Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

JAHRESBERICHT 2016/17

JAHRESBERICHT 2016/17

Ein Bericht über uns,
unsere Forschung und
unsere Verantwortung
für die Zukunft!

VORWORT

Liebe Leserin, lieber Leser,

ich darf Sie einladen, einen Blick in die Forschungslabore des Fraunhofer FKIE zu werfen, und ich möchte Ihnen mit diesem Bericht einige unserer Forschungs-Highlights vorstellen. Mit unserer Arbeit tragen wir dazu bei, »die Welt jeden Tag sicherer zu machen«. Mit diesem Mission Statement haben wir es uns zur Aufgabe gemacht, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen. Eine große Herausforderung, der wir uns täglich stellen, aber gleichzeitig auch ein großer Ansporn, in unserer anwendungsorientierten Forschung immer herausragende Ergebnisse zu erreichen.

Unser Ziel ist es, wissenschaftlich fundiert neue Technologien zu erforschen und zu entwickeln. Gemeinsam mit den Anwendern arbeiten wir intensiv daran, diese Technologien in die Praxis zu bringen, sicherheitskritische Prozesse formal zu erfassen, weiterzuentwickeln und zu optimieren. Für uns steht dabei stets der Mensch im Mittelpunkt: Vieles kann und muss automatisiert werden, damit der Mensch sich bei existenzbedrohenden Risiken auf das wirklich Wesentliche beschränken und Verantwortung für sein Tun und für die eingesetzte Technik übernehmen kann. So begleiten und gestalten wir gemeinsam mit unseren Partnern, Zuwendungs- und Auftraggebern den Fortschritt in die Zukunft zum Nutzen und zum Schutz unserer Gesellschaft!

Der »Künstlichen Intelligenz« haben wir in diesem Jahr das Cover gewidmet. Ein Thema, das derzeit in aller Munde ist und eine breite Diskussion entfacht hat. Längst setzen sich Wirtschaftsunternehmen, die Wissenschaft von der Informatik bis zur Philosophie, die Filmindustrie und nicht zuletzt die Politik mit »KI« auseinander. Für das Fraunhofer FKIE ist der Einsatz von Methoden aus dem Bereich der KI längst gelebter Forschungsalltag in allen Fachabteilungen – ausgewählte Beispiele präsentieren wir auf den nachfolgenden Seiten.

2016 und 2017 waren für das FKIE bedeutende und wirtschaftlich sehr erfolgreiche Jahre, in denen wir unseren Partnern als verlässlicher Forschungsdienstleister zur Seite standen und uns gut positionieren konnten. Gleichzeitig sind wir in zahlreichen Projekten entscheidend vorangekommen – einen Querschnitt dieser von uns konzipierten und prototypisch umgesetzten Innovationen finden Sie in diesem Bericht dokumentiert.

Darüber hinaus stellen wir Ihnen wichtige Meilensteine vor, mit denen wir unsere Sichtbarkeit verstärken konnten. Herausragend ist an dieser Stelle unser »Technologieforum«, bei dem wir in zweijährigem Turnus unsere anwendungsorientierte Forschung präsentieren.

Weltweite Beachtung fand der Takedown der Botnetzinfrastruktur »Avalanche«, an dem das Fraunhofer FKIE maßgeblich mitgearbeitet hat.

Natürlich gehörte für unser Institut und unsere Mitarbeiterinnen und Mitarbeiter auch die Eröffnung des neuen Standortes in Bonn zu den Highlights der vergangenen zwei Jahre.

Ich wünsche Ihnen eine interessante Lektüre und spannende Einblicke in unsere Tätigkeitsfelder. Allerdings kann und soll ein solcher Bericht den persönlichen Dialog mit uns nicht ersetzen. Daher freuen wir uns auf den intensiven, persönlichen Austausch mit Ihnen über unsere Arbeit und über unsere bestehenden und kommenden Projekte!

Ihr

Prof. Dr. Peter Martini
Institutsleiter

INHALT

UNSER INSTITUT

MISSION STATEMENT

Wir arbeiten jeden Tag daran, die Welt sicherer zu machen.

Unser Ziel ist es, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen.

KURZPORTRAIT

Getreu seinem Mission Statement befasst sich das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE mit der frühzeitigen Erkennung, Minimierung und Beherrschung existenzbedrohender Risiken. In enger Kooperation mit strategischen Partnern aus dem militärischen wie auch dem zivilen Sektor entwickelt das Institut zu diesem Zweck Technologien und Prozesse für die gesamte Verarbeitungskette von Daten und Informationen.

Die Forschung des Fraunhofer FKIE ist dabei auf die Verbesserung der Leistungsfähigkeit cyber-physischer Systeme ausgerichtet. Hier liegt der Fokus auf der Weiterentwicklung informationstechnischer Systeme hinsichtlich Bedienbarkeit, Datensicherheit, Interoperabilität und Vernetzung sowie der Auswertung verfügbarer Informationen mit hoher Präzision und Zuverlässigkeit. Methoden des Machine Learning und der Künstlichen Intelligenz sind dabei besonders hervorzuheben und werden am Institut anwendungsorientiert entwickelt und eingesetzt.

Für ihre Auftraggeber aus dem Bereich der Bundeswehr, verschiedener ziviler Sicherheitsorgane und aus der Industrie erforschen die Wissenschaftler am Fraunhofer FKIE zu diesem Zweck Methoden und Verfahren für sämtliche Sicherheitsbereiche – auf dem Boden, in der Luft, zur See, unter Wasser und im Cyberspace. Im Fokus der Forschungsarbeit steht dabei immer der »Faktor Mensch«. Als letztlich verantwortlicher Entscheider und Akteur ist er der Dreh- und Angelpunkt bei der Entwicklung effizienter Mensch-Maschine-Systeme.

Anwendungsorientiert und praxisnah

Als führendes Institut für anwendungsorientierte Forschung und praxisnahe Innovation in der Informations- und Kommunikationstechnologie forscht das Fraunhofer FKIE hierbei schwerpunktmäßig in fünf Themenfeldern:

I Informationsgewinnung, Entscheidung und Führung
II Cyber- und Informationsraum
III Aviation and Space
IV Maritime Systems
V Land Systems

Das Fraunhofer FKIE verfügt in diesen Bereichen über umfangreiches Domänenwissen. Die Forschungsleistungen erstrecken sich hierbei von Studien und Tests bis hin zur Entwicklung von Prototypen. Dank insgesamt elf Abteilungen mit unterschiedlichen, einander ergänzenden Kernkompetenzen ist das Institut fachlich breit aufgestellt und in der Lage, systemische Lösungen anzubieten. Jede Abteilung betreibt Forschung und Entwicklung auf dem hohen wissenschaftlichen Niveau, für das der Name Fraunhofer steht. Mit Kompetenz in der Breite und Exzellenz im Detail stellt sich das Fraunhofer FKIE Tag für Tag den aktuellen wissenschaftlich-technologischen Herausforderungen in sicherheitsbezogenen Fragestellungen.

ANSPRECHPARTNER

INSTITUTSLEITER

Prof. Dr. Peter Martini
Telefon 0228 9435-287
peter.martini@fkie.fraunhofer.de

VERWALTUNGSLEITERIN

Ursula Fuchs
Telefon 0228 9435-280
ursula.fuchs@fkie.fraunhofer.de

LEITER STRATEGIE & MARKTERSCHLIESSUNG

Dr. Kai Nürnberger
Telefon 0228 9435-118
kai.nuernberger@fkie.fraunhofer.de

Abteilungsleiter
SENSORDATEN- UND INFORMATIONSFUSION

Priv.-Doz. Dr. Wolfgang Koch
Telefon 0228 9435-373
wolfgang.koch@fkie.fraunhofer.de

Abteilungsleiter
KOMMUNIKATIONSSYSTEME

Dr. Markus Antweiler
Telefon 0228 9435-811
markus.antweiler@fkie.fraunhofer.de

Abteilungsleiter
INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME

Dr. Michael Wunder
Telefon 0228 9435-511
michael.wunder@fkie.fraunhofer.de

Abteilungsleiter
HUMAN FACTORS

Dr. Thomas Alexander
Telefon 0228 50212-432
thomas.alexander@fkie.fraunhofer.de

Abteilungsleiterin
MENSCH-MASCHINE-SYSTEME

Annette Kaster
Telefon 0228 9435-492
annette.kaster@fkie.fraunhofer.de

Abteilungsleiter
SYSTEMERGONOMIE

Prof. Dr. Frank Flemisch
Telefon 0228 9435-573
frank.flemisch@fkie.fraunhofer.de

Abteilungsleiter
USABLE SECURITY & PRIVACY

Prof. Dr. Matthew Smith
Telefon 0228 73-54218
matthew.smith@fkie.fraunhofer.de

Abteilungsleiter
CYBER ANALYSIS & DEFENSE

Dr. Elmar Padilla
Telefon 0228 50212-595
elmar.padilla@fkie.fraunhofer.de

Abteilungsleiter
CYBER SECURITY

Prof. Dr. Michael Meier
Telefon 0228 73-54249
michael.meier@fkie.fraunhofer.de

Abteilungsleiterin
PRIVACY AND SECURITY IN UBIQUITOUS COMPUTING

Jun.-Prof. Dr. Delphine Reinhardt
Telefon 0228 73-60551
delphine.reinhardt@fkie.fraunhofer.de

Abteilungsleiter
KOGNITIVE MOBILE SYSTEME

Dr. Dirk Schulz
Telefon 0228 9435-483
dirk.schulz@fkie.fraunhofer.de

NACHRUF

Einen tiefen Einschnitt hat das Fraunhofer FKIE im Jahr 2016 durch den viel zu frühen Tod seines stellvertretenden Institutsleiters, Prof. Dr.-Ing. Christopher Schlick, erfahren. Er starb nach kurzer, schwerer Krankheit am 3. Oktober 2016 im Alter von nur 49 Jahren.

