlegefähiger Kommunikationslösungen** der Bundeswehr und etablierter Dienstleistungsanbieter in den Themengebieten **Internetworking, Computing und Virtualisierung**. **dainox** unterstützt bei der **Planung, Implementierung, Dokumentation** und dem **Betrieb** von **IT Infrastrukturen**. Mit Hilfe der **dainox Strategie- und IT Architekturberatung** werden nachhaltige und langlebige **IT Lösungen** geschaffen.
In unseren Projekten wird über eine enge **Zusammenarbeit** mit dem Kunden ein effizienter Ablauf mit einem optimalen **Know-how Transfer** garantiert und so eine **hohe Wertschöpfung** ermöglicht.
Gebündeltes Fachwissen auf den Punkt gebracht – **dainox** ®.
dainox GmbH, info@dainox.net, www.dainox.net

Dell EMC F 45

Dell EMC ist Teil der Unternehmensfamilie Dell Technologies und ermöglicht es Organisationen, ihre Rechenzentren durch den Einsatz branchenführender konvergenter Infrastrukturen, Server, Speichersysteme und Datensicherheits-Technologien zu modernisieren, zu automatisieren und zu transformieren. Unternehmen und Behörden schaffen damit eine verlässliche Grundlage, um ihre IT durch Hybrid-Cloud-Lösungen und ihr Geschäft durch Cloud-native Anwendungen und Big-Data-Lösungen zukunftsfähig zu machen. Kunden in 180 Ländern, einschließlich 98% der Fortune-500-Unternehmen, vertrauen auf die IT-Lösungen von Dell EMC und das branchenweit umfangreichste und innovativste Portfolio - vom Client über Lösungen für das Rechenzentrum bis in die Cloud.

DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT) F 49

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

DIGITTRADE GmbH F 53

Externe verschlüsselte Festplatten mit BSI-Zertifizierung
Mit der externen Festplatte HS256 S3 bietet die DIGITTRADE GmbH Behörden und Unternehmen eine professionelle Lösung zum sicheren Transport von sensiblen Daten und zur Erstellung von datenschutzkonformen Backups. Dieser Datenträger schützt zuverlässig sensible Informationen vor unbefugten Zugriffen falls er verloren, gestohlen oder anderweitig entwendet wird. www.digittrade.de
Chiffry Unterstützungssystem für sichere Einsatzkommunikation
Chiffry ist eine Kommunikationsplattform für Smartphone zum Unterstützen von Einsatzeinheiten durch verschlüsselte Text-, Sprach-, Bild-, Video- und Standort-Nachrichten sowie durch abhörsichere Telefonate und Telefon-Konferenzen. Sie ist im besonderen Maße an die Bedürfnisse von BOS angepasst und beinhaltet die Installation des Servers in die IT-Infrastruktur des Auftraggebers. www.chiffry.de

DSI Datensicherheit GmbH B 01

„Data Security for Harsh Environments“
DSI Datensicherheit GmbH entwickelt seit vielen Jahren hochsichere Kommunikationslösungen u.a. für den Space Bereich. Space Missionen stellen die höchsten Anforderungen sowohl an die Elektronik wie auch an die Sicherheit/Verschlüsselung der Kommunikation. Abgeleitet aus diesen Projekterfahrungen im technologischen Grenzbereich der Satelliten- und Drohnenprojekte realisiert DSI Datensicherheit innovative, hochsichere Kommunikationslösungen, auch für Projekte außerhalb des Aerospace Bereichs. Hochsichere Kommunikation und Abstrahlsicherheit (TEMPEST) gehören in vielen öffentlichen Projekten zusammen. DSI Datensicherheit GmbH verfügt über beide Kernkompetenzen im Unternehmen und realisiert Projekte von der Studie bis zur komplexen Elektronik- und Softwareentwicklung, inklusive Tempest Design und Tempest Tests im firmeneigenen Labor.
Kontakt: www.dsi-ds.de / info@dsi-ds.de

DXC Deutschland GmbH M 03

DXC Technology ist der weltweit führende unabhängige End-to-End IT-Dienstleister. Wir unterstützen unsere Kunden dabei, die vielfältigen Möglichkeiten der Technologie in messbare Erfolge zu verwandeln. Aus dem Zusammenschluss von CSC und der Enterprise Services Sparte von Hewlett Packard Enterprise geboren, sind wir ein 25-Mrd.-USD-Unternehmen, das für annähernd 6.000 privatwirtschaftliche und öffentliche Organisationen in 70 Ländern arbeitet. Dank unserer technologischen Unabhängigkeit, globalen Präsenz und unserem ausgedehnten Partnernetzwerk bieten wir leistungsstarke Next-Generation IT-Services und Lösungen. Wir sind darüber hinaus bekannt als eines der besten Corporate-Citizen-Unternehmen der Welt.

ECOS Technology GmbH F 29

Die ECOS Technology GmbH hat sich auf die Entwicklung und den Vertrieb von IT-Lösungen für den sicheren Fernzugriff auf zentrale Daten und Anwendungen zur Gewährleistung eines erhöhten Schutz vor Spionage und Cyberangriffen bei gleichzeitiger Senkung der Kosten und einer Vereinfachung der Administration, spezialisiert.
Die Lösungen **ECOS SECURE BOOT STICK** und **ECOS SECURE BOOT MODUL** ermöglichen einen hochsicheren Fernzugriff auf Citrix, VMware Horizon oder Webanwendungen der Bundeswehr, von jedem beliebigen PC oder Mac aus.
Unsere Themenschwerpunkte auf der AFCEA 2018:

- Hochsicherer Remote-Zugriff (z.B. auf VS-NfD-Daten)
- Stärkung der Bundeswehr als attraktiver Arbeitgeber
- Remote Access in Weiterbildung und Schulung
- Einbindung von Reservisten in die IT-Infrastruktur
- Ortsunabhängiger Zugriff auf SASPF oder LoNo

EGL Elektronik Vertrieb GmbH M 29

Ihr Partner für Abstrahlsicherheit.
Vielen Nutzern ist es nicht bekannt, dass bei einer Daten-Verarbeitung unweigerlich kompromittierende Abstrahlung direkt an der aktuell genutzten Hardware auftritt. Diese Abstrahlung kann zur Wiederherstellung der Daten genutzt werden und somit zum Verlust der Vertraulichkeit der zu schützenden geheimen Information führen. Mit geeigneten Abschirmmaßnahmen kann diese kompromittierende Abstrahlung auf ein nicht auswertbares Maß reduziert werden. Auf diese Schirmung und Entstörung hat sich die Firma EGL Elektronik Vertrieb GmbH spezialisiert. Gerne stehen wir Ihnen für Fragen zur Verfügung.
Tel.: 06051-71838 E-Mail: info@eglgmbh.de

ELE.SI.A S.p.A. S 02

Elesia S.p.A. wurde 1981 in Rom von einem Team erfahrener Managern mit langjähriger Erfahrung in der internationalen High-Tech-Branche gegründet.
Die Märkte sind:

- Missionskritische Verteidigung
- Home-Land Security (HLS)
- Verkehrstechnik
- Industrie-Technik

In nur wenigen Jahren gelang es Elesia eine führende Position im italienischen und internationalen Markt zu erreichen, die die Lieferung von Echtzeitsystemen und Embedded ComputerPlattformen als „Turnkey-Lösungen für anspruchsvollen Defence-, HLS- und Verkehrstechnik-Märkte zum Ziel hatte“.
Elesia’s Stammsitz liegt in Rom und verfügt über heimische und internationale Vertriebs-Repräsentanzen in Bologna, Turin, München, Madrid, Paris, Tel Aviv, Bangalore und Peking.
Lokaler Kontakt (Deutschland): Elesia S.p.A. – Branch Office Munich, www.elesia.it, Tel.+49-151-22631505, mailto: tomas.vonluepke@elesia.it

ELNO GmbH B 02

Die ELNO GmbH ist Mitglied der internationalen Unternehmensgruppe ELNO bestehend aus mittelständischen Firmen in Frankreich, Italien und Deutschland.
Firmensitz ist Grünstadt in der Pfalz. Wehrtechnischer Umsatzanteil 90%.
ELNO ist Hersteller elektronischer Kommunikationsgeräte und -systeme und verfügt über:

- eine Entwicklungsabteilung mit moderner CAD/CAE Ausstattung
- langjährige Erfahrung in der Herstellung professioneller Elektronikprodukte
- langjährige Erfahrung als Lieferant für den öffentlichen Auftraggeber
- eigene Abteilung für Kundenschulungen
- ein Qualitäts-Management System ISO 9001:2000

Produkte:

- Funktechnik: Handfunksprechgeräte, tragbare Funkgeräte, Fahrzeugfunkanlagen, professionelle und militärische Antennen
- Kommunikationstechnik: Neu: IP-basierende Intercom-Systeme für Ketten und Radfahrzeuge IP-basierende Feldtelefone auch für weite Entfernungen
- Audiotechnik: Handapparate, Kopfsprechsätze, Audiohelme für Piloten- und Fahrzeugbesatzungen

Kontakt: Kirchheimer Str. 49D – 67269 Grünstadt – Tel.: +49 6359 9463 643 – Fax +49 6359 9439 817 – s.eulenhofer@elno.fr – www.elno.fr

ESG Elektroniksystem- und Logistik-GmbH M 04

Die ESG ist eines der führenden System- und Softwarehäuser Deutschlands in den Bereichen Sicherheit und Verteidigung. Unsere langjährige Partnerschaft mit unseren Kunden aus Streitkräften, Behörden und Industrie zeichnet sich durch eine besondere Leidenschaft für Technik, Innovationskraft und -fähigkeit aus. Wir präsentieren maßgeschneiderte verlegefähige und mobile Lösungen im Bereich Führungs- und Gefechtsstandsysteme, zur Verbesserung der Fähigkeiten der Bundeswehr in aktuellen und zukünftigen Einsätzen. Mit unseren Logistic Services begleiten wir Sie als Prozesspartner während des gesamten Lebenszyklus.
Unter der Marke CYOSS präsentieren wir unser Cyber/IT-Serviceportfolio sowie die Möglichkeiten für hocheffizientes Cyber Defence Training und Testing im ersten Cyber Simulation & Training Center Deutschlands.
Kontakt: ESG Elektroniksystem- und Logistik-GmbH, Livry-Gargan-Str. 6, 82256 Fürstenfeldbruck, Tel. 089/9216-0, E-Mail: defenceandsecurity@esg.de, www.esg.de

Esri Deutschland GmbH M 26

Esri ist Anbieter der ArcGIS Plattform für alle Sicherheitsorgane. ArcGIS strukturiert Informationen über Raumbezug und visualisiert Ergebnisse und Zusammenhänge in 2D, 3D und 4D. Damit vernetzt die Technologie alle Beteiligten – vom Analysten bis zum Entscheider – mit einem einheitlichen, räumlichen Verständnis zur Operationsführung.
Kontakt: Esri Deutschland GmbH, Niederlassung Bonn, Rheinallee 24, 53173 Bonn, Tel.: +49 89 207 005 1720, E-Mail: info@bonn.esri.de, www.esri.de

FFG Flensburger Fahrzeugbau Gesellschaft mbH S 02

FFG – das junge Systemhaus
In den letzten fünfzig Jahren hat sich die FFG vom Instandsetzer für die Bundeswehr und Armeen befreundeter Nationen über die Upgrade-Spezialisierung konsequent zum Fahrzeughersteller und Systemanbieter weiterentwickelt. Diese Aktivitäten führten u.a. zu umfangreichen Weiterentwicklungen, wie z.B. für Fahrzeuge der Leopard 1-Familie, M113 und der aktuellen Entwicklung der NDV Wiesel 1. Innerhalb der letzten Jahre investierte die FFG in Eigenentwicklungen und ist seitdem mit eigenen Fahrzeugsystemen am Markt vertreten.
Die hochgeschützten Fahrzeugplattformen G5 und WiSENT 2, bieten dabei dem Kunden mit ihrer Modularität eine Vielzahl von Einsatzmöglichkeiten und bereiten den Weg der FFG, sich als Systemhaus auf dem Weltmarkt zu etablieren.

Forcepoint Deutschland GmbH — ME 17

Forcepoint transformiert die Cybersicherheit, indem es sich auf das konzentriert, was am wichtigsten ist: die Absicht von Menschen zu verstehen, wenn sie mit kritischen Daten und geistigem Eigentum interagieren, wo auch immer es sich befindet. Unsere kompromisslosen Systeme ermöglichen es Unternehmen, ihren Mitarbeitern einen ungehinderten Zugang zu vertraulichen Daten zu ermöglichen, während sie geistiges Eigentum schützen und die Einhaltung von Compliance Richtlinien vereinfachen.

Kontakt: Name: Patricia Buchholz, Tel.: +49 89 244105800,
E-Mail: ceur-info@forcepoint.com

Fraunhofer FKIE — M 25

Das Fraunhofer FKIE erforscht und entwickelt anwendungsorientierte Technologien für die vernetzte Operationsführung. Unter seinem Leitmotiv „Vom Einsatz her gedacht“ agiert Fraunhofer FKIE als verlässlicher Partner. Bei der strategischen Forschungsarbeit für die Bundeswehr geht es u.a. um die Themen Führung, Aufklärung, Unterstützung und Schutz.

Die Forschung ist dabei auf die Verbesserung der Leistungsfähigkeit cyber-physischer Systeme hinsichtlich Bedienbarkeit, Datensicherheit, Interoperabilität und Vernetzung sowie der Auswertung verfügbarer Informationen mit hoher Präzision und Zuverlässigkeit ausgerichtet. Exemplarisch werden auf der AFCEA-Fachausstellung zwei Projekte aus den Abteilungen „Informationstechnik für Führungssysteme“ und „Sensordaten- und Informationsfusion“ präsentiert.

Kontakt: kontakt@fkie.fraunhofer.de, www.fkie.fraunhofer.de

Fraunhofer IOSB — B 12 + S 02

Beratung und Technologie für die Verteidigung: In seinem größten Geschäftsfeld betreibt das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB grundlagenorientierte wehrtechnische Forschung und entwickelt daraus Machbarkeitsstudien und Verfahren. Es bewertet Trends und Technologien, prüft und entwickelt Demonstratoren, unterstützt die Industrie und stellt innovative Ausrüstung her.

Kernkompetenzen sind die Erzeugung von Bildern und verwandten Sensorsignalen, ihre algorithmische Verarbeitung und Auswertung sowie die Nutzbarmachung in benutzerfreundlichen Systemen. Dabei konzentrieren wir uns auf die Bereiche Aufklärung, Navigation, Simulation, Satellitentechnik, land-, luft- und seegestützte Plattformen, Zielannäherung, Wirkung und Schutz, die Ausrüstung des Soldaten sowie Informationstechnologie.

Auf der AFCEA 2018 zeigen wir auf dem griffity defense Gemeinschaftsstand u.a. Implementierungen des Digitalen Lagetischs und Auswerte-/Aufklärungs-/Überwachungssystemen (ABUL, AMFIS) in zwei Rüstsatzmodulen.

www.iosb.fraunhofer.de/verteidigung

FREQUENTIS Deutschland GmbH — B 09

Die Lösungen von Frequentis Defence greifen auf 70 Jahre Erfahrung im Bereich von ATM Lösungen zurück. 50 Jahre davon widmen sich direkt der militärischen Flugsicherung. Diese industrieübergreifende Erfahrung ermöglicht es, Lösungen zu entwickeln, die sich auf den Bereich Luft und See spezialisieren. Der Geschäftsbereich Defence baut auf diesem Wissen auf und entwickelt Lösungen für Kontrollzentralen in den Bereichen Land, See und Luft, um verbesserte Funktionalitäten zur Verfügung zu stellen, die missionskritische Kommunikation der Zukunft ermöglichen. Im Laufe der Zeit bietet die Ergänzung von verschlüsselten mobilen Übertragungen für Sprache und Daten ebenso wie „Situational Awareness“, eine missionskritische Unterstützung für die Anforderungen im Bereich der Luftverteidigung.

Frequentis Comsoft — B 09

Comsoft Solutions heißt nun Frequentis Comsoft. Als Anbieter individueller Systeme und Dienstleistungen beliefern wir zivile und militärische Flugsicherungsbehörden weltweit. Unsere Lösungen sind in Flugkontrollzentren und Flughäfen in mehr als 80 Ländern implementiert. Über 200 Mitarbeiter engagieren sich täglich für unsere anspruchsvollen Kunden, zu denen u.a. die Deutsche Bundeswehr und Armasuisse gehören. Zukunftsweisende Technologien, eine enge Zusammenarbeit mit dem Kunden auch nach Projektabschluss sowie die Implementierung und Einhaltung internationaler Standards sind die Eckpfeiler für unsere Arbeit in einem sicherheitsrelevanten Umfeld. Die Frequentis Comsoft GmbH ist Teil der global sehr erfolgreich agierenden Frequentis Firmengruppe.

GAF AG — ME 18

Die GAF AG ist ein international agierendes Unternehmen mit führenden Kompetenzen und Expertise auf den Gebieten der Fernerkundung, Geodaten und Informationssystemen. Seit der Gründung 1985 in München wurden mehr als 1000 Projekte in Deutschland und über 100 Ländern weltweit erfolgreich durchgeführt. Ausgehend vom Empfang und Vertrieb indischer Erdbeobachtungs- und vieler weiterer Geodaten, nimmt das Unternehmen aufgrund des herausragenden Know-Hows auch eine internationale Spitzenposition in den Bereichen Softwareentwicklung, GIS- und Datenbankanwendungen, Datenveredlung sowie im Geo-Consulting ein. Zurzeit beschäftigt die GAF über 200 Mitarbeiter und hat eine Vielzahl an erfolgreich abgeschlossenen und laufenden Geoinformationsprojekten aus den Bereichen u.a. Sicherheit, Infrastruktur und Landmanagement aufzuweisen.

GBS TEMPEST & Service GmbH — S 03

Die GBS GmbH, mit Sitz in Diepholz, betreibt ein vom BSI anerkanntes Abstrahlprüflabor. Für das Geschäftsfeld TEMPEST verfügt die GBS GmbH über zwei firmeneigene TEMPEST-Labore. Neben der Berechtigung zur Durchführung von Zonenkurzmessungen ist die GBS GmbH auch ein vom BSI anerkanntes Abstrahlprüflabor für Zulassungsmessungen nach SDIP 27 Level A, Level B und Level C (International) und dem Zonenmodell (National).

Kontakt: GBS TEMPEST & Service GmbH, von-Braun-Straße 6, D-49356 Diepholz,
Tel.: +49 5441 9758-100, Fax: +49 5441 9758-129,
Homepage: http://www.gbs-tempest.de, E-Mail: info@gbs-tempest.de

Gebr. Friedrich Industrie- und Elektrotechnik GmbH — S 04

Die Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) ist seit vielen Jahren Rahmenvertragspartner des BAAINBw. Ganz egal ob es sich um die Einrüstung von Kabinen und geschützten Fahrzeugen oder um Instandsetzungsmaßnahmen handelt. In den Bereichen Kommunikationstechnik, IT oder Maschinenbau kämpft das Team der Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) an vorderster Front. GFE stellt sich den Forderungen der Bundeswehr und liefert einsatzfertige Systeme. Selbstverständlich werden dabei die strengen Maßstäbe der VG-Normen erfüllt. Auch ein weltweiter Einsatz ist für GFE selbstverständlich: Überall, wo Einheiten technische Hilfe benötigen, ist GFE vor Ort: auf Zypern genauso wie am Horn von Afrika. Weitere Informationen: www.gfelektro.de

genua gmbh — M 19

Umfassende Lösung für VS-Datenkommunikation

Das deutsche IT-Sicherheitsunternehmen genua bietet eine umfassende Komplettlösung für die VS-Datenkommunikation. Mobile Anwender, Home Offices und verteilte Standorte können Sie mit der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-NfD zugelassenen Kommunikationslösung einfach und sicher anbinden. Der Datenaustausch erfolgt über ein Virtual Private Network (VPN) via Internet oder WAN, die Identifizierung der Anwender komfortabel per Smartcard oder elektronischem Dienstausweis. Im Backend sorgen VPN- und Firewall-Systeme für hochwertige Sicherheit. Die Lösung kann einfach auf bestehende Infrastrukturen aufgesetzt werden.

Darüber hinaus bieten wir IT-Sicherheitslösungen für diese Aufgaben:

- Absicherung und Kontrolle hochsensibler Netzwerk-Schnittstellen
- Fernwartungs-Zugriffe in VS-NfD-Netze

Kontakt: genua gmbh, Domagkstraße 7, 85551 Kirchheim bei München
Tel.: +49 89 991950-0, www.genua.de

griffity defense GmbH S 02

griffity defense steht, neben Aktivitäten im Bereich der Geschäftsentwicklung und Marketing-Services, für die Beratung von Unternehmen und dem öAG bei der Lösung komplexer Herausforderungen.
Unser Fokus liegt auf klaren, umfassenden, zukunftssicheren Strategien und integrierten technischen Lösungen um für die unterschiedlichen Einsatzszenarien bestmögliche Werkzeuge und Infrastruktur bereitzustellen.
Unter dem Motto „Digitalisierung der Landstreitkräfte“, zeigen wir auf der AFCEA 2018 mit unseren Partnern AD2V, Cellebrite, Cubic, ELESIA, FFG, Fraunhofer IOSB, Harris, Saab, SFC Energy und VITES beispielhaft Module für:

- Aufklärung und Auswertung (leistungsstarke Aufklärungs- und Auswertesysteme auf Basis eines luftverlegefähigen Moduls)
- Führung (Führungsfahrzeug mit Arbeitsplätzen für S2-Nachrichtengewinnung und Aufklärung, S3-Führung, S4-Logistik und S6-Kommunikation)
- abgesessene Einsatzkräfte (als vernetztes Teilsystem)

Kontakt: griffity defense GmbH, Hanns-Schwindt-Str. 8, 81829 München
Tel.: +49 (0) 89-43 66 92-0 + +49 (0) 89-43 66 92-66, info@griffity-defense.de, www.griffity-defense.de

Hagenuk Marinekommunikation GmbH S 07

Die Hagenuk Marinekommunikation GmbH (HMK), eine Tochtergesellschaft der ATLAS ELEKTRONIK. HMK ist einer der führenden Hersteller von zertifizierten, schlüsselfertigen internen/externen Kommunikationssystemen für Marineschiffe und HF-Sende-/ Empfangsanlagen für Landstationen. Auf allen Schiffen der Deutschen Marine sind Systeme/Geräte der HMK im Einsatz. Weltweit werden mehr als 560 Systeme von 29 Marinen genutzt.
Zum Portfolio der HMK gehören:

- HF-Sender / Transceiver der 3000er und 3003er Serie bis 10 kW (1,5 – 30 MHz)
- VLF/HF-Empfänger (10 kHz – 30 MHz)
- HF-Verstärker mit Antennenanpassgeräten für das Programm SVFuA
- HF-Breitbandsysteme
- Digitale Audio- und Datenverteilsysteme
- Message Handling und Steuerungssysteme
- Weitere Subsysteme der internen/externen Kommunikation

Kontakt: Hagenuk Marinekommunikation GmbH, 24220 Flintbek
Tel.: +49 (0) 4347-714-0, www.hmk.atlas-elektronik.com,
E-Mail: info@hmk.atlas-elektronik.com

Haivision Network Video F 28

Haivision bietet End-to-End Lösungen für die schnelle und sichere Übertragung von Video zusammen mit zeitkritischen Metadaten (KLV oder Sensorik-Daten) über verschiedene IP-Netzwerke oder Satellitenverbindungen. Haivision Video Encoder/Decoder Produkte erfüllen NATO und MISB Standards (STANAG 4609) und werden bereits weltweit im Bereich C4ISR Ultra Low Latency Videoübertragung auf unterschiedlichsten Plattformen und Programmen erfolgreich eingesetzt.
Haivision ist ein globales Unternehmen mit Hauptsitz in Montreal / Kanada und in Chicago, sowie weiteren regionalen Niederlassungen Europa/Deutschland und in Asien. Haivision Produkte sind ITAR free und werden weltweit über zertifizierte Distributoren, Reseller und Systemintegratoren vertrieben.
Weitere Informationen finden Sie unter: www.haivision.eu / www.haivision.com

Harris Geospatial Solutions S 02

Der Harris-Konzern liefert integrierte Lösungen für Verteidigung und Sicherheit weltweit und besteht aus den drei Geschäftsbereichen

Space and Intelligence Systems	Payload und Sensoren für Satelliten und Luftfahrzeuge, militärisches GPS, Erd- und Wetterbeobachtung, Prozessierung und Analyse von Fernerkundungs- und Geodaten,
Communication Systems	Netzwerke, Funk- und Satellitensysteme für Sprachkommunikation sowie Nachtsichtsysteme,
Electronic Systems	Elektronische Systeme, Radar- und Sonarsysteme, Flugsicherung, Kompositstrukturen für Luftfahrzeuge.

Informieren Sie sich auf unserem diesjährigen Stand auch speziell über

- Jagwire
- ENVI & SARscape
- GSF & Machine Learning
- Geiger-mode LiDAR

Kontakt: Harris Geospatial Solutions GmbH, Talhofstraße 32a, D-82205 Gilching, Tel.: +49 (0)8105 378 0, www.harrisgeospatial.com

Hexagon Safety & Infrastructure – c/o HxGN Safety & Infrastructure GmbH F 15

Als einer der weltweit führenden Anbieter, bewährter Innovator und zuverlässiger Geschäftspartner in Sachen GIS- und Geo-Lösungen konzentriert sich Hexagon Safety & Infrastructure (vormals Intergraph) auf die Branchen Verteidigung und Nachrichtenwesen sowie Sicherheit, Rettung und Katastropenschutz. Unsere Lösungen bereiten umfangreiche, komplexe Datenmengen in aussagekräftigen, graphischen Darstellungen auf. So sind zeit- und situationsgerechte Entscheidungen zum Schutz von Menschen und Infrastrukturen gewährleistet. Die komplette digitale militärische Datenverarbeitung ist abgedeckt: Missionsplanung, Datenmanagement, Datenspeicherung, Datenprozessierung, Informationsverteilung und -auswertung.
Kontakt: Hexagon Safety & Infrastructure – c/o HxGN Safety & Infrastructure GmbH, Niederlassung Bonn, Koblenzer Str. 112, 53177 Bonn, Tel.: +49 (0)228 3915 0, www.hexagonsafetyinfrastructure.com

Hitachi Vantara GmbH M 21

Hitachi Vantara unterstützt Unternehmen und Behörden weltweit, ihre datenorientierten Innovationen im Zeitalter der digitalen Revolution voranzutreiben. Nutzen Sie unsere umfangreiche Expertise aus über 100 Jahren OT und mehr als 58 Jahren IT, um den vollen Wert Ihrer Daten auszuschöpfen und auch unser öffentliches Leben sicherer und angenehmer zu machen. Unsere Lösungen adressieren sämtliche Aspekte eines ganzheitlichen Data Management: eine integrierte IT-Infrastruktur mit hochverfügbarer Speichertechnologie, Data Analytics unter anderem zur intelligenten Videoüberwachung, Big Data, IoT, AI und Predictive Maintenance, Object Storage und Data Governance. Dies macht uns zum idealen Partner für den öffentlichen Bereich. Besuchen Sie uns an unserem Stand M21.