Wir möchten an dieser Stelle noch einmal an Professor Schlick, an sein Wirken für die Wissenschaft und vor allem an sein Engagement für unser Institut erinnern.

Professor Schlick, geboren 1967 in Berlin, absolvierte nach seinem Abitur ein Simultanstudium der Automatisierungstechnik und Wirtschaftswissenschaften an der Technischen Universität Berlin. 1994 begann er seine wissenschaftliche Laufbahn am Institut für Arbeitswissenschaft (IAW) der RWTH Aachen bei Professor em. Dr. Holger Luczak. Dort lag sein Arbeitsschwerpunkt im Bereich der Mensch-Maschine-Schnittstellen autonomer Produktionszellen sowie an computergestützter Teamarbeit in der verteilten Automobilentwicklung.

1997 wurde er am IAW Forschungsgruppenleiter, zwei Jahre später promovierte er an der Fakultät für Maschinenwesen der RWTH zum Dr.-Ing. Seine Habilitation folgte im Jahr 2004. Für beide Arbeiten erhielt Professor Schlick bedeutende Auszeichnungen. Für seine Dissertationsschrift wurde ihm die Borchers-Plakette verliehen, die an Doktorandinnen und Doktoranden der RWTH Aachen verliehen wird, die ihre Prüfung »Mit Auszeichnung« bestanden haben. Seine Habilitationsschrift wurde mit dem Gertraude-Holste-Preis 2004 ausgezeichnet. Von 2000 bis 2004 war er Leiter der damaligen Abteilung »Ergonomie und Führungssysteme« an unserem Institut. Von dort aus folgte er im Jahr 2004 dem Ruf an die RWTH Aachen und leitete seit Dezember 2004 das Institut für Arbeitswissenschaft.

Seit April 2005 war er neben seiner Tätigkeit an der RWTH Mitglied unserer Institutsleitung und trug die wissenschaftliche Verantwortung für den Forschungsbereich »Ergonomie«.

Professor Schlick war als Gutachter und Berater in verschiedenen internationalen Gremien wissenschaftlich tätig. Darüber hinaus war er in die Etablierung und Initiierung wesentlicher ergonomischer Forschungsprogramme involviert. Exemplarisch für die zahlreichen und prägenden Arbeiten und Beteiligungen in diversen nationalen und internationalen Gremien und Ausschüssen sei sein großes Engagement für die Gesellschaft für Arbeitswissenschaft (GfA) erwähnt. Ihr stand er zuletzt als Präsident vor und hat so die Zielsetzung der Ergonomie und Arbeitswissenschaft maßgeblich beeinflusst. Noch im Jahr 2016 hat er den 62. GfA-Frühjahrskongress in Aachen ausgerichtet.

Professor Schlick war ein exzellenter Wissenschaftler, der unser Institut über viele Jahre ganz wesentlich geprägt hat. Vor allem fehlt uns Christopher Schlick als einfühlsamer und in jeglicher Hinsicht aufrichtiger Mensch, der uns jederzeit mit Rat und Tat zur Seite stand. Wir vermissen sein hohes Engagement, seinen fachlichen Rat und seinen persönlichen Einsatz sehr. Wir haben mit ihm nicht nur eine Führungskraft und einen ausgezeichneten Wissenschaftler, sondern auch einen großartigen Menschen und Freund verloren.

Das Fraunhofer FKIE wird Professor Dr.-Ing. Christopher Schlick stets ein ehrendes Andenken bewahren. Sein Werk lebt in uns fort.

Für die Mitarbeiterinnen und Mitarbeiter
des Fraunhofer FKIE

Prof. Dr. Peter Martini

IT-STANDORT BONN

KOMPETENZZENTRUM FÜR IT-SICHERHEIT
STRATEGISCHE PARTNER

KOMPETENZZENTRUM FÜR IT-SICHERHEIT

Die Digitalisierung und der rasante Fortschritt in der Informationstechnologie verändern Wirtschaft und Gesellschaft so schnell wie kaum eine andere technische Revolution zuvor. In allen Lebensbereichen halten neue IT-Systeme und IT-Anwendungen Einzug. Technologien, die allerdings auch anfällig für Angriffe, Sabotage, Spionage, Missbrauch und Datendiebstahl sein können. Aus diesem Grund nimmt die IT-Sicherheit als zentrales Thema im Bereich der Inneren und Äußeren Sicherheit eine zunehmende Bedeutung ein. Sie zählt zu den Schlüsseltechnologien für eine moderne Gesellschaft.

Zahlreiche große und kleinere Unternehmen, Start-ups, Forschungs- und Bildungseinrichtungen, Institute und öffentliche Institutionen widmen sich diesem Themenkomplex, um Sicherheitslücken in IT-Systemen zu verhindern, zu detektieren oder zu schließen. Der Fokus ist hierbei auch auf die Bewertung aktueller Sicherheitsrisiken gerichtet sowie auf die Berücksichtigung von Sicherheitsaspekten bereits im Entwicklungsstadium von IT-Systemen. Der Kampf gegen feindliche IT-Angriffe auf Unternehmen, kritische Infrastrukturen oder öffentliche Verwaltungen kann zudem nicht allein gewonnen werden. Aus diesem Grund steht auch die Weiterbildung von Fach- und Führungskräften im Blickfeld der IT-Sicherheitskonzepte.

Im Ballungsgebiet der Bundesstadt Bonn finden sich besonders viele IT-Spezialisten, die global agieren, aber auch lokal miteinander kooperieren. So hat sich Bonn in den vergangenen Jahren zu *dem* Standort und vor allem zu *dem* Kompetenzzentrum für IT-Sicherheit in Deutschland und Europa entwickelt. Wer für den IT-Sicherheitssektor arbeitet, kommt am Standort Bonn nicht vorbei. Hier sind die Akteure auf vielfältige Weise miteinander vernetzt und entwickeln gemeinsam Lösungen für eine sichere digitale Welt. Zwar nicht unbedingt vom Standort, dafür aber von seiner Verzahnung her mittendrin befindet sich das Fraunhofer FKIE. Mit seinen elf renommierten Forschungsabteilungen unterstützt das Institut all diese Player als verlässlicher Partner im Hintergrund.

Bei den zivilen öffentlichen Einrichtungen ganz vorn zu nennen, sind sicherlich das Bundesamt für Sicherheit in der Informationstechnik (BSI), das seinen Sitz in Bonn hat. Mit seinen derzeit 700 Mitarbeitern ist das BSI der zentrale IT-Sicherheitsdienstleister des Bundes. Seine Aufgabe ist es, für einen sicheren Einsatz von Informations- und Kommunikationstechnik in der Gesellschaft zu sorgen.

Mit ihrem neu in Dienst gestellten militärischen Kommando Cyber- und Informationsraum (KdoCIR) hat auch die Bundeswehr ein klares Zeichen in Richtung IT-Sicherheit gesetzt. Ähnlich wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft und See zuständig sind, ist das Kommando CIR für die Dimension Cyber- und Informationsraum verantwortlich. Schließlich kennen Bedrohungen aus dem Netz keine Ländergrenzen. Die Wahl des Dienstortes wird auch als klares Bekenntnis der Bundeswehr zum IT-Kompetenzzentrum Bonn bewertet. Dies wurde auch im Rahmen der feierlichen Indienststellung betont, in dem ausdrücklich die Nähe zum Bundesministerium der Verteidigung, wie auch zum BSI und dem FKIE hervorgehoben wurde. Gleichzeitig hat die Bundeswehr mit dem neuen Kommando die Verantwortlichkeiten für die Themen Cyber und IT gebündelt. So wurden in der Region Bonn das Kommando Informationstechnik der Bundeswehr (KdoIT Bw), inklusive des Betriebszentrums IT-System der Bundeswehr (BtrbZ IT-Sys Bw) in Rheinbach, das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCS Bw) in Euskirchen, das Kommando Strategische Aufklärung (KSA) in Grafschaft-Gelsdorf und das Zentrum für Geoinfomationswesen der Bundeswehr in Euskirchen dem Kommando CIR unterstellt.

Weiterhin stellen der externe IT-Dienstleister der Bundeswehr, BWI, wie auch die Bundespolizei in Swisttal, das Bundeskriminalamt in Meckenheim, der Verfassungsschutz in Köln und die verschiedenen Einrichtungen der Vereinten Nationen wesentliche Bestandteile des regionalen Cyber-Clusters dar.

Umfangreiches Know-how ergänzen zudem die zahlreichen in Bonn ansässigen Unternehmen der IT-Security-Branche. Allen voran steht hierbei als führender europäischer Telekommunikationsanbieter sicherlich die Deutsche Telekom. Dort ist das Thema IT- und Cybersicherheit nicht erst seit den massiven Hacker-Angriffen auf ihre Kommunikationsnetze zentral angesiedelt. Der Schutz der vernetzten Welt wird bei der Telekom als Bestandteil der digitalen Verantwortung des Weltkonzerns gesehen. Auch hier leistet das FKIE über einen sehr engen Austausch mit den Verantwortlichen für Cybersicherheit einen großen Beitrag.

Kein Kompetenzzentrum ohne akademischen Background. Den liefert die Universität Bonn, mit der das FKIE über verschiedene Forschungsaktivitäten wie auch personelle Strukturen sehr eng verknüpft ist. So ist FKIE-Institutsleiter Prof. Dr. Peter Martini gleichzeitig Leiter des Instituts für Informatik 4 an der Hochschule und hält jedes Semester zahlreiche Lehrveranstaltungen. Ein weiteres Ergebnis der engen Kooperation zwischen FKIE und Universität ist eine Professur für IT-Sicherheit. Prof. Dr. Michael Meier wurde von der Universität auf diese Professur berufen und leitet gleichzeitig die Abteilung »Cyber Security« (CS) am FKIE. Insgesamt sind neun Wissenschaftler des FKIE in die Lehre der Uni Bonn, der RWTH Aachen sowie der Hochschule Bonn-Rhein-Sieg eingebunden. Der Dreiklang aus Forschung, Lehre und Anwendung, eines der Grundprinzipien der Fraunhofer-Gesellschaft, wird auf diese Weise tagtäglich mit Leben gefüllt.