IABG mbH M 27

Die IABG arbeitet an Lösungen für eine sichere und zuverlässige Kommunikation und IT-Unterstützung für Streitkräfte und BOS. Hierbei betrachten wir die gesamte Prozesskette und den Lebenszyklus von ITK-Systemen. Wir beschäftigen uns u.a. mit Ausbildungs- und Trainingskonzepten zum Thema Cyber Security, Risikoanalysen sowie Detection & Response Mechanismen für Cyberangriffe. Mit der IABG Cyber Range stellen wir eine Testplattform für die virtualisierte Abbildung der Umgebung der Bundeswehr bereit, in der wir auch komplexe Cyberszenare simulieren und die Widerstandsfähigkeit von ITK-Systemen beurteilen können. Zudem unterstützen wir bei der Erstellung und Weiterentwicklung von IT-Sicherheitskonzepten auf Basis der neuen zentralen Dienstvorschrift A-960/1.

IBM Deutschland GmbH M 17

IBM ist einer der weltweit größten Anbieter von Informationstechnologie. Das Lösungsportfolio reicht vom Quantencomputer über Software und Beratungsleistungen bis hin zur Erarbeitung komplexer Anwendungslösungen sowie Outsourcing.
Mit hohen Investitionen in Forschung und Entwicklung adressiert IBM die Wachstumsinitiativen Business Analytics, Cloud Computing, Mobile Enterprise, Social Computing und Security.
Der kognitiven Erschließung komplexer und großer Datenmengen trägt IBM Rechnung durch den neuen Geschäftsbereich Watson IoT, der gemeinsam mit dem ersten europäische Watson Innovation Center in München seine Zentrale hat.
Kontakt: IBM Deutschland GmbH, Godesberger Allee 127, D-53175 Bonn
Klaus Lilge, klaus_lilge@de.ibm.com, Mobile: +49-175-5813842

iesy GmbH & Co. KG F 42

Individuelle Lösungen für Verteidigung und Sicherheit

Marktführende Unternehmen aus den Bereichen Avionics & Defence setzen auf iesy, wenn es um die Entwicklung und Anpassung von Elektronik oder Mechanik für raue Umgebungen geht. iesy ist ein Systemhaus für Embedded Computing.

Mit Leidenschaft für Technik und einem eingespielten Team in den Bereichen Soft- und Hardwareentwicklung, Materialbeschaffung, Fertigung und Geräteprüfung sind wir seit 1966 ein idealer OEM- und Outsourcing-Partner zur Entwicklung, Serienfertigung und Pflege individueller Elektronikprodukte. Als Full-Service Dienstleister für Embedded Computing begleiten wir Sie beim gesamten Entwicklungsprozess von Ihrer Idee bis zum fertigen Produkt.

Kontakt: iesy GmbH & Co. KG, Darmcher Grund 22, 58540 Meinerzhagen
Tel.: +49 (2354) 70655 0 | E: sales@iesy.com, www.iesy.com

Indra Sistemas S.A. S 09

Indra Sistemas S.A. ist der führende Spanische Elektronik Konzern, der sich in den letzten 30 Jahren zu einer multinationalen welt-weit operierenden Verteidigungs- und Sicherheitstechnologie-Firma entwickelt hat. Im Sicherheits- und Verteidigungsbereich unterstütz Indra u.a. Anwendungen in den Bereichen Grenzschutz, Schutz kritischer Infrastrukturen, Krisenmanagement, Interoperabilität verschiedener Einsatzkräfte auf allen Ebenen. Die wichtigsten Technologien in diesem Bereich sind Simulationsumgebungen, Radarsysteme, Wissensmanagement und Flex IT/Cloud Lösungen.

Kontakt: Thomas Mattick, Programm Manager Bundeswehr, Bahnhofplatz 1, 88045 Friedrichshafen, Tel.: +49(0)7541/282-0, www.avitech.aero

INFODAS GmbH M 20

Die **INFODAS** ist seit 1974 als unabhängiges und herstellerneutrales Software- und Beratungsunternehmen ein verlässlicher Partner der Bundeswehr.

Schwerpunktthemen sind:

- SDoT Security Gateway, bidirektionale Netzkopplung unterschiedlicher Sicherheitsdomänen mit BSI Zulassung GEHEIM
- SDoT Diode, hochsichere High-Speed-Datenübertragung mit BSI Zulassung GEHEIM
- SDoT Labelling Service, Kennzeichnung und Auswertung von Security Labeln
- SDoT SIS & SD, elektronische VS-Registratur zur Behandlung von digitalen Verschlusssachen für Informationsverarbeitende Systeme
- SAVe, IT-Sicherheitsdatenbank mit integrierten Sicherheitsvorgaben ZDv A-960/1
- PATCH.works, Patch-Managementsystem für geschlossene IT-Systeme der Bw
- Informationssicherheitsberatung und Erstellung von IT-Sicherheitskonzepten
- Anforderungs-, Konfigurations-, Projekt- und Qualitätsmanagement
- Architekturentwürfe und -umsetzung sowie technische Studien im IT-Umfeld
- Betriebskonzepterstellung und -überwachung

www.infodas.de – vertrieb@infodas.de

interface projects GmbH F 43

Die interface projects GmbH wurde 1993 in Dresden gegründet und ist einer der führenden deutschen Anbieter für intelligente Informationsmanagement-Lösungen, basierend auf dem eigenen Produkt intergator. Bei intergator handelt es sich um eine auf maschinellen Lernverfahren basierende systemübergreifende Suchmaschine und Wissensmanagement-Plattform.

Die interface:projects unterstützt seit vielen Jahren Maßnahmen auf dem Weg zu effizienterem Informationsmanagement und eGovernment durch die Realisierung von Enterprise Search- und Wissensmanagement-Projekten auf Bundes-, Landes- und kommunaler Ebene.

intergator ist u.a. im Einsatz bei:

- Bundesministerium des Innern, Deutsches Patent- und Markenamt, LKA Niedersachsen, Planungsamt der Bundeswehr
- Abgeordnetenhaus Berlin, Landtag von Baden-Württemberg, Landtag Sachsen-Anhalt, Thüringer Landtag, Sächsischer Landtag
- Stadt Chemnitz, Dresden, Erfurt, Leipzig

IT-Standort Bonn F 04

Bonn gehört zu den wichtigsten IT-Standorten in Europa. Die Europäische Kommission hat in einer europaweiten Studie die wichtigsten Zentren der IT-Wirtschaft analysieren lassen (European Poles of ICT Excellence EIPE). Bonn liegt im europäischen Standortwettbewerb auf Rang 12 von 1300 Regionen in Europa. Besondere Stärken sind hier die lokale Wissenschaft und die bestehenden Wirtschaftsunternehmen am Standort Bonn. Die Schwerpunktsetzung liegt in den Bereichen Geoinformatik, IT für Gesundheit und Ernährung, sowie im Bereich der Cybersicherheit

Kontakt: Thomas Poggenpohl, Amt für Wirtschaftförderung, Liegenschaften und Tourismus
Besucher: Loggia am Stadthaus, Thomas-Mann-Straße 4, 53111 Bonn
Postanschrift: Bundesstadt Bonn, 53103 Bonn, Tel.: +49 (0)228 / 77 57 88,
Fax: +49 (0)228 / 77 20 34, E-Mail: thomas.poggenpohl@bonn.de

itWatch GmbH F 26 + ME 13

itWatch ist im zersplitterten Markt der IT-Sicherheitshersteller in Deutschland eines der wenigen vollständig unabhängigen, inhabergeführten Unternehmen. Erste Produkte der itWatch wurden 1997 entwickelt und in 2000 patentiert. Der Fokus liegt auf dem Schutz gegen Datendiebstahl über alle möglichen Kanäle, bis zum Ausdruck (Data Loss Prevention), technischer Vertrauensketten von der Tatstatur bis zu den Daten, deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endgeräte-Sicherheit (Endpoint Security), sowie Mobile Security und Verschlüsselung. Integrierte Lösungen für Datenschleusen mit Datenwäsche und PrivateDataRoom bringen hohe Kundenmehrwerte. Die Lösungen der itWatch Enterprise Security Suite (itWESS) werden ohne Zukauf im Hause der itWatch hergestellt.

JK Defence & Security Products GmbH F 41

JK DEFENCE & SECURITY PRODUCTS GMBH steht seit über 25 Jahren für Qualität und Zuverlässigkeit im Bundeswehrgeschäft.

Zusammen mit **HARRIS CORPORATION / COMMUNICATION SYSTEMS**, dem größten Hersteller von militärischen Funkgeräten, bieten wir die komplette Bandbreite von portablen und stationären Funkgeräten an. Ob als Hand-Held oder Man-Pack, modular oder fest eingebaut in gepanzerten Land- oder Wasser-Fahrzeugen:

Wir haben immer eine Lösung für Kommunikation und Aufklärung. Zum Beispiel das Software Defined Radio PRC-117/G, welches bestehende und zukünftige Wellenformen in einem Frequenzbereich von 30MHz bis 2GHz abdecken kann.

Kontakt: JK Defence & Security Products GmbH / Industriering Ost 74 / 47906 Kempen / www.jkdefence.de / info@jkdefence.de

Kommando Cyber- und Informationsraum der Bundeswehr ME 22

Im April 2017 wurde das Kommando Cyber- und Informationsraum (KdoCIR) in Bonn in Dienst gestellt. Mit dem neuen Organisationsbereich stellt sich die Bundeswehr den immer weiter ansteigenden Gefahren aus dem Cyber- und Informationsraum. Bereits vorhandene Expertise wurde dafür unter dem KdoCIR gebündelt. Dazu gehören das Kommando Strategische Aufklärung inklusive des Zentrums für Operative Kommunikation der Bundeswehr, das Kommando Informationstechnik der Bundeswehr sowie das Zentrum für Geoinformationswesen der Bundeswehr. In Zukunft wird weitere Expertise aufgebaut, um die Fähigkeiten „Cyber-Operationen“, „Cyber-Sicherheit“ und „Softwarekompetenz“ zu stärken. Im Jahr 2021 wird der Organisationsbereich CIR rund 15.000 militärische und zivile Dienstposten umfassen.

K&K Medienverlag-Hardthöhe GmbH ME 01

Der Hardthöhenkurier ist ein periodisch erscheinendes Magazin, das sich seit 34 Jahren mit aktueller Berichterstattung an Soldaten der Bundeswehr wendet und sich als Bindeglied zwischen der Bundeswehr, der wehrtechnischen Industrie und der Wirtschaft versteht. Der Hardthöhenkurier informiert über sicherheitspolitische Rahmenbedingungen, Einsätze der Bundeswehr, aktuelle Vorhaben der Streitkräfte sowie Neuerungen in der Wehrtechnik und der Rüstungsindustrie. Das Fachmagazin ist eine in Deutschland und in den europäischen Nachbarländern anerkannte Informationsquelle für Streitkräfte und Wehrtechnik.

Kontakt: Verlagsdirektion Bonn • Postanschrift: Borsigallee 12, 53125 Bonn, Tel.: +49 (0)228 / 25900-344 • Telefax: +49 (0)228 / 25900-342, E-Mail: redaktion@hardthoehenkurier.de • Internet: www.hardthoehenkurier.de

Lachen helfen ME 14

Im ehemaligen Jugoslawien beschlossen Bundeswehrsoldaten Mitte der 90er Jahre, sich neben ihren dienstlichen Aufgaben auch privat für humanitäre Projekte zugunsten von Kindern zu engagieren. Um den traumatisierten, verwundeten oder elternlosen Kindern dauerhaft, schnell und unbürokratisch zu helfen, gründeten sie 1998 einen gemeinnützigen Verein.

Die gute Zusammenarbeit mit der Polizei führte 2009 zu dem Entschluss, sie in den Verein zu integrieren. Seitdem ist Lachen Helfen e.V. die **„Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten“**.

Seit dem Jahre 2001 sind wir nach wie vor in Afghanistan und auf dem Balkan tätig. Momentan werden jedoch insbesondere im **Irak**, in **Mali**, im **Südsudan**, in **Somalia**, in der **Ukraine** und seit einiger Zeit auch in **Syrien** Hilfsprojekte erkundet.

Leonardo, vertreten durch SELEX ES GmbH B 04

Leonardo is a global high-tech player in the Aerospace, Defence and Security sector. The Company, with headquarters in Italy, has over 45,600 employees and is present with 180 sites across the globe. Leonardo has a consolidated industrial presence in Europe and US markets and an important network of strategic partnerships in the main high potential markets worldwide.

The Company operates through seven Divisions (Helicopters, Aircraft, Aerostructures, Airborne & Space Systems, Land & Naval Defence Electronics, Defence Systems, Security & Information Systems). Each year, Leonardo invests 11% of its revenues in Research and Development.

Kontakt: www.leonardocompany.com, Tel.: +49 (0)2137-782-328

Luciad S 05

Luciad ist Anbieter von Softwarelösungen zur räumlichen Lagebilddarstellung von Geoinformationen für Anwendungen in missionskritischen Systemen. Luciad Softwarekomponenten bieten eine effiziente und visuelle Datenanalyse, die es ermöglicht, Echtzeit-Lagebilder zu erstellen und damit die Grundlage für Geoinformationssysteme der nächsten Generation zu schaffen. Von militärisch genutzten Command and Control Systemen bis hin zur Schaffung von digitaler Infrastruktur für Smart Cities helfen Luciad Softwarekomponenten eine intuitive Lagebilddarstellung zu generieren. Weltweit verlassen sich Kunden auf leistungsstarke Visualisierungslösungen aus dem Hause Luciad. Unser Motto lautet: „Connect, visualize, analyze, act“.

Materna GmbH F 14

Materna ist ein Full-Service-Dienstleister im Premium-Segment und realisiert seit fast vier Jahrzehnten sehr erfolgreich ITK-Projekte für ihre Kunden. Weltweit arbeiten mehr als 1.900 Mitarbeiter für das Familienunternehmen. Wir betreuen Behörden in allen Phasen der Wertschöpfungskette: von der Beratung, Konzeption, Realisierung über die Einführung bis zum Betrieb mithilfe standardisierter und skalierbarer Lösungen. Das Leistungsspektrum umfasst die Konzeption und Einführung von Internet- und Intranet-Lösungen sowie von Kollaboration und Wissens-Management, die Optimierung von Verwaltungsabläufen, die Einführung von IT-Service-Management sowie die Entwicklung und Integration ressortspezifischer Fachverfahren.

Media Broadcast Satellite GmbH F 27

Media Broadcast Satellite bietet weltweit Kommunikationslösungen für satellitengestützte und terrestrische Anwendungen. Zu unseren Kunden zählen Streitkräfte und Behörden verschiedener Nationen sowie die Industrie. Neben standardisierten Datenverbindungen können ebenso vollständig integrierte / gemanagte Leistungen erbracht werden. Wir agieren als unabhängiger Integrator mit eigener Infrastruktur, Satellitensegment und dedizierten Teams, die den Kunden unterstützen, unabhängig von der Sicherheitslage vor Ort. Ein Maximum an Sicherheit und Stabilität erzielen wir durch unseren eigenen Teleport in Deutschland sowie einem rund um die Uhr bemanntem zweisprachigen Network Operation Center. Unser Produktportfolio deckt alle Bedarfe über die gesamte Servicelaufzeit: der Aufplanung, der Bereitstellung, des Betriebes, der Verlegung sowie dem Rückbau. www.mb-satellite.com

Mellanox Technologies M 13

Mellanox Technologies ist der führende Hersteller von Hochgeschwindigkeit-Interconnect Lösungen mit höchster Bandbreite und niedrigster Latenz. Der israelische Halbleiterhersteller mit Sitz in Yokneam, Nähe Haifa produziert Silizium, Netzwerkadapter, Kabel und Switch-Systeme für den Einsatz in anspruchsvollen Kommunikationsumgebungen.

Als Marktführer in der Vernetzung von Supercomputern und Höchstleistungsrechenzentren auf Basis des Infiniband-Netzwerkprotokolls, bietet Mellanox eine breite Palette an Komponenten für den Einsatz in modernen Cloud-Infrastrukturen an. Die Ethernet-Technologien von Mellanox ermöglichen den effizienten Betrieb virtualisierter Server- und Storagelösungen und bilden die Basis moderner Hyper-Converged-Technologien von Microsoft, VMware und verschiedener Open Source-Standards.

Kontakt: Michael Frings, Senior Regional Manager, E-Mail: michaelfr@mellanox.com, Mobil +49 175 2430000

Microsoft Deutschland GmbH F 09

Die Leistungsfähigkeit moderner Streitkräfte hängt von erfolgreicher Interoperabilität ab. Auf technischer Seite steht dabei die nahtlose Zusammenarbeit von IT-Systemen und Geräten, wie Hololens oder Surface, im Fokus. Insbesondere wenn verschiedene Einheiten oder internationale Koalitionen Informationen austauschen müssen, ohne die Informationssicherheit zu gefährden. Microsoft unterstützt Sie mit einer hochintegrativen Plattform bei diesen Herausforderungen. Mit SharePoint für Zusammenarbeit und Skype for Business für die vereinheitlichte Echtzeitkommunikation wird eine flexible, zeitgemäße Zusammenarbeit ermöglicht. Mit der Microsoft Cloud für Deutschland bietet Microsoft diese Dienste auch aus Rechenzentren in Deutschland an – mit T-Systems als Datentreuhänder für Ihre Daten.

Mittler Report Verlag ME 03

Der Mittler Report Verlag gilt als führender Fachverlag für Sicherheitspolitik, Streitkräfte, Wehrtechnik, Rüstung, IT und Logistik im deutschsprachigen Raum. Das Portfolio umfasst Zeitschriften, Broschüren, Informationsdienste und Fachtagungen. Dazu zählen die in vertraglich geregelter Zusammenarbeit mit dem Bundesministerium der Verteidigung herausgegebene Monatszeitschrift „Europäische Sicherheit & Technik“, die neunmal jährlich erscheinende internationale Fachzeitschrift „European Security and Defence“, die Fachzeitschrift „MarineForum“, die Broschürenreihen „Wehrtechnischer Report“ und „Sicherheitstechnischer Report“ sowie die Online-Newsletter „ESD Spotlight“ und „Wehrwirtschaft“. Daneben gelten die jährlich stattfindende Sicherheitspolitische und Wehrtechnische Tagung in Bonn sowie die NATO LCM Conference in Brüssel als etablierte Foren für den Informationsaustausch unter Experten und Entscheidungsträgern.

www.mittler-report.de

Mönch Verlagsgesellschaft mbH — ME 02

MÖNCH ist einer der weltweit führenden Zeitschriftenverlage in den Bereichen Verteidigung und Sicherheit. Die Zeitschriften erscheinen auf deutsch, englisch, arabisch, spanisch und auf italienisch und sind sowohl in Druckform wie auch Digital erhältlich. Zusätzlich bietet MÖNCH unter www.monch.com den **M**önch **O**nline **N**ews **S**ervice (**MONS**) mit den aktuellsten Nachrichten online.
Zu den Zeitschriften :

- WEHRTECHNIK : Erscheinungsweise zweimonatlich
- MILITARY TECHNOLOGY: erscheint monatlich
- NAVAL FORCES : Erscheinungsweise zweimonatlich
- SAFETY & SECURITY INTERNATIONAL : Erscheinungsweise zweimonatlich.
- HANDBUCH der BUNDESWEHR

Kontakt: Herr Christian LAUTERER, MÖNCH Verlagsges.mbH,
Christine-Demmer-Str. 7, 53474 Bad Neuenahr-Ahrweiler,
Tel.: 02641 3703-0,
E-Mail: info@moench-group.com, www.monch.com

Motorola Solutions — M 30

Motorola Solutions bietet innovative sicherheitskritische Kommunikationslösungen und -services für Streitkräfte, Behörden und Organisationen mit Sicherheitsaufgaben sowie Unternehmen. Die zukunftsweisenden und hochverfügbaren Lösungen ermöglichen Anwendern eine zuverlässige Kommunikation.
Das Angebot reicht von Endgeräten und Infrastruktur bis hin zu Software und Services für Militär, Polizei, Feuerwehr, Rettungsdienste, Bundesbehörden sowie Energie- und Versorgungsunternehmen, Fertigung, Transport und Logistik, Gastgewerbe, Einzelhandel und Bildungsinstitute.
Weitere Informationen unter www.motorolasolutions.de sowie auf Twitter unter @MotSolsDE oder in der Motorola Solutions LinkedIn-Community.

MSAB — S 10

MSAB ist weltweit führend in der Mobilgeräte-Forensik-Technologie, um Daten von mobilen Geräten, Apps, Fahrzeugen und Drohnen zu extrahieren, zu analysieren und zu managen. Wir konzentrieren uns zu 100% auf Mobilgeräte- Forensik.
Wir entwickeln die besten Systeme der Mobilgeräteforensik und unterstützen damit Regierungen, Militär und Nachrichtendienste dabei, Bedrohungen zu erkennen und Fälle mit vertretbaren Beweisen schneller lösen zu können. Als Innovationsführer in diesem Bereich bieten wir ein komplettes System der Mobilgeräte-Forensik für alle Anforderungen und Missionen - von internen Untersuchungen bis hin zu strategischen Operationen.
Erfahren Sie mehr an unserem Stand S 10.

ND SatCom GmbH — F 07

Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist ND SatCom der weltweit führende Lieferant von satellitenbasierten Kommunikationssystemen und Bodenstationen, um Kunden mit kritischen Operationen überall auf der Welt zu unterstützen. Kunden in mehr als 130 Ländern haben sich für ND SatCom als eine zuverlässige Quelle für qualitativ hochwertige und sichere Lösungen, die schlüsselfertige und maßgeschneiderte Systeme beinhalten, entschieden. Die innovativen Technologien des Unternehmens werden weltweit von Regierungen, dem Militär sowie in den Bereichen Fernseh- und Rundfunkübertragung, der Telekommunikation und von Unternehmen eingesetzt.
Das Kernprodukt SKYWAN ermöglicht Tausenden von Nutzern täglich, eine sichere, zuverlässige und schnelle Kommunikation.
Kontakt: ND SatCom GmbH, Graf-von-Soden-Strasse D-88090 Immenstaad
Tel.: +49 (0) 7545 939 0, Fax: +49 (0) 7545 939 8702,
E-Mail: info@ndsatcom.com

NSSLGlobal GmbH — F 48

NSSLGlobal ist ein unabhängiger Service-Provider für Satellitenkommunikation und bietet seinen Kunden weltweit, unabhängig von Ort und Zeit, hochwertige Sprach- und Datendienste, sowie IT-Unterstützung. Neben dem NSSLGlobal eigenen high-end VSAT-Netzwerk, bietet das Unternehmen via Inmarsat, Iridium und Thuraya hochwertige Satellitenlösungen im C-, L-, Ka- und Ku-Band.
Im Jahr 2014 fusionierte NSSLGlobal mit der ESL Gruppe zu einem Satellitenkommunikations-Powerhouse und sind ihren Kunden aufgrund der Bündelung ihrer Erfahrung seither ein einzigartiger Partner in der Branche. Gemeinsames Ziel der Unternehmen ist es die Kunden vor Ort zu unterstützen und ihnen eine Infrastruktur, bestehend aus auf allen Kontinenten verfügbaren Büros, Teleports, Servicezentren und lokalen Distributoren, zu bieten. Unterstützend stehen dafür 24/7 Network Operation Centers bereit, die nonstop jedem Kunden technische Unterstützung an Land, auf See oder in der Luft bereitstellen.

NVIDIA — F 45

NVIDIA war Vorreiter bei der Entwicklung einer hochleistungsfähigen Form des Computing, die von den anspruchsvollsten Computernutzern der Welt, Wissenschaftlern, Designern, Künstlern und Spielern, geliebt wird. Unsere Erfindung, die Graphics Processing Unit (GPU), ist der Motor der modernen künstlichen Intelligenz. Unsere Technologie beschleunigt auch die schnellsten Supercomputer, unterstützt hochmoderne Design- und VR-Anwendungen und ist die weltweit größte Gaming-Plattform. Wir ermöglichen es, den da Vincis und Einsteins unserer Zeit ihre schwierigsten Probleme zu lösen: vom Bau selbstfahrender Autos und KI-fähiger Rechenzentren bis hin zur Bekämpfung verheerender Krankheiten wie Krebs und Demenz.

NYNEX satellite OHG — F 27

Als ein führender Integrator von satellitenbasierenden Datenverbindungen für Europa, Afrika und dem Nahen Osten verfügt die NYNEX satellite OHG über eigene HUB-Infrastruktur und über eigene Satellitenkapazität – somit ist ein techniknaher Support, ein individuelles Consulting sowie die professionelle Integration von VSAT-Projekten aus einer Hand möglich.
Die Produktpalette reicht von Internet- bzw, Intranet-Anbindungen land- oder seebasierter Einzelstandorte bis zur Realisierung von länder- oder kontinentübergreifenden Mehrstandort-Netzwerken.
Wir betreiben unsere Satellitennetzwerke von Darmstadt aus, verfügen über ein weltweites Installateurnetzwerk und haben umfangreiche Erfahrungen bei Planung, Betrieb und Aufbau von internationalen Sattelitennetzwerken im Bereich Ministerien und Behörden. Professional satellite services made in Germany!