Das gebündelte Know-how und Wissen um IT-Sicherheit und Cyberangriffe geben die Experten aus Wissenschaft und Lehre direkt an Fach- und Führungskräfte aus Behörden und Industrie weiter. Im Rahmen des Lernlabors Cybersicherheit, das von den beteiligten Instituten und Fachhochschulen zusammen mit der Fraunhofer Acadamy ins Leben gerufen wurde, vermitteln Mitarbeiter des FKIE in Seminaren und Workshops kompaktes Wissen über Cyberangriffe und sorgen in den Unternehmen für die erforderliche IT-Sicherheitskompetenz. Eine weitere Säule für das Cyber-Cluster Bonn-Rhein-Sieg.

STRATEGISCHE PARTNER IN DER REGION BONN

STADT KÖLN

RHEIN

RHEIN

RHEINISCHE FRIEDRICH-WILHELMS-UNIVERSITÄT BONN
Institut für Informatik
Philosophische Fakulät

HOCHSCHULE BONN-RHEIN-SIEG
Lernlabor Cybersicherheit

KOMMANDO INFORMATIONSTECHNIK DER BUNDESWEHR
KdoIT Bw

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONS-TECHNIK
BSI

KOMMANDO CYBER- UND INFORMATIONSRAUM
KdoCIR

FRAUNHOFER FKIE
Standort Bonn

BUNDESSTADT BONN

FRAUNHOFER FKIE
Hauptsitz Wachtberg

KREIS EUSKIRCHEN

BUNDESPOLIZEI

SWISTTAL

ZENTRUM FÜR CYBER-SICHERHEIT DER BUNDESWEHR
ZCS Bw

EUSKIRCHEN

BUNDESKRIMINALAMT

BETRIEBSZENTRUM IT-SYSTEME DER BUNDESWEHR UND ZCO
BtrbZ IT-Sys Bw

RHEINBACH

MECKENHEIM

RHEIN-SIEG KREIS
KREIS AHRWEILER

KOMMANDO STRATEGISCHE AUFKLÄRUNG
KdoStratAufkl (KSA)

GRAFSCHAFT

RHEIN

● Ämter ● Bundeswehr ● Bundespolizei ● Hochschulen

Auszug Landkreiskarte © GeoBasis-DE / BKG 2013

Stand Oktober 2017

SCHWERPUNKT »KÜNSTLICHE INTELLIGENZ«

KI-BASIERTE ENTSCHEIDUNGSUNTERSTÜTZUNG
Fake News
Deep Learning
Machine Learning

KI-BASIERTE ENTSCHEIDUNGSUNTERSTÜTZUNG

Das Thema »Künstliche Intelligenz« (KI) ist schon längst keine Science Fiction mehr, sondern Realität. Sie ist allgegenwärtig im zivilen und hochgradig relevant im militärischen Bereich. Denn der militärische Einsatz von KI ist nicht mehr eine Frage des »ob«, sondern vielmehr des »wie«. Und genau dort setzt Fraunhofer FKIE mit seiner FuE-Arbeit an: Forschungsgegenstand sind dabei nicht die Grundlagen der Künstlichen Intelligenz, sondern die Anwendung von Methoden der KI in ausgewählten Einsatzgebieten – ganz gemäß dem FKIE-eigenen Leitspruch »vom Einsatz her gedacht«.

Was aber meint der Begriff »Künstliche Intelligenz« eigentlich genau? KI ist in Forschung und Anwendung in unterschiedlichen Ausprägungen zu finden. Als oberste Kategorie wird häufig zwischen »starker KI« und »schwacher KI« unterschieden. Starke KI erhebt den Anspruch, sämtliche intellektuelle Fähigkeiten des Menschen zu erreichen oder gar zu übertreffen. Das ist spannender Stoff für das Kino, Science Fiction à la HAL 9000 und Spielbergs Film »AI – Künstliche Intelligenz«. Umstritten ist jedoch, ob starke KI überhaupt möglich ist.

Zwischenzeitlich ist die Forschung längst jenseits derartiger Schreckensszenarien und Dystopien angekommen. Im Gegensatz zur starken KI löst die schwache KI konkrete Aufgaben oder Fragestellungen: bei den Spielen Go und Schach zum Beispiel, aber auch die Fragen, welches Produkt der Amazon-Kunde wohl sonst noch kaufen würde oder welche Aktien man kaufen oder besser schnell verkaufen sollte.

Intelligente Assistenzsysteme für die militärische Anwendung

KI unterliegt im militärischen Bereich besonderen Bedingungen, aus denen sich jedoch auch Optimierungen der im zivilen Bereich genutzten KI ableiten lassen. Das größte Potenzial hat in jedem Fall das Teaming mit intelligenten Assistenzsystemen. Vieles lässt sich mit KI automatisieren, aber selbst die leistungsstärksten heutigen 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.

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 bzw. besser lösen, Prozesse optimieren, Vorschläge unterbreiten (Entscheidungsunterstützung) und den Nutzer verstehen sowie seine Intention erkennen.

Insgesamt müssen die Systeme den Menschen entlasten, Routineaufgaben wie Analysen und Auswertungen übernehmen, damit der Mensch sich auf die wirklich wichtigen Dinge konzentrieren kann. Kurz gesagt: Benötigt werden intelligente Assistenzsysteme.

Deep Learning für selbstadaptive Systeme

Die jüngsten Erfolge der KI gründen vor allem auf dem Einsatz von Deep Learning. Hierbei handelt es sich um die hochskalierte Erweiterung einer älteren Technik, nämlich der Technik der künstlichen neuronalen Netze. Diese orientiert sich grob an der Arbeitsweise des Gehirns. Deep Learning ordnet die simulierten Nervenzellen in hierarchisch strukturierten Schichten an. Sinnvoll interpretierbar für den Nutzer sind im Regelfall nur Input und Output. Was genau dazwischen, in

KI-BASIERTE ENTSCHEIDUNGSUNTERSTÜTZUNG

den inneren Schichten, geschieht, bleibt verborgen – sie werden daher als »hidden layers« bezeichnet und realisieren somit einen sogenannten Blackbox-Ansatz. Mittels Deep Learning kann ein System etwa lernen, ein menschliches Gesicht zu identifizieren. Oder auch Texte und Funksignale zu klassifizieren. Oder Funksignale überhaupt erst erfassbar zu machen.

Bayes'sche Verfahren für die Frage nach dem Warum

Deep Learning ist aber bei Weitem nicht das einzige Verfahren der KI, das in der Praxis zum Einsatz kommt. Als Alternative seien beispielhaft die Bayes'schen Schätzer genannt. Diese sind seit Jahren mit sehr guten Erfolgen in probabilistischen Expertensystemen, z. B. in der Medizin, im Einsatz. Im Gegensatz zu Deep Learning stehen hier Kausal-Zusammenhänge im Vordergrund, die durch abduktive und deduktive Schlüsse ermöglicht werden, also die Frage: Warum ist das so? Die Graphenstruktur einer Wahrscheinlichkeitsverteilung wird hier ebenso durch das System erlernt wie deren Parameter. Mit Bayes'schen Verfahren ermittelt beispielsweise die Abteilung »Sensordaten- und Informationsfusion« (SDF), mit welcher Wahrscheinlichkeit Sensordaten einem bestimmten physikalischen Phänomen zuzuordnen sind: Mittels eines Weitbereichsradars können die Wissenschaftler etwa unter widrigen Bedingungen gleichzeitig stattfindende Luftkampfübungen aufklären. Die Daten, die das Radar erfasst, werden mithilfe Bayes'scher Inferenz analysiert. Nur so gelingt es, die beteiligten Kampfjets zu detektieren, zu klassifizieren und über längere Zeit hinweg zu verfolgen.

Automatisierte Hilfe bei der IT-Sicherheit durch maschinelles Lernen

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 zu verarbeiten.

Nicht zuletzt gilt es auch, Angriffe auf militärische KI-Systeme zu verhindern. Denn diese sind besonders gefährdet: Sie stellen Hochwert-Ziele für Angriffe im Cyber- und Informationsraum dar und müssen folglich besonders geschützt werden.

Der Mensch bleibt im Mittelpunkt

Doch es gibt auch gravierende Risiken, die bei naiver Nutzung gerade ziviler KI bestehen. Zahlreiche KI-Ansätze – insbesondere auch Deep Learning – 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. Denn auch bei maschinellem Lernen gilt der alte Grundsatz: Garbage in, Garbage out. Für derartige Systeme ist es von zentraler Bedeutung, ob für angestrebte Einsatzgebiete überhaupt hinreichend viel brauchbares Trainingsmaterial vorliegt – und ob dieses Trainingsmaterial nicht eventuell manipuliert ist.

Hier ist die Einbindung des Menschen in die – in der Maschine ablaufenden – Prozesse von vorrangiger Bedeutung. Der Mensch muss als Entscheider und als Träger von Verantwortung »im Loop« oder zumindest hinreichend nah an automatisierten Prozessen gehalten werden.