OHB System AG — F 01

Kreative und verlässliche Konzepte für die Raumfahrt
Der Systemintegrator OHB System AG ist erfolgreich in umfangreichen Anwendungsbereichen für raum-, boden- und luftgestützte Systeme etabliert. Für die Bundeswehr realisiert OHB die raumgestützte Aufklärung SAR-Lupe und SARah inklusive des Bodensegmentes und Betrieb. Zudem realisiert OHB den EnMAP Hyperspektralsatelliten, die sechs Wettersatelliten MTG und ein elektro-optisches System für die Bundesregierung und 32 Galileo FOC Navigationssatelliten. Die SmallGEO Produktlinie bedient die Satellitenkommunikation in Missionen wie Heinrich-Hertz mit ihrem SATCOMBw Anteil, sowie weiteren Satelliten für Laserkommunikation (EDRS-C), flexiblen digitalen Nutzlasten (H36W-1) und vollelektrischen Antrieben (ELECTRA). Im Bodensegment hat OHB kürzlich die Leistungsfähigkeit der Ankerstation Gerolstein um eine UHF-DAMA Fähigkeit erweitert und ist im Luftfahrtbereich ein Kernpartner im Vorhaben FCAS.

ORACLE Deutschland B.V. & Co. KG — F 11

Für mehr als 400.000 Kunden – darunter alle Fortune 100 Unternehmen – und in allen vertikalen Märkten in mehr als 145 Ländern bietet Oracle ein umfassendes und komplett integriertes Set an Cloud-Anwendungen, Plattform Services und Engineered Systems. Da alle Oracle Produkte für den traditionellen On-Premise Einsatz und für Private, Public oder Oracle Cloud at Customer identisch sind, wird es den Kunden ermöglicht, das jeweils geeignete Cloud Modell zu wählen. Bei der Bundeswehr haben sich Oracle Produkte seit vielen Jahren als robuste und zuverlässige Grundlage für Datenmanagement bei einsatzkritischen Systemen bewährt.
Mehr Informationen hier:
https://www.oracle.com/de/corporate/features/oeffentlicher-sektor/index.html

NATO Industry Conference in Berlin

Top officials from NATO, European and North American companies will meet at NITEC18, the NCI Agency's industry conference, to discuss NATO's digital transformation and the Alliance's emerging technological and cyber needs.
The three-day event will also provide an opportunity for Agency representatives to explain how companies can take part in NATO business.
This year, the prestigious conference is held in Berlin and organized under the auspices of the German Ministry of Defence.

"NITEC18 – NATO's Digital Endeavour: Expanding the Ecosystem" will offer a unique opportunity to discuss how the private sector, think-tanks, academia and the NATO Communications and Information Agency can work together to leverage new-generation information technologies to advance the Alliance into the digital future.

Some 600 senior government, military and industry leaders, as well as defence and security experts are expected to attend.
NITEC18 is a collaborative venture between the NATO Communications and Information Agency and AFCEA Europe.

NITEC18 Highlights:

- New trends in digital transformation, disruptive digital technologies and business models that significantly affect the value proposition of digital transformation;
- Top speakers;
- Upcoming business opportunities in the areas of NATO IT modernization, missile defense, Air Command and Control, cyber security, intelligence, etc;
- Interactive events with high-level defence experts;
- Get-together opportunities for NATO, academia, tech hubs and commercial tech companies (including start-ups, entrepreneurs, and Small and Medium Enterprises);
- Breakout sessions on NATO-Industry cooperation;
- Direct access to NATO Programme managers;
- Defence Innovation Challenge;
- Workshops on NCI Agency procurement procedures;
- Women in Tech workshop;
- AFCEA TechNet International exhibition, B2B speed dating workshop and networking opportunities;
- Small Business mentoring sessions - challenge your ideas and get valuable feedback.

NITEC18

NATO's DIGITAL ENDEAVOUR:

Expanding the Ecosystem

22-24 MAY 2018

Berlin Germany

Registration and event updates:
www.nitec.nato.int

SPONSORSHIP AND EXHIBITION OPPORTUNITIES: CONTACT MANDY RIZZO AT MRIZZO@AFCEA.ORG OR +32 (0) 2 705 4384

NCI AGENCY
NCI Agency
events@ncia.nato.int
Tel: +31 (0) 70 374 3090

AFCEA Europe
europe@afcea.org
Tel: +32 (0) 2 705 2731

REGISTRATION NOW OPEN

Panasonic Computer Product Solution F 02

Panasonic Computer Product Solutions (CPS) bietet Unternehmen und Behörden besonders robuste, energieeffiziente und extrem zuverlässige mobile Computing-Lösungen für IT-feindliche Bedingungen. Von robusten TOUGHBOOK Notebooks für Outdoor- oder Büroumgebungen bis hin zu TOUGHPAD Tablets und Handhelds sowie zahlreiche Serviceleistungen und Zubehör für optimale Bedienung. Mit 30 Jahren Erfahrung auf diesem Gebiet ist Panasonic Marktführer am europäischen Markt für robuste Notebooks (VDC Research, März 2017).

„Full-Ruggedized“ Schutz gemäß aller notwendigen Standards (IP65- und teils IP68-Zertifizierung) sowie Militär-Standards (MIL-STD 810G, MIL-STD 461F),

- ergonomische Formfaktoren und geringes Gewicht,
- leuchtstarke Outdoor-Displays für ideale Ablesbarkeit auch unter Sonnenlicht sowie
- äußerst lange Akkulaufzeiten und Hot-Swap Funktionen für unterbrechungsfreien 24-Stunden-Einsatz

Kontakt: www.toughbook.de/kontakt oder Tel.: +49 611 1252

PELI PRODUCTS, S.L.U. S 01

Peli-Hardigg™, der weltweit größte Hersteller von wiederverwendbaren Versand- und Lagerbehältern aus Kunststoff, mit Zulassung für die Verwendung in den Bereichen Militär und Luftfahrt, präsentiert auf der **AFCEA** das extrem widerstandsfähige 19-Zoll Rack-Gehäuse für einsatzkritische IT- & Kommunikationslösungen. Es bietet kompakte Mobilität für Ihr Equipment und erfüllt dabei die Anforderungen und Standards des Militärs.

Die PELI-Hardigg Militärbehälter sind nicht nur nahezu unverwüstlich, luftdicht, wasserdicht und dekontaminierbar – sie sind auch wiederverwendbar. Einsatz für Einsatz kann man sich auch unter den härtesten Bedingungen auf sie verlassen, um überlebenswichtige Ausrüstung zu schützen, zu transportieren und zu verteidigen.

promegis GmbH B 08

Als Spezialist für Geoinformatik, Geoinformationssysteme, Bildverarbeitung, Bildauswertung, Softwareentwicklung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen und fachspezifische Systemlösungen für die Bereiche der öffentlichen Verwaltung, der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), des militärischen Nachrichtenwesens (MilNW) und der militärischen Aufklärung sowie der Energie- und Versorgungswirtschaft. Darüber hinaus unterstützen wir unsere Kunden bei der Umsetzung umfangreicher IT-Projekte.

Die promegis setzt auf innovative und gleichzeitig zukunftssichere Lösungen und steht Ihnen mit langjähriger Erfahrung bei der Realisierung komplexer, integrationsfähiger Systemlösungen zur Seite. Als deutscher Vertriebs- und Entwicklungspartner der Firma Textron Systems bieten wir Ihnen die volle Bandbreite der High-End GIS und Image Analysis Lösungen.

Weitere Informationen finden Sie unter www.promegis.de.

Kontakt: Klaus Scholle, Tel.: +49 (0) 5422 9629-0,
E-Mail: klaus.scholle@promegis.de

PWA Electronic Service- und Vertriebs-GmbH F 02

PWA – Ihr Spezialist für Beratung, Vertrieb, Service und Support von gehärteten Notebooks, Komponenten und Peripherie für mobile Anwendungen. Inzwischen blicken wir gemeinsam mit Panasonic Computer Product Solutions auf eine Erfahrung von mehr als 20 Jahren zurück. Wir bieten für die Panasonic Toughbooks und Toughpads das komplette Sortiment an Unterstützung an: Neugeräte, Zubehör, Restposten, Ersatzteile, Service und Support. Seit September 2007 sind wir außerdem exklusiver Panasonic Service-Partner für Deutschland und Österreich. Zusammen mit unserem Partner Panasonic Computer Product Solutions (CPS) zeigen wir auf der diesjährigen AFCEA die aktuellsten Mobile Computing Geräte von Panasonic Toughbook und Toughpad live vor Ort.

Weitere Informationen finden Sie auf unserer Homepage: www.pwa-electronic.de

QGroup GmbH F 51

Die QGroup besteht seit dem Jahr 1993 und ist als Unternehmen im Bereich IT-Sicherheit und IT-Hochverfügbarkeit tätig. Das Unternehmen hat seinen zentralen Sitz in Frankfurt am Main und zudem Mitarbeiter in den USA und Kanada. Für das Unternehmen General Dynamics ist die QGroup Center of Excellence IT Security und hat langjährige Erfahrungen mit Kunden aus dem Bereich militärische IT-Sicherheit sowie dem behördlichen wie auch dem kommerziellen Sektor. Die QGroup berät Unternehmen in Sicherheitsfragen, unterstützt mit Penetrationstests und unterhält ein 7x24h Security Incident Response Team für Kunden. Dabei überträgt die QGroup pragmatische militärische Sicherheitsstrategien auf nichtmilitärische Kunden, um den Sicherheitsanforderungen von heute besser begegnen zu können.

Rafael Advanced Defense Systems Ltd. M 28

Rafael Advanced Defence Systems Ltd. entwirft, entwickelt, fertigt und liefert für Kunden weltweit eine breite Palette von Hightech-Verteidigungssystemen für Luft-, Land-, See-, Weltraum- und Cyber-Anwendungen. Das Unternehmen bietet seinen Kunden innovative, moderne Lösungen.

Diese Systeme basieren auf umfangreicher Erfahrung, technologischem Know-how und einem tiefgreifenden Verständnis der spezifischen Anforderungen.

Rafael stellt das weltweit ausgereifteste System für den Sensor-zu-Effektor-Zyklus bei einem „Time Critical Target“ TCT (Zeitkritisches Ziel) vor.

Die landbasierten taktischen Kommunikationslösungen von Rafael umfassen moderne Software-basierte Funkgeräte im UHF-/VHF-Bereich, mobile Satcom-Endgeräte, taktische Mobilfunksysteme, taktische Router für mobile Kommunikationsknoten und C2-Anwendungen.

Rheinmetall Defence M 05

Rheinmetall stellt Ansätze zur Digitalisierung der Landstreitkräfte vor

Auf der Fachmesse AFCEA präsentiert Rheinmetall am 11. und 12. April 2018 in Bonn seine Lösungsansätze für das „Deutsche Heer 4.0“. Neben Informationssicherheit und digitaler technischer Dokumentation liegt der Schwerpunkt auf dem Thema Führungsfähigkeit auf der mobilen taktischen Ebene.

Das Hochtechnologieunternehmen für Sicherheit und Mobilität hat sich zusammen mit der Rohde & Schwarz für die Großvorhaben der Bundeswehr MoTaKo (Mobile Taktische Kommunikation) und MoTIV (Mobiler Taktischer Informationsverbund) aufgestellt. Ein Joint Venture wird als Programmorganisation die notwendigen Kompetenzen aus den relevanten Bereichen der Unternehmen, ergänzt um die Fähigkeiten weiterer Partner, bündeln.

roda computer GmbH F 03

... hat sich auf die Entwicklung, Herstellung und den Vertrieb gehärteter Rechnersysteme, Netzwerke und Stromversorgungen spezialisiert. Als führender Anbieter von robuster, mobiler und kundenspezifischer IT-Lösungen für den Einsatz in rauen Umgebungen kann roda auf eine nunmehr 30-jährige Firmenhistorie zurückblicken.

2016 wurde zum 4. Mal in Folge der Rahmenvertrag „gehärtete Notebooks“ mit der Bundeswehr gewonnen, über den auch Toughbook® und Toughpad® der Panasonic bezogen werden können.

Aktuelle Entwicklungen im Hause roda zielen darauf ab, internationalen Standards wie GVA/NGVA gerecht zu werden, um somit auch künftige Bedarfe, die über Projekte wie MoTaKo entstehen, decken zu können.

Kontakt: roda computer GmbH, Landstr. 6, 77839 Lichtenau / Baden
Tel.: +49 7227 / 9579-0, E-Mail@roda-computer.com, www.roda-computer.com

Rohde & Schwarz M 08

Der Technologiekonzern Rohde & Schwarz entwickelt, produziert und vermarktet innovative Produkte der Mess-, Informations- und Kommunikationstechnik für professionelle Nutzer. Um ihre Missionen erfolgreich durchführen zu können und die nationale Souveränität zu gewährleisten, brauchen Streitkräfte unabhängige, hochsichere Kommunikationsmittel.
Mit seinen interoperablen, digitalen Software Defined Radios bietet das Unternehmen für alle wesentlichen robusten Bedarfe der Digitalisierung verfügbare wie zukunftsweisende Lösungen. Der Auftrag der Bundeswehr zur Lieferung der streitkräftegemeinsamen, verbundfähigen Funkgeräteausstattung (SVFuA) für die Landstreitkräfte ist die erste Säule des Großvorhabens MoTaKo (Mobile Taktische Kommunikation).
Rohde & Schwarz Cybersecurity schützt mit seinen Sicherheitslösungen Wirtschaft und Behörden vor Sabotage-Angriffen und Spionage.
www.rohde-schwarz.com

rola Security Solutions GmbH B 11

Jederzeit an jedem Ort auf jede relevante Information zugreifen zu können ist für uns längst Realität. Bei komplexen Ermittlungen, Gefährdungsanalysen oder der Auswertung von Angriffen kommt es darauf an, wichtige Informationen zu erkennen, zusammenzuführen und zu analysieren. Ohne diese Möglichkeiten trägt die bloße Information im Zeitalter des Datenüberflusses kaum noch zur Lösung bei.
rola entwickelt, vertreibt und integriert IT-Lösungen für die Innere und Äußere Sicherheit. Nationale und internationale Sicherheits- und Ermittlungsbehörden vertrauen unserer Kompetenz. Wir versorgen unsere Kunden mit intelligenten IT-Systemen, die auf den einzelnen Anwender zugeschnitten sind.

- Militärische Lagebilderstellung (rsIntCent®)
- Analyse von Massendaten (rsExTract®)
- Auswertung Sozialer Medien (rsNetMAn®)
- Cyber Threat Intelligence (rsCyInt®)

www.rola.com

RUAG Defence F 07

Das Unternehmen RUAG Defence steht für Technologiekompetenz auf allerhöchstem Niveau. Zum Kerngeschäft gehören Produkte und Dienstleistungen für zuverlässige Informations- und Kommunikationsinfrastrukturen, Ketten- und Radfahrzeuge sowie die realistische Soldatenausbildung. Hinzu kommen ballistische und elektromagnetische Schutzlösungen.
Zu den Kunden von RUAG Defence gehören die Schweizer Armee und internationale Streitkräfte sowie Rettungs- und Sicherheitsorganisationen, Behörden und zivile Organisationen auf der ganzen Welt. An der AFCEA tritt RUAG Defence zusammen mit ND SatCom auf. Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist ND SatCom der weltweit führende Lieferant von satellitenbasierten Kommunikationssystemen und Bodenstationen.

Saab Deutschland GmbH S 02
Saab Medav Technologies GmbH

Saab bietet als Hochtechnologie-Unternehmen Weltmarkt führende Lösungen, Dienstleistungen und Produkte in den Bereichen Verteidigung, Luftfahrt, Weltraumtechnik und zivile Sicherheit an. Seit mehr als vier Jahrzehnten haben wir kundenspezifische Lösungen für überlegene taktische Fähigkeiten sowie herausragende Betriebsunterstützung entwickelt und integriert. Systemintegration ist eine von Saabs herausragenden Kompetenzen – die Fähigkeit zukunftsweisende komplexe technische Systemlösungen zu entwickeln, die alle Elemente effizient und zielführend zusammenbringt.
Auf der AFCEA zeigen wir Lösungsbeiträge für die Digitalisierung von Landstreitkräften am Beispiel von interoperablen Kommunikationssystemen, der Detektion von Störsendern, COMINT- und C-ESM-Systemen und weiteren EloKa-Anwendungen sowie eine durchgängige Implementierung eines Führungssystems.
Kontakt: Saab Deutschland GmbH, Jägerstr. 59, D-10117 Berlin, Tel.: +49 (0)30 40899660-0, www.saab.com

SAF Tehnika JSC F 44

Wir, bei SAF Tehnika, sind einer der weltweit führenden Produzenten von Richtfunkequipment mit einer globalen Präsenz in über 130 Ländern und bieten maßgeschneiderte Lösungen für verschiedenste Industrien an.
Eine unserer neuesten Entwicklungen ist unser handheld Spektrumanalysator Spectrum Compact, der den Frequenzbereich von 300MHz bis 87Ghz abdeckt. Das batteriebetriebene Gerät ist bei der Installation, Fehlerbehebung und Planung von Richtfunkstrecken alternativlos. Unsere Punkt-zu-Punkt-Richtfunksysteme bieten die bestmögliche Alternative zur Glasfaser und ermöglichen eine Übertragungsrate von bis zu 1,5Gbps bei einer niedrigeren Latenz und hoher Effizienz. Richtfunksysteme von SAF Tehnika können dabei Distanzen von bis zu 150km überbrücken.
www.saftehnika.com

Samsung Electronics GmbH M 17

Samsung zählt zu den weltweit führenden Elektronikherstellern. Wir haben diese Position erreicht, weil wir eine Vision verfolgen, die fest in unseren Kernkompetenzen, Werten und Zielsetzungen verankert ist.
Wir möchten die Welt inspirieren und die Zukunft auf Grundlage unserer Kreativität, Innovation und Technologien mitgestalten. Als ein weltweiter Marktführer erkennen wir unsere Verantwortung gegenüber der globalen Gesellschaft an. Daher setzen wir unsere Bemühungen und wirtschaftlichen Ressourcen unter anderem dafür ein, in der Elektronik-Branche gemeinsam mit all unseren Kunden, Mitarbeitern und Partnern neue Werte zu etablieren.

SAP Deutschland SE & Co. KG M 15

Als Marktführer für Unternehmenssoftware unterstützt die SAP SE Firmen jeder Größe und Branche, ihr Geschäft profitabel zu betreiben, sich kontinuierlich anzupassen und nachhaltig zu wachsen. Vom Back Office bis zur Vorstandsetage, vom Warenlager bis ins Regal, vom Desktop bis hin zum mobilen Endgerät – SAP versetzt Menschen und Organisationen in die Lage, effizienter zusammenzuarbeiten und Geschäftsinformationen effektiver zu nutzen als die Konkurrenz. Über 365.000 Kunden aus der privaten Wirtschaft und der öffentlichen Verwaltung setzen auf SAP-Anwendungen und Dienstleistungen, um ihre Ziele besser zu erreichen. Weitere Informationen unter www.sap.com.

Schneider Digital F 22

Full-Service Lösungsanbieter für professionelle 3D-Stereo-,VR/AR- und 4K-Hardware
Schneider Digital ist ein weltweit tätiger Full-Service Lösungsanbieter für professionelle 3D-Stereo, 4K- und VR/AR-Hardware und zuverlässiger, zertifizierter Lieferant für Behörden und öffentliche Ämter. Das Schneider Digital Produktportfolio umfasst die richtige professionelle Hardware-Lösung für die jeweilige Anforderung in den Anwendungsbereichen Mapping, Scanning, GIS, Bildauswertung u.v.a.
Unsere Produkte und Lösungen umfassen High Resolution 4K-Monitore (UHD), 3D-Stereo und Touch-Monitore bis 4K-Auflösung und Größen von 27″ bis 98″, VR/AR-Lösungen, von Desktop-System bis hin zur Powerwalls und Multi-Display-Walls, Profi-Grafikkarten von AMD FirePro/Radeon Pro und NVIDIA Quadro, Performance-Workstations sowie innovative Hardware-Peripherie (Tracking, Eingabegeräte u.v.a.). Schneider Digital ist Hersteller einer eignen Powerwall-Lösung (smart VR-Wall) sowie des passiven 3D-Stereo-Monitors 3D PluraView.

Schönhofer Sales and Engineering GmbH F 25

Die Schönhofer Sales and Engineering GmbH ist ein führender, unabhängiger Anbieter von Systemlösungen zur Analyse von Massendaten für Behörden und Privatunternehmen. Unsere Lösungen decken die Datenerfassung (Sensoren), die Verarbeitung und Informationsgewinnung so wie das Datenmanagement und die IT-Infrastruktur ab.
Basis vieler Lösungen ist die Schönhofer TARAN Suite®. Die TARAN Suite® bietet für jeden Auswerteschritt und Analysebedarf das richtige Werkzeug: Signal-, Netzwerk- und Geoanalysen, umfangreiche Text- und Medienanalyse, statistische und lernende Verfahren sowie flexible Berichts- und Ausgabewerkzeuge.
Bestandteile unserer Lösungen sind Robot-basierte Komponenten auf Basis der Kofax Kapow Software und die IBM i2 Analysesoftware. In Kombination unterstützen diese Komponenten den Anwender bei der effizienten Datenerhebung und bringen Transparenz in komplexe Zusammenhänge im Kontext von Ermittlung, Analyse und Auswertung.

SciEngines GmbH B 03

Die SciEngines GmbH bietet spezialisierte Hochleistungsrechner sowie weltweit einzigartige Kryptanalyse Lösungen.
„The SciEngines GmbH RIVYERA S6-LX150 system is the only system that can reasonably be expected to meet the Government's requirements relative to performance, space, and power consumption."
Diese Aussage einer NATO Streitmacht wird durch die Vorteile der verwendeten FPGA Technologie ermöglicht. Im Vergleich zu herkömmlichen Computern ist das Preis-Leistungsverhältnis für spezialisierte Anwendungen 10x verbessert. Platz- und Energieeffizienz 20x.
Naheliegende Anwendungen für solch massive Rechenleistung:

- Cyber (reaktive defense, -warfare, CNO)
- Aufklärung (SIGINT/COMINT) und „ethical hacking"
- Überprüfung eigener IT-Sicherheit / Penetrationstests

Weitere Informationen: www.SciEngines.com oder
E-Mail: info@sciengines.com bzw.
Tel.: 0431-90862000.

secunet Security Networks AG M 13

secunet ist einer der führenden europäischen Anbieter für anspruchsvolle IT-Sicherheitslösungen. Die secunet Division Verteidigung unterstützt militärische Kunden – fokussiert auf Verschlüsselung und Cybersicherheit – beratend, konzeptionell und systemintegrativ. Unsere in nationalen Hochsicherheitsnetzen etablierte, querschnittlich eingesetzte Kryptoarchitektur SINA schützt sensible Informationen im Verteidigungssektor. Sicherheitstechnologien aus den Bereichen Netzwerk-Monitoring (Cyber Defence), digitale Identitäten sowie biometrische Sicherheitslösungen runden das Leistungsportfolio ab.
Unsere Ausstellungsschwerpunkte:

- HaFIS s/v-Clients: SINA Workstation H Client III, SINA Workstation H R RW11
- RAS-Lösung SINA Workstation S des BMVg
- SINA S (R) Ausstattungsoptionen für MoTaKo/MoTIV
- SINA H Lösungen für GEHEIM-Telefonie
- Datei-basierte Verschlüsselung für GEHEIM
- Erste für GEHEIM einsetzbare VS-Nachweisführung
- Mobile SINA Client S Innovationen

Secusmart GmbH M 11

Von ihrer Gründung im Jahr 2007 bis heute hat sich die Secusmart GmbH zu einem globalen Experten für abhörsichere Kommunikation entwickelt. Seit mehr als acht Jahren stattet Secusmart die deutschen Behörden, Ministerien und andere behördliche Institutionen mit abhörsicherer mobiler Kommunikation aus. Seit Ende 2014 ist Secusmart ein Tochterunternehmen von BlackBerry.
Secusmart wird von dem Gründer Dr. Christoph Erdmann und Daniel Fuhrmann, Mitarbeiter der ersten Stunde, geführt. Unter ihrer Geschäftsführung vertrauen mittlerweile mehr als 20 Regierungen weltweit auf die Secusmart-Lösungen.
Die Erfolgsgeschichte der sicheren mobilen Kommunikation wird Secusmart dank ihrer großen Innovations- und Entwicklerkraft in den folgenden Jahren ganz gezielt weiter fortsetzen.

SELECTRIC Nachrichten-Systeme GmbH ME 10

Bereits über 40 Jahre bietet das Familienunternehmen SELECTRIC Nachrichten-Systeme GmbH aus Münster zuverlässige, innovative und wirtschaftliche Hard- und Softwarelösungen sowie Dienstleistungen für die BOS, Industrie, Geschäfts- und Privatkunden. SELECTRIC bietet ein umfassendes Servicekonzept, das u.a. Reparaturpauschalen für BOS-Funkgeräte und Pager, Reparaturen ex-geschützter Endgeräte sowie ein kostenloses Shuttlebox-System zur Minimierung von Ausfallzeiten enthält. Zu den Kernkompetenzen des Unternehmens gehört zudem die Systemtechnik sowie die Projektierung, Realisierung und Wartung kompletter Infrastrukturen für die flächendeckende Funkversorgung.
In Zusammenarbeit mit den großen Netzbetreibern Telekom, Vodafone, Telefonica O2 , 1&1 und yourfone betreut die SELECTRIC Nachrichten-Systeme GmbH als Mobilfunk-Distributor Fachhandels-Partner im gesamten Bundesgebiet. Diesen bietet SELECTRIC ein abgestimmtes Produkt-Portfolio mit einer großen Auswahl aktueller Endgeräte, einer breiten Zubehörpalette, umfangreicher Marketingunterstützung, der kompletten Provisionsabrechnung sowie Hotline- und Servicedienstleistungen.