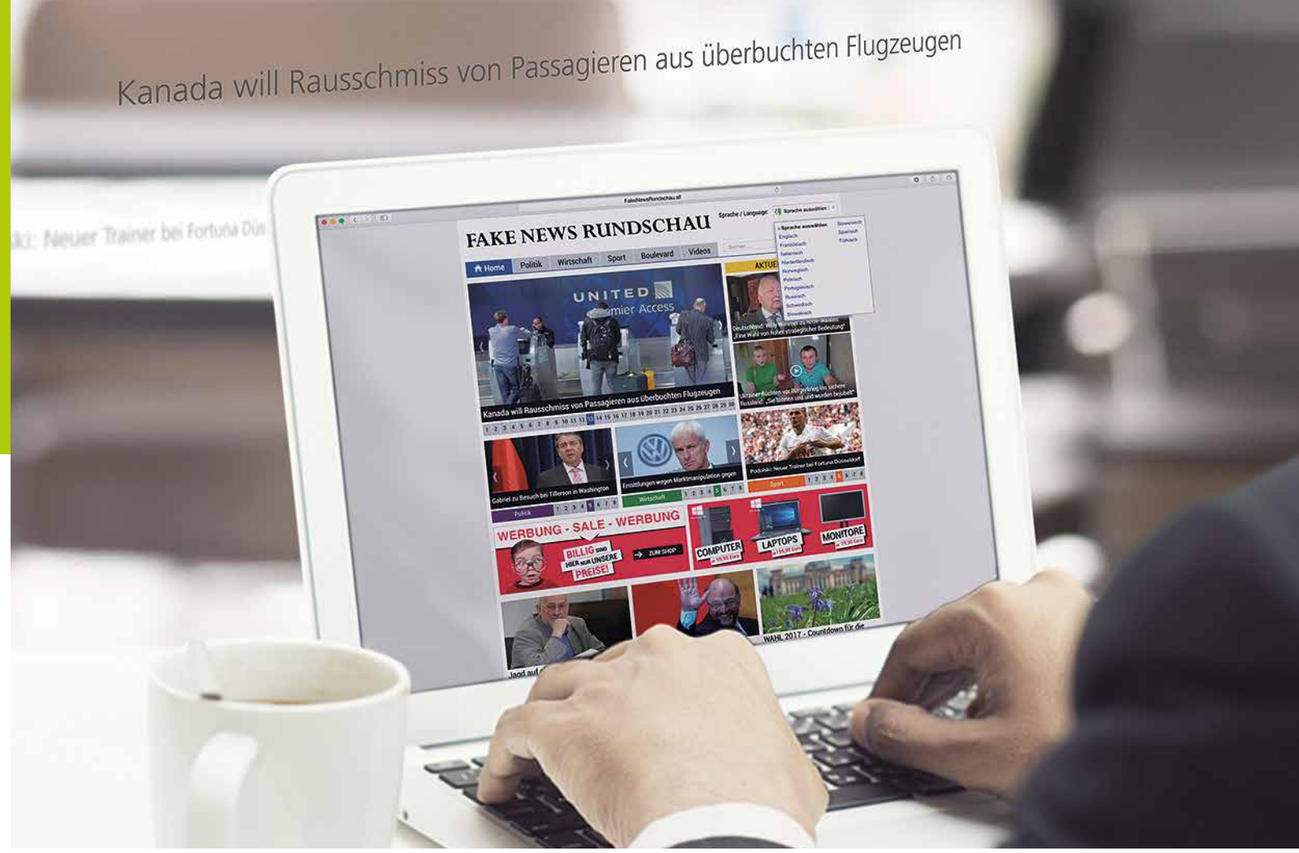
Das Fraunhofer FKIE entwickelt auch hierfür Technologien: Human-Machine-Interfaces, die den speziellen Anforderungen wie Usability und User Experience gerecht werden, aber auch multimodaler Interaktion und der Anpassung an natürliche menschliche Interaktionsformen sowie an den jeweiligen Zustand des Benutzers. Auch zu diesem Zweck werden Methoden der KI eingesetzt, beispielsweise um Situations- oder Verhaltensmuster sowie kognitive Problemzustände zu erkennen oder um die Assistenzfunktionen dynamisch an die Benutzerzustände anzupassen.

Geschichte:
KI hält Einzug in immer mehr Lebensbereiche. Die Entwicklung begann bereits in den 50er Jahren in den USA. In den Fokus der Öffentlichkeit schaffte es die KI spätestens mit dem Schachcomputer Deep Blue, dem es 1996 als erste Maschine gelang, den Schachweltmeister Juri Kasparow in einer Partie zu schlagen. In Rechenzentren und auf Großrechnern kommen AI-Algorithmen seit vielen Jahren zum Einsatz.

Definition:
Die Begriffsdefinition von KI bezeichnet ein Teilgebiet der Informatik, das sich mit der Automatisierung intelligenten Verhaltens befasst. Da bereits die Definition von Intelligenz an sich nicht exakt gefasst werden kann, ist auch die Künstliche Intelligenz nur schwer abzugrenzen. Allgemein wird der Begriff verwendet, um Systeme zu beschreiben, die das Ziel haben, die menschliche Intelligenz und entsprechendes Verhalten mit Maschinen nachzubilden und zu simulieren.

Methoden & Werkzeuge:
Für die Umsetzung von KI in reale Szenarien gibt es verschiedene Werkzeuge und Methoden, die auch parallel verwendet werden können. Grundlage von allem ist Machine Learning. Darunter versteht man Systeme, die aus Efahrungen Wissen aufbauen, d. h. Muster und Gesetzmäßigkeiten erkennen und das mit stetig steigender Geschwindigkeit und Genauigkeit. Eine immer wichtiger werdende Unterart des Maschinellen Lernens ist Deep Learning. Hier kommt ausschließlich neuronale KI zum Einsatz. Deep Learning ist die Basis für die meisten neuen KI-Anwendungen. Das System ist in der Lage, den Aufbau der neuronalen Netze stetig zu erweitern. Mittels zusätzlicher Schichten soll es komplexer und an viele Einsatzzwecke angepasst werden.

FAKE NEWS



FÜR SAUBERE WAHLEN IN DEUTSCHLAND

Filterblase, Wahlbeeinflussung, Propaganda 2.0 – das Thema »Fake News« ist omnipräsent in den Medien und beeinflusst die heutige Gesellschaft stark, nicht zuletzt, weil dadurch auch ein Metadiskurs in den Medien über die Medien entstanden ist. Seit Sommer 2017 aber hat das Thema für und in Deutschland noch weiter an Relevanz und Brisanz gewonnen. Denn noch bis vor kurzem hätten es vermutlich die Wenigsten für möglich gehalten, dass Wahlkämpfe in Deutschland durch »Fake News« beeinflussbar sind.

Hilfe in diesem Szenario verspricht ein Tool des Fraunhofer FKIE, das das Wissenschaftler-Team um Professor Dr. Ulrich Schade, Forschungsgruppenleiter »Informationsanalyse« in der Abteilung »Informationstechnik für Führungssysteme« (ITF), entwickelt hat und das sich mittels Machine Learning selbstadaptiv programmiert. Schon lange beschäftigt sich der Linguist und Mathematiker damit, wie Texte automatisiert, mit und ohne Hilfe von KI, analysiert, verarbeitet oder gar generiert werden können. In Zeiten von Big Data und Social Media, hier insbesondere Twitter, haben diese Fragen an Bedeutung gewonnen. So haben sich beispielsweise Regierungsstellen mit dem Ziel der Durchführung und Gewährleistung einer »sauberen« Bundestagswahl 2017 an das Fraunhofer FKIE gewandt und um technische Unterstützung gebeten. Eine »saubere Wahl« oder »clean election«, wie der Projekttitel lautet, meint, dass das Wählervotum nach demokratischen Prinzipien und somit ohne eine Manipulation der Meinung durch Desinformation mittels Fake News abläuft.

Wie das System selbst lernt, Fake News zu erkennen

Das Klassifikationstool können die Wissenschaftler auf unterschiedliche Zwecke anpassen, sodass alle Arten von Texten kategorisiert werden können. Automatisch ordnet das Tool diese den zuvor festgelegten Kategorien zu. Zunächst aber müssen die Forscher um Schade das Tool für die aktuelle Aufgabe vorbereiten und dafür selbst analytisch tätig werden: Für jede Klassifikation, so auch für die Unterscheidung von »richtigen« und »falschen« Meldungen, müssen sie Merkmale definieren, über die das Tool die Kategorien erlernt.

Hierbei stehen die Forscher vor der besonderen Herausforderung, dass sie nicht nach einem bestimmten Inhalt suchen können, sondern zunächst allgemein falsche Informationen herausfiltern müssen. So können zum Beispiel auf semantischer Ebene Formulierungen und Wortkombinationen, die auf eine undemokratische Haltung hindeuten, analysierbare Kennzeichen von Fake News sein: Wer schreibt »die aktuelle Bundeskanzlerin«, impliziert, dass sie wahrscheinlich nicht mehr lange im Amt sein wird. Formulierungen wie diese finden sich weder im alltäglichen Sprachgebrauch, noch in der journalistischen Berichterstattung, nicht einmal in Wahlkampftexten der Parteien.

Die Metadaten sind entscheidend

Ein weiterer Hinweis sind orthografische Fehler. Eine hohe Anzahl oder auch deutliche Schwankungen der Fehlerverteilung in einem Text können ein Indiz dafür sein, dass es sich um eine Falschmeldung handelt. Der wichtigste Aspekt aber sind die Metadaten: Wann wird gepostet und in welchen Abständen? Der Zeitpunkt eines Posts kann Aufschlüsse geben über die Zeitzone, mitunter sogar über das genaue Herkunftsland, wenn beispielsweise an einzelnen Tagen, die in einem bestimmten Land Feiertage sind, keine Posts eingestellt werden. Die Häufigkeit ist vor allem von Bedeutung, wenn es darum geht, Bots zu identifizieren. Hier kann zusätzlich das Verhältnis derjeniger, denen ein Account folgt, zu denjenigen, die diesem Account folgen, Aufschluss geben. Bleiben noch die Hashtags: Auch hier werden die Forscher bereits vorab aktiv und durchsuchen das Netz – insbesondere Twitter – mithilfe eines initialen Hashtags nach weiteren passenden Hashtags. Auf diese Weise werden Beispieltexte gesammelt, die in das Trainingskorpus eingehen können. Denn auch hier gilt: je besser der Trainingsdatensatz, desto besser die Ergebnisse.

Ein noch schärferes Bild kann das System durch die Einführung von Unterkategorien liefern, wie zum Beispiel die weitere Unterscheidung zwischen islamistisch motivierter, russischer und innerdeutscher rechter Propaganda. »Eine Erwähnung des Sykes-Picot-Abkommens von 1916, in dem Großbritannien und Frankreich Einflusszonen im Nahen Osten abgesprochen haben«, erläutert Prof. Schade, »ist beispielsweise ein ganz konkreter Hinweis auf den IS.«

Vorverarbeitung massenhafter Textdaten

Nun müssen die Wissenschaftler noch die Metrik auswählen, mit der die besten Ergebnisse erzielt werden können. Hierzu testen sie unterschiedliche statistische Lernverfahren auf einem Fünftel des Textkorpus. Die übrigen vier Fünftel des Korpus werden für das Training verwendet. Hiermit ist die Arbeit der Forscher erst einmal getan. Das System beginnt mit der Kategorisierung aktueller, etwa aus Twitter stammender Meldungen.

Insgesamt entsteht auf diese Weise eine »Social Media«-Lageübersicht, die den involvierten Behörden als Frühwarnsystem dienen kann. Das Tool des Fraunhofer FKIE befähigt sie, medial gegenzuhalten und beim Aufkommen von Fake News auf die gezielte Desinformation aufmerksam zu machen. So bleibt gewährleistet, dass Wahlen möglichst ohne Manipulation und nach demokratischen Kriterien ablaufen.

KONTAKT
Prof. Dr. Ulrich Schade
Telefon +49 228 9435-376
ulrich.schade@fkie.fraunhofer.de

DEEP LEARNING

DATEN-VORSELEKTION FÜR DIE AUFKLÄRUNG

Mit dem technologischen Fortschritt bei Sensoren und Sensorsystemen wächst die Menge der Daten, die diese einsammeln und zur Auswertung liefern. So auch im Bereich der Funkaufklärung. 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 detektierter Einzelsignale 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. KI bietet auch hierfür innovative Lösungsansätze.

»Die zentrale Fragestellung heute lautet: Ist da in den Massen verfügbarer Daten etwas, das ich suche?«, erläutert Professor Dr. Frank Kurth die Herausforderung, der sich Bundeswehr und Behörden und Organisationen mit Sicherheitsaufgaben aktuell gegenübersehen. Gemeinsam mit Alexander Höck leitet er die Forschungsgruppe »Aufklärung und Störung« am Fraunhofer FKIE. »Unsere Forschungsarbeit zielt daher auf Möglichkeiten zur Klassifikation und Vorselektion der eingehenden Signaldaten ab.« Denn auch bei Militär und Sicherheitsbehörden ist der Personalschlüssel eng, eine automatisierte Voranalyse angesichts der Fülle von Daten für ihre Verwendung zu Aufklärungszwecken daher unabdingbar. Die beiden Informatiker und ihr Team von Wissenschaftlern setzen deswegen in mehreren Anwendungen Methoden der KI zur Unterstützung des Menschen beim Vorselektionsprozess von Massendaten ein.

Automatische Klassifikation von Funkverfahren

Demodulierte Funksignaldaten liegen in Form von Bitstrings vor. Klassifiziert und einem bestimmten Funkverfahren zugeordnet wurden sie bislang durch Operateure, also Menschen. Dies geschah mittels Verfahren, die in Form von Regeln beschrieben waren. Doch können auch künstliche neuronale Netze, also Computer, diese Regeln erlernen? Und anschließend aus ihren Erfahrungen weiterlernen, um das Verfahren so fortlaufend zu optimieren? Um dies herauszufinden, modellierten die Wissenschaftler die Vorgehensweise der Operateure. Ziel war es, eine geeignete mathematische Beschreibung der Bitstrings zu finden, denn das wäre Voraussetzung für eine automatisch erlernbare Erkennungsmethode. Tatsächlich zeigte sich dabei, dass relevante Bitstrings mittels komplexer Abhängigkeiten einzelner Bits charakterisiert werden können. Mithilfe dieses Resultats war es dann möglich, unter Einsatz von Convolutional Neural Networks (CNNs) und Deep Belief Nets (DBNs), zwei Konzepten des maschinellen Lernens, eine automatische Klassifikationsmethode abzuleiten.

Automatische Vorselektion von Sprachdaten

Auch bei der Schlüsselwort- und Sprechererkennung unterstützt KI. Die besonderen Herausforderungen liegen hier in einer von Anwendungsszenario zu Anwendungsszenario variierenden Qualität der Sprachsignale, dadurch bedingt möglicherweise ungünstig konfigurierten Erkennungsalgorithmen, und wenig verfügbarem Trainingsmaterial, gerade bei ressourcenarmen Sprachen. Als Vorselektionsverfahren zur Sprechererkennung mit der niedrigsten Fehlerrate stellte sich hierbei ein neues, kombiniertes Klassifikationsmaß heraus: die Verbindung des klassischen Vorgehens (»i-vector«-Ansatz) mit tiefen neuronalen Netzen.

Kurth: »Lernverfahren zur Selektierung von Daten sind für die Aufklärung von höchster Relevanz, denn die rohen Signalmassendaten haben für sich genommen keinen explizit ersichtlichen Informationswert. Sie liefern keine Antworten auf die Fragestellungen der Aufklärungsprozesse: Ist da etwas, das ich suche? Um was handelt es sich? Stellt es eine Bedrohung dar? Was muss/soll ich tun? Die Daten-Vorselektion mittels Deep-Learning-Methoden erleichtert und beschleunigt die Analyse und somit den gesamten Aufklärungsprozess.«

KONTAKT
Prof. Dr. Frank Kurth
Telefon +49 228 9435-868
frank.kurth@fkie.fraunhofer.de

MACHINE LEARNING

25 MERKMALE FÜR DIE SUCHE NACH SCHADSOFTWARE

Auch im Bereich der IT- und Cybersicherheit kann Machine Learning einen großen Mehrwert bieten: einen Vorsprung vor Hackern, Internetkriminalität und Spionage. Denn durch maschinelles Lernen können Muster in enorm großen Datenmengen oft in einem Bruchteil der Zeit erkannt werden, die eine manuelle Analyse in Anspruch nehmen würde. Die Abteilung »Cyber Analysis & Defense« (CA&D) des Fraunhofer FKIE setzt diese Methode der KI daher ganz gezielt zu diesem Zweck ein.

Rafael Uetz, wissenschaftlicher Mitarbeiter bei CA&D, beispielsweise nutzt Machine Learning zur Anomalie-Erkennung in Netzwerken. Sein Augenmerk ist auf Cyberangriffe sowie Fehlkonfigurationen des Netzwerks gerichtet, die mittels einer Identifizierung von Ausreißern gefunden werden können. Dabei definieren sich Ausreißer als statistische Abweichungen vom Normalzustand – also von dem Zustand, in dem sich ein System in letzter Zeit hauptsächlich befand. Das Entscheidende ist, dass die Merkmale zahlreich sind, auf deren Basis die Ausreißer erkannt werden. Sie werden durch das System gelernt und anschließend automatisiert angewandt.

Auf die richtigen Kriterien und Trainingsdaten kommt es an

Die Merkmale müssen zudem so entworfen sein, dass »das System weiß, wonach es suchen muss«. Es ist folglich viel Wissen und Vorarbeit seitens der Wissenschaftler notwendig, das betont auch Thomas Barabosch, ein Kollege von Uetz: »Die richtigen Merkmale für den jeweiligen Zweck abzuleiten, ist eine sehr zeitintensive Aufgabe.« Dem großen Zeitgewinn bei der endgültigen Analyse steht also zunächst noch ein hoher initialer Zeitinvest gegenüber. Barabosch hebt zudem die Bedeutung der Qualität der Trainingsdaten hervor: Sie müssten sauber sein, gut benannt, damit die Maschine die Klassifikation eindeutig erlernen kann, und so zahlreich und vor allem auch so vielfältig wie möglich. Nur bei einer hohen Varianz der Daten kann das System die richtigen Unterscheidungen treffen.

Finden die Systeme, die Uetz mithilfe von Kollegen und Studenten entwickelt und dann trainiert hat, nun Auffälligkeiten, muss es sich dabei nicht zwingend um einen Angriff auf das Netzwerk handeln. So kann es unter Umständen auch sein, dass die Anomalie einfach eine versehentliche Fehlkonfiguration darstellt. In beiden Fällen ist es aber wichtig, dass zu diesem Zeitpunkt ein Mensch auf die Ergebnisse der Suche schaut und entscheidet, was zu tun ist. Ob dieser nun aber den Angriff im Detail analysiert, nachdem er den infizierten Rechner separiert hat, oder ob er eine durch die Fehlkonfiguration möglicherweise entstandene Sicherheitslücke schließt: In jedem Fall hat die Maschine ihm sehr viel Arbeit abgenommen und gegebenenfalls Vorfälle entdeckt, die sonst unerkannt geblieben wären.

Schutz gegen einen »Man-in-the-Browser«-Angriff

Barabosch nutzt Machine Learning, um Schadsoftware in Prozessen zu finden, beispielsweise eine Schadsoftware, die in einen Browser injiziert ist. Er nennt es einen »Man-in-the-Browser«-Angriff, mit dem die Schadsoftware etwa Kreditkartendaten abgreifen kann. 25 Merkmale benötigt Barabosch in der Regel hierzu. So sei z. B. die Tatsache auffällig, dass ein Speicherbereich in einem Prozess sowohl lesbar, schreibbar als auch ausführbar sei.