Selex ES GmbH, a Leonardo company B 04

Leonardo is a global high-tech player in the Aerospace, Defence and Security sector. The Company, with headquarters in Italy, has over 45,600 employees and is present with 180 sites across the globe. Leonardo has a consolidated industrial presence in Europe and US markets and an important network of strategic partnerships in the main high potential markets worldwide. The Company operates through seven Divisions (Helicopters, Aircraft, Aerostructures, Airborne & Space Systems, Land & Naval Defence Electronics, Defence Systems, Security & Information Systems). Each year, Leonardo invests 11% of its revenues in Research and Development.
Contact: www.leonardocompany.com,
Tel: +49 (0)2137-782-328

Sennheiser Vertrieb und Service GmbH & Co. KG F 32

Professionelle Headset-Lösungen für ATC und Contact Center & Office
Sennheiser ist einer der führenden Hersteller von hochwertigen kabellosen und kabelgebundenen Headsets sowie Telefon-/Web-Konferenzlösungen. Die innovative Technologie unterstützt Sie einfach und intuitiv in jeder Business- und Meeting-Situation. Die Headsets überzeugen durch HD Sound, erstklassiges Design, robuste Verarbeitung und benutzerfreundliche Handhabung. Sie eignen sich besonders für ATC, Contact Center, Offices, Unified Communications-Umgebungen und mobiles Business.
Die perfekte Ergonomie der Sennheiser Produkte garantiert den notwendigen Tragekomfort für langes, ermüdungsfreies Arbeiten. Der Einsatz hochwertigster Materialien lässt Sie selbst und Ihren Gesprächspartner von glasklarer Sprachqualität profitieren.
Besuchen Sie uns auf: www.sennheiser.de/cco

SES Networks F 47

Gesicherte Kommunikationslösungen für militärische Missionen, Zivilschutz und humanitäre Einsätze
Organisationen aus dem Bereich BOS, Zivilschutz und Verteidigung sowie militärische Verbände und Einheiten aller Teilstreitkräfte benötigen zuverlässige Breitband-Kommunikationslösungen, die auch unter extrem erschwerten Bedingungen sowie in schlecht zugänglichen Regionen umgehend bereitgestellt werden können.
SES Networks bietet ein breites Portfolio satellitengestützter Lösungen für Daten-, Sprach- und Echtzeitvideoübertragungen, um sicherheitskritische oder

lebensrettende Einsätze optimal zu unterstützen. Mit den SES Networks Satelliten im MEO (Medium Earth Orbit) und GEO (geostationärer Orbit) werden Soldaten, Einsatzkräfte und Hilfsorganisationen in die Lage versetzt, ihre Missionen schnellstmöglich zu erfüllen, Wiederaufbaumaßnahmen zu unterstützen und die Kommunikationsinfrastruktur weltweit zu verbessern.
Mehr Infos zu unseren Lösungen: www.ses.com/networks/government

SFC Energy AG — S 02

Die SFC Energy AG (www.sfc.com) ist ein führender internationaler Anbieter von stationären und mobilen Hybrid-Stromversorgungslösungen. Mit über 38.000 verkauften Brennstoffzellen steht SFC Energy auf Platz eins der Brennstoffzellenhersteller.
Seine zahlreichen mehrfach ausgezeichneten Produkte vertreibt das Unternehmen in der Öl- und Gasindustrie, in Sicherheits- und Industrieanwendungen und im Endverbrauchermarkt.
Das Unternehmen hat seinen Hauptsitz in Brunnthal bei München, Deutschland, und betreibt Produktionsstandorte in den Niederlanden, Rumänien und Kanada sowie Vertriebsniederlassungen in den USA und Kanada.
Die SFC Energy AG notiert im Prime Standard der Deutschen Börse (WKN: 756857 ISIN: DE0007568578).

SINUS Electronic GmbH — F 31

Smarte Feldlagervernetzung im digitalen Zeitalter
Seit mehr als 30 Jahren entwickelt, integriert und liefert die SINUS Electronic innovative Produkte an das deutsche Militär.
Mit unseren kundenorientierten Verbindungsschnittstellen für Kommandofahrzeuge und -Shelter sorgen wir für schnellen und sicheren Datenaustausch, Anwendungssicherheit und hohe Verfügbarkeit. Unsere Produkte entsprechen den strengen Anforderungen der Bundeswehr, NATO und MIL-STD.
Mit unserer SINUS Power-Line-Solution und SINUS Hybrid-Line-Solution bieten wir komplette Infrastrukturen für mobile Gefechtsstände:
- Strom, Daten und Telefonie – alles in einem Kabel
- One-of-a-kind Lösung ermöglicht eine schnelle Bereitstellung im Feld
- Das System kann an die bestehende Infrastruktur angepasst werden
- Das SINUS-Induktiv-Mobil-Telefon bietet eine bis jetzt ungeahnte Flexibilität

Kontakt: info@sinus-electronic.de

Software AG — M 14

INNOVATIV, LEISTUNGSSTARK, PARTNER DER BUNDESWEHR
Die Software AG hilft Unternehmen, Behörden und Streitkräften ihre Prozesse zu digitalisieren. Mit Lösungen für Military Internet of Things, Prozessmanagement und IT-Management steigern Streitkräfte die Effizienz und optimieren ihre Prozesse, um qualifizierte Entscheidungen in Echtzeit zu treffen.
Als Innovationspartner unterstützt die Software AG die Bundeswehr, ihre Prozesse agil an neue Herausforderungen anzupassen und die IT-Landschaft dynamisch zu skalieren. www.SoftwareAG.com
Kontakt: Software AG, Uhlandstr. 9, 64297 Darmstadt
Christoph Reich, Director Defense Business, Tel.: +49 6151 92 4111, +49 170 4549 537, E-Mail: christoph.reich@softwareag.com

Sophos — S 08

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Seit über 30 Jahren ist Sophos ein sicherer Partner für öffentliche Einrichtungen und staatliche Institutionen. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile-und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind sowie untereinander mittels Synchronized Security kommunizieren. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt. Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Sopra Steria Consulting — M 12

Sopra Steria Consulting zählt zu den Top Business Transformation Partnern in Deutschland. Als ein führender europäischer Anbieter für digitale Transformation bietet Sopra Steria eines der umfassendsten Angebotsportfolios für End-to-End-Services: Beratung, Systemintegration, Softwareentwicklung, Infrastrukturmanagement und Business Process Services. Unternehmen und Behörden vertrauen auf unsere Expertise, komplexe Transformationsvorhaben, erfolgreich umzusetzen. Im Zusammenspiel von Qualität, Leistung, Mehrwert und Innovation befähigen wir unsere Kunden, Informationstechnologien optimal zu nutzen.
Themenschwerpunkte:
- IT-Service-Management
- IT-Architekturmanagement
- ILS, LSA, Technische Dokumentation
- Master Data Management & Governance
- Betriebsunterstützung
- IT-Sicherheit
- Organisationsmanagement
- Digitalisierung der Verwaltungsarbeit
- Nutzung der Rahmenverträge des Bundes für die Bundeswehr

SQS Software Quality Systems AG — F 52

SQS: Wir bieten Qualitätssicherung für den öffentlichen Sektor
Sie möchten Ihre Qualitätssicherungsprozesse und -systeme optimieren, die Einführungszeit digitaler Dienste verkürzen und die gesamte interaktive Erfahrung Ihrer Mitarbeiter und der Bürger verbessern? Sie können dies nur durch eine Entwicklungsstrategie für Ihre Software und Systeme erreichen, die von erstklassiger kontinuierlicher Qualitätssicherung sowie von Testverfahren und -methoden untermauert ist. Genau hier setzen wir an.
Wir sind ein globales, unabhängiges Unternehmen für Qualitätssicherung und Softwaretests und besitzen langjährige Erfahrung im öffentlichen Sektor. Wir haben Beschaffungsorganisationen, Gesundheitsstiftungen, Bildungsanbieter und andere zentrale Regierungsstellen durch Beratung hinsichtlich Softwarequalität und Schulungen zu Best Practices bei der Implementierung und Bereitstellung digitaler Dienste unterstützt. Weitere Informationen auf www.sqs.com

steep GmbH — M 07

Die steep GmbH ist ein international erfolgreicher technischer Dienstleister mit mehr als 30 Standorten und rund 750 Mitarbeitern in Deutschland und Europa. Neben den Kernfähigkeiten in den Bereichen Radar-Service, IT-Services, Systemintegration, Training und Mobile Netze zeichnet sich steep durch ein weiteres großes Kompetenzspektrum aus: In Kombination mit den Geschäftsbereichen Logistik und Technische Dokumentation, Material Management, EMV-Service, Managed Services in Partnership und Facility Management profitieren unsere Kunden von der einzigartigen Möglichkeit, alle aufeinander abgestimmten Einzelleistungen in einer gesamtheitlichen Lösung aus einer Hand zu erhalten.
In Anlehnung an das diesjährige Thema der AFCEA-Fachausstellung zeigen wir Ihnen unsere neuesten Lösungen für die Bereiche Compliance, Mobile Device Management und vernetzte Operationsführung.
www.steep.de

SVA System Vertrieb Alexander GmbH — F 23

Die SVA System Vertrieb Alexander GmbH ist einer der führenden deutschen System-Integratoren im Bereich von RZ-Infrastrukturen und beschäftigt mehr als 750 Mitarbeiter an 16 Standorten in Deutschland. Das unternehmerische Ziel der SVA ist es, hochwertige IT-Produkte und -Lösungen unterschiedlichster Hersteller mit dem Know-How und der Flexibilität von SVA zu verknüpfen, um optimale Lösungen zu erzielen. Kernthemen des Unternehmens sind im Rechenzentrum angesiedelt. Weiterhin bietet die SVA aber auch hochwertige Dienst- und Beratungsleistungen im Bereich der Informationstechnik an. Das zertifizierte Solution Center der SVA in Wiesbaden bietet unseren Kunden umfassende Demo-, Entwicklungs- und Schulungsszenarien mit aktuellsten Hardware- und Software-Lösungen.

SYKO Gesellschaft für Leistungselektronik mbH M 22

SYKO entwickelt und produziert Standard und kundenspezifische Leistungselektronik für mobile und stationäre Applikationen an Land, zu Wasser und in der Luft. Wir bedienen die Märkte Bahntechnik, Wehrtechnik, Offshore, Luftfahrt und Schiffbau. Unser Produktportfolio erstreckt sich über DC/DC-Wandler-Frontendgeräte, AC-Einspeisegeräte, Batterieladungssysteme, Dreh-/Wechsel-und Frequenzumrichter. Ströme bis › 800 A, Spannungen bis › 5000 V, Leistungen bis n x 6 kW werden beherrscht. Weltweit gelieferte innovative und normenkonforme Produkte sowie eine Kundenzufriedenheit stehen für Qualität, Funktionalität, Langlebigkeit und Systemverständnis.

Kontakt: SYKO Gesellschaft für Leistungselektronik mbH, Jahnstraße 2, D-63533 Mainhausen, Frau Birgit Tunk, Tel.: 06182 9352-0, Fax: 06182 9352-15, www.syko.de, info@syko.de

Systematic GmbH M 18

Systematic bietet Führungsinformationssysteme und Lösungen für die militärische Interoperabilität und ist Marktführer im Bereich C4I-Software. Die Commercial-off-the-Shelf Produkte der SitaWare und IRIS Produktsuiten haben sich weltweit in multinationalen und streitkräftegemeinsamen Einsätzen bewährt und werden permanent weiterentwickelt. Einsetzbar in stationären, verlegefähigen, mobilen und seegehenden Systemumgebungen, bietet die C4I-Software einen sofortigen operationellen Mehrwert. Intelligente Dienste zur Datenkommunikation ermöglichen die Nutzung vorhandener militärischer Kommunikationsmittel und ermöglichen damit eine gesamtheitliche Betrachtung der Digitalisierung der Streitkräfte. Die Interoperabilität mit nationalen-, internationalen- und NATO-Systemen ist dabei stets im Fokus. SitaWare Headquarters ist in der Bundeswehr bereits erfolgreich in Nutzung. Mit aktuell 26 Nutzerstaaten ist SitaWare das meist genutzte Führungsinformationssystem weltweit.

Kontakt: Systematic GmbH, Im Zollhafen 24, 50678 Köln, www.systematic.com, more.info.de@systematic.com

systerra computer GmbH ME 15

systerra computer GmbH ist seit über 15 Jahren Anbieter von MIL-konformen Rechner-, Speicher- und Netzwerkplattformen für den erweiterten Betriebstemperaturbereich. Unser Schwerpunkt liegt auf Spitzentechnologie mit hoher Verfügbarkeit in anspruchsvoller Umgebung (mobiler und stationärer Einsatz).

Wir setzen dabei auf bewährte und neueste Hard- und Software-Standards. Mit unserer Erfahrung und Expertise erstellen wir in enger Zusammenarbeit mit Kunden und Herstellern auch gerne applikationsspezifische Hardware-Sonderlösungen oder beraten bei der Projektierung.