Ein dritter Wissenschaftler aus der Abteilung, der sich mit Machine Learning befasst, ist Tobias Albertsson: Er beschäftigt sich mit der Klassifikation von Domains bzw. Domain Generation Algorithms (DGAs). Eine Domain ist ein im Web einmaliger und eindeutiger Name. Ein Domain Generation Algorithm wiederum ist ein Bestandteil von Malware zum Generieren von Domänennamen. Durch einen solchen Algorithmus generierte Domains werden vom Botnet-Betreiber, d. h. dem Betreiber einer Gruppe automatisierter Schadprogramme, registriert und als Kontaktpunkt zum Command-&-Control-Server (C&C) verwendet. Die auf diese Weise häufig, wenn nicht sogar täglich wechselnden Domänennamen erschweren den ermittelnden Behörden die Rückverfolgung des C&C des Botnetzes. Albertsson hat ein System aufgebaut, das diese bösartigen Domains aufspürt. Ist diese Suche erfolgreich, können so die zugehörigen Botnet-Betreiber identifiziert oder die Nutzer der als Bot missbrauchten PCs gewarnt werden.

Der Gewinn durch Machine Learning: Zeitvorsprung

So unterschiedlich die Analyseabsichten der drei Wissenschaftler auch sind, ihr gemeinsamer Nenner ist, dass Machine Learning zur Vorverarbeitung massenhafter Daten eingesetzt wird. Aufgrund des dadurch erzielten Zeitvorteils werden Cyber-Analysten in die Lage versetzt, auf Augenhöhe mit Internetkriminellen und Spionagediensten zu bleiben.

KONTAKT
Dr. Elmar Padilla
Telefon +49 228 50212-595
elmar.padilla@fkie.fraunhofer.de

PROJEKT-HIGHLIGHTS

INFORMATIONSGEWINNUNG, ENTSCHEIDUNG UND FÜHRUNG

Business-Intelligence-Dashboard
Funksignalerkennung
Adaptive Mensch-Maschine-Interaktion
REHSTRAIN

CYBER- UND INFORMATIONSRAUM

PA-SIEM
Cloud Computing
FACT
EIDI

AVIATION AND SPACE

AMBOS
Prozessoptimierung
Passiv

MARITIME SYSTEMS

PASSAGES
EFAS

LAND SYSTEMS

PAA
CBRNE-Roboter
Unimog

PROJEKT-HIGHLIGHTS

THEMENFELD I

INFORMATIONSGEWINNUNG, ENTSCHEIDUNG UND FÜHRUNG

Die Bewältigung militärischer Einsätze oder auch kritischer Situationen im zivilen Umfeld hängt entscheidend von echtzeitnahem Lagebewusstsein und effektiver Zusammenarbeit ab. Um beide Ziele zu erreichen, ist es erforderlich, schwer zugängliche oder verborgene Daten und Informationen zu erschließen, diese in entscheidungsunterstützende Bilder einzubinden und für Führungsaufgaben in komplexen Umgebungen bereitzustellen. Nahezu alle wissenschaftlichen Abteilungen des Fraunhofer FKIE sind mit ausgewählten Aspekten dieser Aufgabenstellungen befasst. Sie unterstützen die Entwicklung von Assistenzsystemen, die der Steuerung sicherheitsrelevanter oder betrieblicher Prozesse dienen.

Die Gewinnung, Übertragung und Fusion heterogener Rohdaten schafft die Grundlage zur Erstellung von Lagebildern. Bei der Informationsgewinnung werden verschiedenste Datenquellen, zum Beispiel mithilfe von Sensoren, erschlossen. Die Art der erfassten Daten ist vielfältig und reicht von akustischen Signalen über elektrooptische Informationen und chemische Stoffeigenschaften bis hin zu automatisiert erschlossenen textbasierten und sprachlichen Informationen. Weitere statische und dynamische Informationen wie Plangrößen oder Wettervorhersagen werden zusätzlich einbezogen. Die sich ergebende Datenheterogenität wird mittels Fusion bewältigt und mithilfe maßgeschneiderter Algorithmen auf ein Format angepasst. Die anschließende Analyse bzw. Vorverarbeitung und logische Verknüpfung erfolgt in vielen Fällen automatisiert durch intelligente Algorithmen, beispielsweise durch Deep-Learning-Verfahren.

Damit entsteht die Grundlage für ein echtzeitnahes, konsolidiertes Lagebild, das zum Beispiel den Zustand von Objekten, Prozessen und Ressourcen sowie relevante Kontextinformationen in einer georeferenzierten Karte nutzergerecht darstellt. Der Nutzer kann somit unter Wahrung von Transparenz und Entscheidungshoheit frühzeitig auf potenzielle Risiken (wie zum Beispiel auf eine schmutzige Bombe) und mögliche Handlungsoptionen hingewiesen werden.

Effektives Lagemanagement erfordert neben verlässlichen Informationen entsprechend auch Interaktionsmöglichkeiten zwischen zentralen koordinierenden und dezentralen ausführenden Kräften. Hierbei unterstützen bidirektionale Führungsassistenzsysteme, die die gesamte Wirkkette von Entscheidung, Kommunikation, Quittierung, Ausführung und Feedback über alle Führungsebenen abdecken. Beispielhaft zeigt dies das Dashboard zur Visualisierung der Ausrüstungslage der Bundeswehr. Moderne Technologie unterstützt darüber hinaus die Interaktion zwischen System und Nutzer, indem sie unter anderem vor Gefahren durch Unaufmerksamkeit warnt.

Eine wichtige Rolle spielt in diesem Themenfeld zudem der Aspekt der Sicherheit bei der Übertragung und Speicherung der Daten. Unter Berücksichtigung der infrastrukturellen Rahmenbedingungen , historisch gewachsener Merkmale der IT-Landschaft und spezifischer Kundenbedingungen unterstützt Fraunhofer FKIE bei der Konzeption und Implementierung geeigneter Lösungen oder entwickelt diese bis zum einsatzreifen Prototypen. So hält das Institut im Bereich Kommunikation unter anderem Patente an einem Netzwerkprotokoll für die akustische Unterwasserkommunikation und an einem Verfahren zur effizienten und robusten Erkennung von Funkverfahren in Breitband-Quellsignalen.

BUSINESS-INTELLIGENCE-DASHBOARD

INTUITIVE DARSTELLUNG MIT VISUAL ANALYTICS

Prozesse im Bereich Management und Controlling werden aufgrund vielfältiger Abhängigkeiten immer komplexer, die Analyse der – mitunter sehr großen – Datensätze entsprechend aufwändiger. Neue Datenbanktechnologien, wie NoSQL und Graphdatenbanken, ermöglichen innovative Ansätze, interaktive und intuitive Dashboards für die Informationsanalyse und Darstellung zu entwickeln. In einem interdisziplinären Team untersucht die Abteilung »Mensch-Maschine-Systeme« (MMS) des Fraunhofer FKIE wie die Anforderung an eine hohe Flexibilität mit einer einfachen intuitiven Bedienbarkeit vereinbart werden kann.

Motiviert sind diese Forschungsarbeiten durch Anforderungen aus dem Rüstungsmanagement. Das Management für Entwicklung, Beschaffung und Erhalt wehrtechnischer Systeme und Anlagen muss komplexe Zusammenhänge berücksichtigen – sowohl bei Logistik und Finanzplanung, als auch bei der Projektierung neuer Systeme, die in eine bestehende komplexe Systemlandschaft integriert werden müssen. Für das Begreifbarmachen der in den Daten verborgenen Zusammenhänge reichen die üblichen einfachen Visualisierungen wie Kuchen- und Balkendiagrammen nicht aus.

Für die Lösung der Gestaltungsprobleme haben die FKIE-Wissenschaftler um Forschungsgruppenleiter Dr. Carsten Winkelholz ein Experimentalsystem mithilfe eines interdisziplinären Ansatzes erarbeitet. Der verwendete methodische »Visual Analytics«-Ansatz eignet sich besonders dazu, komplexe und große Datensätze so aufzubereiten, dass der Nutzer diese interaktiv analysieren und damit ihren Informationsgehalt erfassen kann, um in der Folge auf dieser Basis adäquate Entscheidungen zu treffen. Mit Hilfe des Experimentalsystems testen die Forscher verschiedene Visualisierungen und Interaktionskonzepte für einzelne Use Cases, um im Endergebnis einen Prototyp des Dashboards zu entwickeln, der flexibel an die Bedürfnisse verschiedener Nutzer angepasst werden kann.

Balance zwischen hoher Flexibilität und klarer Nutzerführung nötig

Basierend auf Graphdatenbanken haben die FKIE-Wissenschaftler ein interaktives Dashboard zur Visualisierung der Ausrüstungslage entwickelt, mit dem neben den üblichen Statistiken auch die Verknüpfung zwischen den verschiedenen Einheiten, wie beispielsweise Projekten und dem Wehrmaterial in Nutzung, dargestellt werden kann. Jede Visualisierung im Dashboard ist interaktiv und erlaubt es dem Nutzer intuitiv neue Filter auf die Daten zu erstellen, sei es durch die Auswahl von einzelnen Projekten in einer Übersichtsdarstellung oder eines Projektstatus in einem Kuchen- oder Balkendiagramm. Alle Änderungen in der Darstellung, die sich aufgrund der Änderung im Filter ergeben, sind durch animiert gestaltete Übergänge leicht nachvollziehbar.

Die Nutzer haben aber ebenso die Möglichkeit, alle Dashboard-Elemente miteinander zu verknüpfen und das dynamische Layout nach ihren Vorstellungen und in Abhängigkeit von ihren Suchanfragen anzupassen, einzelne Attribute hervorzuheben und verschiedene Darstellungsformen zu kombinieren. Diese hohe Flexibilität ist notwendig, um immer wieder neue Sichten auf die Daten zu generieren. Zudem können die klassischen Portfoliodarstellungen um Graphvisualisierungen ergänzt werden, die die Auswirkungen klar nachvollziehbar machen.

Vielfältiger Einsatz zu Lagedarstellung und Monitoring

Neben dem Einsatz für den Bereich »Business Intelligence« können mittels »Visual Analytics« entwickelte Dashboards auch in anderen Bereichen sehr hilfreich sein. So können sie beispielsweise beim Monitoring der Cyber-Lage unterstützen, um eine Übersicht über die präventiven Maßnahmen, aber auch über detektierte Angriffe zu erhalten. Ein weiteres Anwendungsszenario ist das Monitoring von Social-Media-Diensten wie Twitter. Hier lassen sich Nachrichten mithilfe eines derartigen Dashboards etwa schlüsselwortspezifisch darstellen und durchsuchen.

KONTAKT
Dr. Carsten Winkelholz
Telefon +49 228 9435-494
carsten.winkelholz@fkie.fraunhofer.de

FUNKSIGNALERKENNUNG

DIE STECKNADEL IM HEUHAUFEN FINDEN

Schon seit einiger Zeit forscht und entwickelt das Fraunhofer FKIE im Bereich der Funksignalerkennung. Die Expertise der Abteilung »Kommunikationssysteme« (KOM) erlaubt es, Kommunikationssysteme bezüglich Sicherheit, Zuverlässigkeit und Mobilität über alle Schichten der Netzwerkprotokollarchitektur hinweg zu untersuchen. Diese ermöglicht den Entwurf rasch einsetzbarer Kommunikations- und Aufklärungssysteme, die zu einer informationstechnischen Überlegenheit und zu gesteigerten Fähigkeiten führen.

Die Forschungsgruppe »Aufklärung und Störung« untersucht Analog- und Digitaltechniken für moderne Aufklärungssysteme. Ein Schwerpunkt liegt dabei auf der robusten und effizienten Funksignalaufklärung.

Klassifikation digitaler Funkübertragungsverfahren

Ziel der Forscher ist dabei unter anderem, bekannte Funkübertragungen zu detektieren und die Ergebnisse in einem georeferenzierten Lagebild aufzubereiten. Dazu setzen die Forscher der Abteilung KOM verschiedene Methoden zu Erkennung und Klassifikation bekannter wie auch unbekannter digitaler Funkübertragungsverfahren in Breitbandsignalgemischen ein und evaluieren diese im Experimentalaufbau wie auch im Praxistest.

Detektion sogar unter widrigen Bedingungen

So detektiert der von den Wissenschaftlern um die Forschungsgruppenleiter Prof. Dr. Frank Kurth und Alexander Höck entwickelte Musterklassifikator zum Beispiel zeitnah definierte Funksignale in breitbandig aufgezeichneten Signaldaten. Damit können inzwischen auch Signale, die unter dem Rauschen liegen, erkannt werden. Durch den Einsatz moderner Rechencluster ist das System in der Lage, hohe Bandbreiten echtzeitschritthaltend lückenlos zu bearbeiten.

Abgleich mit Musterdatenbank

Dabei basiert das System auf einer Datenbank, in der charakteristische Muster von Zielsignalen abgelegt werden. Während der Analyse der aufgezeichneten Signaldaten werden diese effizient berechenbaren Muster für jede Aufzeichnung bestimmt und mit den Inhalten der Musterdatenbank abgeglichen. So können die Wissenschaftler beispielsweise einmal definierte Signale gezielt in Breitbandaufzeichnungen in großen Frequenzbereichen aufspüren und damit sprichwörtlich die »Stecknadel im Heuhaufen« finden.

KONTAKT
Alexander Höck
Telefon +49 228 9435-622
alexander.hoeck@fkie.fraunhofer.de

ADAPTIVE MENSCH-MASCHINE-INTERAKTION

TECHNOLOGIE PASST SICH DEM MENSCHEN DYNAMISCH AN

Jeder Mensch macht Fehler. Es gibt allerdings Bereiche, in denen sie besonders verheerende Folgen haben können: Nur ein Moment der Unaufmerksamkeit eines Fluglotsen etwa reicht aus, um ein Flugzeug und – noch viel wichtiger – die Insassen zu gefährden. Es sind gerade solche sicherheitskritische Tätigkeiten, die die ganze Aufmerksamkeit des Benutzers erfordern. Jessica Schwarz und Sven Fuchs aus der Abteilung »Mensch-Maschine-Systeme« (MMS) haben eine Technologie entwickelt, durch die ein technisches System den Zustand dieses Lotsen überwachen kann. Bei Nachlassen der Leistungsfähigkeit leitet sie zudem noch die geeigneten Gegenmaßnahmen ein.

Von der messbaren Wirkung zur Ursache

Damit ein technisches System überhaupt erst bemerken kann, dass die Leistungsfähigkeit seines Benutzers absinkt, wird die Mensch-Maschine-Schnittstelle mit zusätzlichen diagnostischen Funktionen ausgestattet: Die Diagnosekomponente überwacht die Leistung des Benutzers und ermittelt im Falle eines Leistungsabfalls mögliche Ursachen. Zunächst einmal wird der Benutzer, etwa der Fluglotse, physiologisch überwacht. Dies kann Aufschluss über Nutzerzustände geben, z. B. hohe Beanspruchung oder Müdigkeit, die sich auf die Leistung negativ auswirken. Für eine ganzheitliche Bewertung werden darüber hinaus weitere Einflussfaktoren in die Analyse einbezogen: die individuelle Erfahrung etwa sowie Art und Anzahl der momentanen Aufgaben.

Damit die Leistungsveränderungen auf ihre Ursachen zurückgeführt werden können, haben Schwarz und Fuchs ihrem Konzept mehrere Dimensionen des Nutzerzustands zugrunde gelegt, die die Leistungsfähigkeit beeinflussen können. Wie genau diese Zustände bestimmt werden können, und welche Abhängigkeiten bestehen, hat Diplom-Psychologin Schwarz in ihrer Doktorarbeit untersucht. So bedeute eine gestiegene Herzrate beim Lotsen nicht automatisch, dass er gestresst sei. Koffeinkonsum könne hier auch eine Erklärung sein. In Echtzeit wird nun ermittelt, wie es dem Fluglotsen geht: Ist er müde, über- oder unterbeansprucht, wie motiviert ist er, wie aufmerksam, wie sind sein emotionaler Zustand und sein Situationsbewusstsein?

Das System greift ein

Bis zu diesem Punkt hat das System eher passiv Daten gesammelt und diese ausgewertet. Durch den Part, an dem Diplom-Informatiker Fuchs gerade arbeitet, wird das System nun selbst aktiv. Stellt es fest, dass die volle Leistungsfähigkeit nicht mehr gegeben ist, leitet es Maßnahmen ein, um dem kritischen Zustand entgegenzuwirken, der als Ursache des Leistungseinbruchs erkannt wurde. So kann der Fluglotse zum Beispiel bei hoher Beanspruchung durch ein Assistenzsystem unterstützt werden. Ist er unaufmerksam, weist das System ihn durch visuelle Hervorhebung auf eine wichtige und dringende Aufgabe hin. Bei Müdigkeit hingegen wird ein akustischer Reiz abgegeben, um den Fluglotsen zu aktivieren. Das System entscheidet situationsabhängig in Echtzeit, welche Maßnahme dem kritischen Nutzerzustand entgegenwirken und den Menschen so bedarfsgerecht unterstützen kann.

Vielfältige Anwendungsszenarien

Die fehlerfreie Bedienung von komplexen Systemen wird immer wichtiger werden, nicht zuletzt, weil ihr Einsatz mit fortschreitender Automation immer weitreichendere Auswirkungen hat. Gerade aus diesem Grund sind die Anwendungsszenarien vielfältig. Überall da, wo es um die Vermeidung von Fehlern bei überwachenden Tätigkeiten geht, kann die dynamische Adaption von Technik helfen. Genauso kann sie im Trainings- und Ausbildungsbereich eingesetzt werden: um die Lerninhalte dynamisch anzupassen, wenn der Lernende unter- oder auch überfordert ist. Denn immer geht es um die bestmögliche Unterstützung des Menschen durch Technik, nicht um seine Verdrängung!

KONTAKT

Jessica Schwarz
Telefon +49 228 9435-491
jessica.schwarz@fkie.fraunhofer.de

Sven Fuchs
Telefon +49 228 9435-393
sven.fuchs@fkie.fraunhofer.de

REHSTRAIN

ASSISTENZSYSTEM WARNT VOR SCHMUTZIGEN BOMBEN

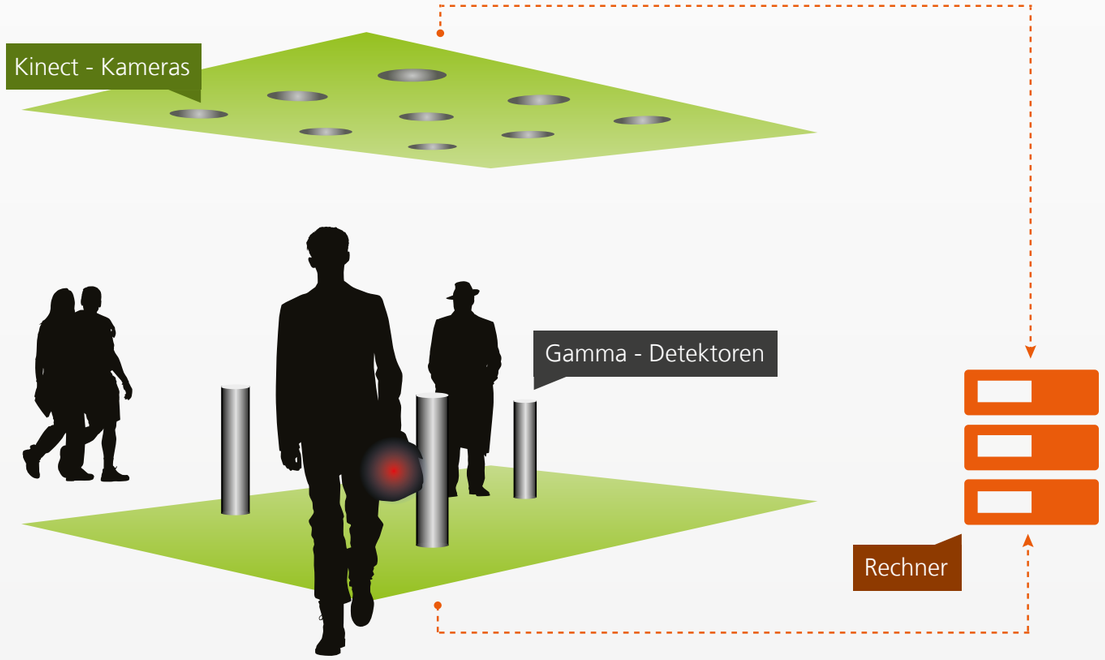
Die Terrorgefahr in Europa hat in den vergangenen Jahren zugenommen. Sorgen bereitet Fachleuten und Politikern der mögliche Einsatz von sogenannten »schmutzigen Bomben«. Ein neues System soll künftig potenzielle Träger von radioaktiven Stoffen sogar in großen Menschenmengen identifizieren. Die Lösung ist eine von verschiedenen Abwehrmaßnahmen, die in dem Projekt »REHSTRAIN« umgesetzt werden. Im Fokus des Vorhabens steht die Sicherheit der deutsch-französischen Hochgeschwindigkeitszüge ICE und TGV.