Partner sind u.a.: MPL, Themis Computer, Moxa, RTD und Acromag

Kontakt: systerra computer GmbH, Kreuzberger Ring 22, 65205 Wiesbaden, Tel.: 0611 / 44 88 9 – 470, E-Mail: info@systerra.de, Internet: www.systerra.de

TELEFUNKEN Radio Communication Systems GmbH & Co. KG M 10

TELEFUNKEN RACOMS entwickelt und vertreibt Funkkommunikationssysteme für moderne, sicherheitsrelevante und hochtechnologische Anwendungen. Für die militärische Nutzung steht ein breit gefächertes Angebot an taktischen und strategischen HF-Funksystemen sowie taktischen VHF- und UHF-Funksystemen zur Verfügung. Diese Systeme sind zu Lande, zu Wasser und in der Luft im Einsatz. Die Kompetenz von TELEFUNKEN RACOMS umfasst alle Bereiche der Produktentstehung – vom Systemdesign, der Entwicklung hochperformanter Produkte und der Produktion bis zur Komplettintegration von Funkübertragungssystemen. Neben dem Kerngeschäft der Funkkommunikation erweitert TELEFUNKEN RACOMS kontinuierlich seine Geschäftstätigkeiten speziell auf den Gebieten Elektrooptische Systeme (z.B. Nachtsichtgeräte, Laserwarnsysteme) und Sensorik und reagiert somit auf den wachsenden Bedarf der Bundeswehr an zuverlässigen und leistungsstarken Systemen zur Unterstützung der Auftragserfüllung in den Einsatzgebieten.

Kontakt: TELEFUNKEN Radio Communication Systems GmbH & Co. KG, Eberhard-Finckh-Str. 55, 89075 Ulm, info@tfk-racoms.com, www.tfk-racoms.com

Textron Systems B 08

Textron Systems Geospatial Solutions flagship software products, ELT®, GIV® and RemoteView™, deliver an extensive set of GEOINT collection tools to enhance the intelligence gathering and analysis process. From imgery analysis and radar exploitation, to terrain feature extraction and advanced 3D visualization, Textron offers a proven solution for situational understanding and interoperability. Textron Systems Geospatial Solutions are used across a broad spectrum of industries: military and defense, border security, disaster relief, environmental engineering, ecosystems monitoring, urban planning, insurance, oil and gas exploration, utility companies and more to provide unmatched fidelity and accuracy in mission planning, actionable intelligence and rapid decision making. See www.textronsystems.com for more information.

Kontakt: Kevin Opitz, E-Mail: geosalesteam@overwatch.textron.com

Thales Deutschland F 13

Thales ist seit Jahrzehnten bei Ausrüstung und Service von Mobilen Taktischen Kommunikationssystemen Partner der Bundeswehr und der NATO. Durch ein hochmodernes, Einsatzerprobtes Portfolio steht Thales als Systemanbieter der Bundeswehr bei der Digitalisierung der Streitkräfte mit Beratung, Entwicklung, Design, Inbetriebnahme und Service zur Seite. Thales verfügt über ein Produktportfolio, das modular an den einsatzbedingten Kommunikationsbedarf angepasst werden kann. Eine moderne Systemarchitektur ermöglicht eine nahtlose, medienbruchfreie Kommunikation und bildet einen wichtigen Beitrag zum Missionserfolg. Einsatzerprobte C2-Kommunikationssysteme sowie die Entwicklung der Breitbandwellenform ESSOR bilden die Säulen einer dienste-orientierten Kommunikation.

Moderne Funksysteme wie die neue Software-Defined-Radio-Produktfamilie SYNAPS, leistungsfähige Kryptologie- und Schlüsselmanagementlösungen sowie moderne SOTM-Systeme stellen die notwendigen Kommunikationsplattformen zur Sicherstellung eines „Quality of Services“ sicher.

www.thalesgroup.com/germany

T-Systems International GmbH B 10

Mit Standorten in über 20 Ländern, 43.700 Mitarbeitern und einem externen Umsatz von 7,9 Milliarden Euro (2016) ist T-Systems einer der weltweit führenden herstellerübergreifenden Digitaldienstleister mit Hauptsitz in Europa. T-Systems ist Partner seiner Kunden auf dem Weg der Digitalisierung. Das Unternehmen bietet integrierte Lösungen für Geschäftskunden. Bei der Tochtergesellschaft der Deutschen Telekom kommt alles aus einer Hand: vom sicheren Betrieb der Bestandssysteme und klassischen IT- und Telekommunikations-Services über die Transformation in die Cloud einschließlich internationaler Netze, bedarfsgerechter Infrastruktur, Plattformen und Software bis hin zu neuen Geschäftsmodellen und Innovationsprojekten im Internet der Dinge. Grundlage dafür sind globale Reichweite für Festnetz- und Mobilfunk, hochsichere Rechenzentren, ein umfassendes Cloud-Ökosystem mit standardisierten Plattformen und weltweiten Partnerschaften sowie höchste Sicherheit.

tukom GmbH ME 11

tukom steht für Telemetrie und Kommunikation. Zusammen mit unseren renommierten, internationalen Partnern liefern wir Lösungen für breitbandige, funkbasierte Kommunikation sowie Analyse- und Planungswerkzeuge für unterschiedliche Plattformen zu Land, Luft, See und im Weltraum. Bei der der AFCEA-Fachausstellung demonstrieren wir zusammen mit L3 Communication Systems West Fähigkeit zur multinationalen Air-Land-Integration auf Basis der ROVER-Technologie sowie das Management von ISR-Missionen mit dem Network-Control-System (NCS).

Zudem demonstrieren wir mit unserem Partner Silvus Technologies militärische Mesh-MANET-Technologie für breitbandige Kommunikation in urbaner Umgebung sowie für land- luft- und seegestützte Plattformen. Sehen Sie außerdem, wie mit dem System-Tool-Kit in 4d komplexe Waffensysteme modelliert und analysiert werden.

Utimaco S 08

Utimaco gehört zu den führenden Herstellern für Hardware-Sicherheitsmodule (HSM). Diese erzeugen und verwalten kryptografische Schlüssel und sichern digitale Identitäten. Damit bilden HSM den Vertrauensanker zum Schutz digitaler Daten und kritischer Infrastrukturen - etwa im Finanzsektor, in der Automobilindustrie, für Cloud-Dienstleister oder den öffentlichen Dienst. Die Module lassen sich mühelos in bestehende Software-Lösungen integrieren.
Utimaco entwickelt und fertigt am Standort Aachen und beschäftigt dort sowie in den USA, Großbritannien und Singapur etwa 170 Mitarbeiter. Seit der Unternehmensgründung im Jahr 1983 setzen Unternehmen aller Branchen sowie Banken und Behörden in über 80 Ländern Hardware-Sicherheitsmodule von Utimaco ein und schützen weltweit Millionen von Endkunden.
Weitere Informationen: hsm.utimaco.com/de/

Verband der Reservisten der deutschen Bundeswehr e.V. ME 08

Der Verband der Reservisten der Deutschen Bundeswehr (VdRBw) hat mehr als 115.000 Mitglieder. Wir vertreten die Reservisten in allen militärischen Angelegenheiten. Sie sind: Reservisten der Bundeswehr (ordentliche Mitglieder), aktive Soldaten (außerordentliche Mitglieder), Personen ohne Wehrdienst (fördernde Mitglieder).Vertreten sind alle Dienstgrade – vom Gefreiten bis zum General. Unser attraktives und breitgefächertes Angebot und das kameradschaftliche Miteinander im Verband sind auch bei jungen Leuten sehr gefragt. Die Hälfte unserer Mitglieder ist jünger als 50 Jahre.
Als Reservist der Bundeswehr haben Sie Vorteile durch Ihre Mitgliedschaft im Reservistenverband:

- das Angebot des Verbandes, um sich militärisch, körperlich und geistig fit zu halten,
- Engagement für die Streitkräfte und Sicherheitspolitik,
- Teamgeist und kameradschaftliches Miteinander,
- Öffentlichkeitsarbeit als Mittler zwischen Bundeswehr und Gesellschaft.

Der Reservistenverband im Netz: www.reservistenverband.de – www.facebook.com/Reservistenverband – www.twitter.com/diereserve

VITES GmbH S 02

Die VITES GmbH („VITES“) ist ein junges, stark wachsendes Unternehmen, das sich auf Produkte der Breitband-Funktechnik für professionelle Einsatzgebiete spezialisiert hat. Fokusgebiet des Unternehmens ist eine innovative Funktechnologie für vollelektronische Strahlformung und –nachführung. Auf Basis von Phased-Array-Antennentechnologie und Software-Defined-Radio (SDR) werden SATCOM-on-the-Move (SOTM) Lösungen und breitbandige Datenlinks entwickelt, die auch in Defense-Anwendungen deutliche Vorteile gegenüber herkömmlichen Systemen aufweisen. Ein weiterer Schwerpunkt ist "HiMoNN", die marktführende Produktlösung für breitbandige Ad-Hoc-Funksysteme im Bereich der öffentlichen Sicherheit und im Katastrophenschutz. HiMoNN ist dort als zuverlässige, robuste, ausgereifte und kosteneffiziente Lösung sehr erfolgreich und lässt sich auch in Defense-Szenarien einsetzen.
Standort des Unternehmens ist Ottobrunn bei München.
Pressekontakt: VITES GmbH, Einsteinstraße 32, 85521 Ottobrunn, www.vites.de
Kontakt: Martin Gassner, Geschäftsführer, Tel. 089 6088-4600, E-Mail:info@vites-gmbh.de

ZARGES GmbH B 14

In den ZARGES Produkten vereinen sich seit über 80 Jahren die vielfältigen Vorteile des Leichtmetall-Werkstoffs Aluminium wie hohe Stabilität bei gleichzeitig geringem Gewicht, Korrosionsfestigkeit sowie Flexibilität im Einsatz. So hat ZARGES für jeden das geeignete Produkt und kann auch individuelle Lösungen anbieten. Ob es ums Konfektionieren, Lagern, Transportieren, Organisieren, Schützen oder Steigen geht: bei ZARGES finden Sie immer eine optimale Lösung auch im Bereich Speziallösungen.
ZARGES fertigt nach aktuellen gesetzlichen Normen und Standards für Industrie und Militär. Individuelle Lösungen werden für unsere Kunden maßgeschneidert und können mit offiziellen Zulassungen z.B. nach BAM ausgeliefert werden.
Kontakt: ZARGES GmbH, Tel.: +49 881 687-0, Fax: +49 881 687-500
Internet: www.zarges.de, E-Mail: zarges@zarges.de

AFCEA-Fachausstellung 2017

Fotos: Stefan Veres

BSC Berlin Security Conference

17th Congress on European Security and Defence

Impressions BSC 2017

For further photos and information please see

www.euro-defence.eu

BSC Berlin Security Conference

17th Congress on European Security and Defence

Berlin Security Conference 2018

European Security and Defence – remaining transatlantic, acting more European

27 – 28 November 2018, Vienna House Andel's Berlin

Photos: Dombrowsky

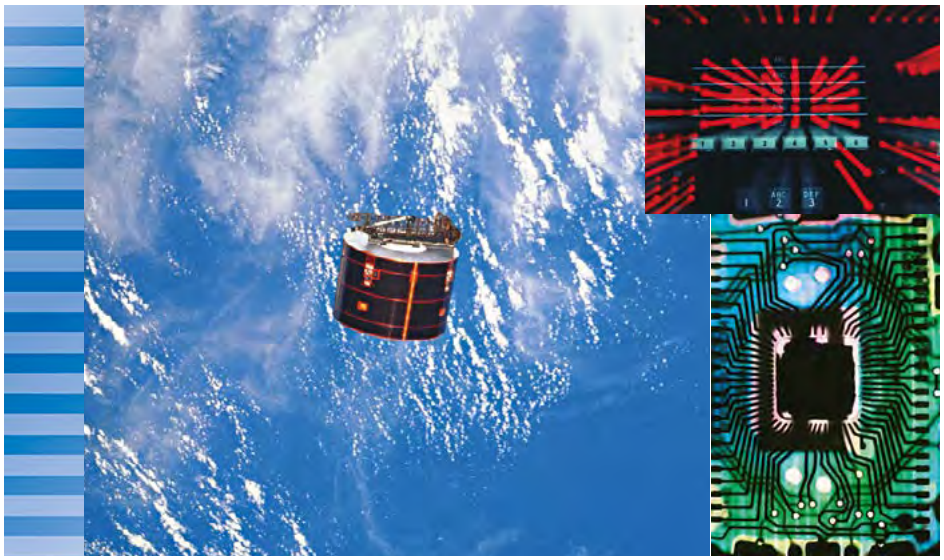
Impressions of the BSC 2017

The Berlin Security Conference

- One of the largest yearly events on European Security and Defence
- Meeting place for up to 1 000 participants from more than 50 countries
- International forum for members of parliament, politicians and representatives of the armed forces, security organisations and industry
- Partner in 2018: Netherlands
- Former Partners: Russia, United Kingdom, Turkey, USA, France, Sweden
- Exhibitions with companies from Europe and abroad
- Organised by the Behörden Spiegel – Germany's leading independent Newspaper for the Civil and Military Services

Further Information:

www.euro-defence.eu



Vorankündigung:

33. AFCEA-Fachausstellung

10./11. April 2019

www.afcea.de