Experten warnen seit langem vor Anschlägen mit schmutzigen Bomben. Sie befürchten, dass Terroristen konventionellem Sprengstoff radioaktives Material beimischen könnten, das durch die Explosionswirkung verteilt wird. Die Gefahr ist real, der IS gibt beispielsweise an, über radioaktive Stoffe zu verfügen. Die Sicherheitsbehörden sind sensibilisiert.

Schäden in Milliardenhöhe

Die für den Bau von schmutzigen Bomben erforderlichen Radioisotope wie Cäsium 137, Cobalt 60, Americium 241 oder Iridium 192 sind leichter zu beschaffen als spaltbares Material für Kernwaffen – schmutzige Bomben sind keine Kernwaffen, bei deren Zündung ein nuklearer Kettenprozess abläuft: Radioisotope werden in vielen nuklearmedizinischen Abteilungen von Krankenhäusern oder in Forschungszentren genutzt, kommen aber auch für die Werkstoffprüfung in Industrieanlagen zum Einsatz. »Fünf Gramm Cäsium – verteilt mit einigen Kilogramm Sprengstoff – reichen aus, um einen Schaden in Milliardenhöhe zu verursachen, ganz zu schweigen von den psychosozialen und gesundheitlichen Folgeschäden. Zwar riskieren potenzielle Bombenbauer den Strahlentod, das dürfte Terroristen jedoch nicht abschrecken«, so Dr. Wolfgang Koch, Leiter der Abteilung »Sensordaten- und Informationsfusion« (SDF) am Fraunhofer FKIE. Die Entwicklung eines Assistenzsystems, das radiologische Gefährder in einem Personenstrom erkennt und das Sicherheitspersonal alarmiert, ist der Beitrag des FKIE zu »REHSTRAIN«, das die Verwundbarkeit der deutschen und französischen Hochgeschwindigkeitszüge erforscht. Das Fraunhofer FKIE entwickelte das System im Unterauftrag der Hochschule Bonn-Rhein-Sieg.

Das Assistenzsystem setzt sich aus mehreren Komponenten zusammen: einem Sensornetzwerk, handelsüblichen Kinect-Kameras sowie einer Software zur Datenfusion. Das Sensornetzwerk besteht aus Gammaspektrometern, die Gammastrahlen detektieren und klassifizieren. »Die meisten für radiologische Bomben in Frage kommenden Stoffe senden Gammastrahlen aus, die sich nicht abschirmen lassen. Daher bedienen wir uns dieser Art von Sensoren«, erläutert Koch. In der nächsten Ausbaustufe erkennt das System, um welche Substanz es sich handelt, und unterscheidet zudem, ob sie am Körper mitgeführt wird oder ob sie sich im Körper befindet – etwa weil eine Person aus gesundheitlichen Gründen Medikamente wie radioaktives Jod einnehmen muss. Doch obwohl einzelne Sensoren Daten über die Art und Intensität des radioaktiven Stoffs liefern, sind sie nicht in der Lage, ihn zu



lokalisieren. Hierfür ist ein Netz aus verteilten Gammasensoren erforderlich, die mit Kinect-Kameras aus der Spieleindustrie verknüpft sind. Deren Vorteil: Die Kameras liefern neben Bildern auch Entfernungsinformationen. An der Decke montiert nehmen sie Menschenmengen wie ein Hügelgebirge wahr, auf diese Weise können selbst dichte Personenströme präzise getrackt werden. »Wir wissen zu jedem Zeitpunkt wo sich Person XYZ befindet. Die Identität kennen wir natürlich nicht – ein wichtiger Aspekt, was den Datenschutz anbelangt«, so Koch. Die biometrische Erfassung potenzieller Gefährder solle nur nach hinreichendem Verdacht erfolgen.

Identifizierung potenzieller Attentäter

Die derart vernetzten Geräte erfassen Menschen also zeitlich und räumlich, die Daten werden fusioniert. Dank ausgeklügelter mathematischer Auswertealgorithmen werden die gewünschten Informationen aus den riesigen Datensätzen herausgefiltert. »Wir bedienen uns hier künstlicher Intelligenz. Mithilfe der Algorithmen errechnen wir den Bewegungsverlauf einer Person, die allein sich den Messdaten der Gammasensoren zuordnen lässt. Damit ist der potenzielle Attentäter identifiziert«, erläutert der Forscher.

An neuralgischen Punkten angebracht, also in Eingangsbereichen, Auf- und Abgängen von Bahnhöfen, Flughäfen oder anderen öffentlichen Gebäuden, könnten solche Assistenzsysteme künftig Informationen über radiologische Gefährder an die Überwachungssysteme etwa der Verkehrsbetriebe übertragen. Die Frage des Zugriffs obliegt dem Sicherheitspersonal und der Polizei. Die Kontrolle im öffentlichen Raum wäre allerdings nicht die einzige denkbare Anwendung für das Assistenzsystem. Stahlwerke zum Beispiel haben ebenfalls ein großes Interesse daran, dass sie keinen kontaminierten Schrott verarbeiten.

KONTAKT
Dr. Josef Heinskill
Telefon +49 228 9435-630
josef.heinskill@fkie.fraunhofer.de

PROJEKT-HIGHLIGHTS

THEMENFELD II

CYBER- UND INFORMATIONSRAUM

Digitalisierung und Vernetzung durchdringen mittlerweile nahezu alle Lebens- und Arbeitsbereiche. Das bietet Unternehmen, öffentlichen Institutionen und unserer Gesellschaft insgesamt enorme Chancen. Gleichzeitig entstehen dadurch aber auch neue Schwachstellen und Risiken, die vielfach skrupellos ausgenutzt werden und bereits zu erheblichen materiellen und immateriellen Schäden geführt haben. Das Fraunhofer FKIE befasst sich in diesem Themenfeld mit zentralen Fragestellungen einer sicheren Nutzung des Cyber- und Informationsraums. Vorrangig widmet sich das Institut dabei technischen Aspekten. Im Sinne eines ganzheitlichen Ansatzes adressiert es jedoch auch organisatorische und prozessuale Gesichtspunkte.

Im Rahmen seiner Forschungsarbeiten folgt das Institut prinzipiell dem Dreiklang »Prävention – Detektion – Reaktion« und entwickelt geeignete Werkzeuge und Verfahren zum Schutz eigener Systeme. Wesentliche Bausteine sind unter anderem die technische Analyse und Aufklärung von Täterwerkzeugen, die Bewertung der Robustheit (respektive Verwundbarkeit) eigener Systeme und die Entwicklung verbesserter Schutzmechanismen jenseits marktverfügbarer Lösungen. Beispielhaft zu nennen sind hier das aktuelle Firmware Analysis and Comparison Tool (FACT) zur automatisierten Überprüfung von Firmware oder das DG Archive zur frühzeitigen Erkennung möglicher Cyberangriffe.

Wie oben angedeutet erstrecken sich die Untersuchungen auch auf »weichere« Aspekte wie Möglichkeiten eines kooperativen Monitorings über Organisationsgrenzen hinweg oder die Sensibilisierung von Mitarbeitern für Risiken durch unbedarftes Verhalten und unsachgemäße Nutzung von IT-Systemen. Zur Vermittlung von IT-Sicherheitskompetenzen für Fach- und Führungskräfte beteiligt sich das Fraunhofer FKIE seit Frühjahr 2017 gemeinsam mit der Hochschule Bonn-Rhein-Sieg an der Initiative »Lernlabor Cybersicherheit« der Fraunhofer-Gesellschaft. Der Schwerpunkt liegt hier auf den Themen »Hochsicherheit und Emergency Response«.

Im Einklang mit seiner strategischen Ausrichtung kooperiert das Institut im Bereich Cybersicherheit intensiv mit Behörden und Organisationen mit Sicherheitsaufgaben wie beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundespolizei und verschiedenen Staatsanwaltschaften. Selbstverständlich arbeitet es auch eng mit den entsprechenden Verantwortungsbereichen in der Bundeswehr zusammen. Zusätzlich hat Fraunhofer FKIE diverse Projekte zur IT-Sicherheit in den Bereichen zivile Schifffahrt oder Energieversorgung durchgeführt. Die FKIE-Mitarbeiterinnen und -Mitarbeiter leisten hier handfeste, pragmatische Unterstützung im besten Sinne anwendungsorientierter Forschung. An dieser Stelle profitieren die Partner sehr von der Berücksichtigung der Bedürfnisse der Nutzer bei der Konzeption und Entwicklung komplexer technischer Systeme und der aktiven Adressierung ergonomischer Aspekte. Weiterhin verfügt das Fraunhofer FKIE über langjährige Erfahrungen im Umgang mit vertraulichen Daten und Informationen.

PA-SIEM

DATENKLAU – SCHNELL ENTDECKT!

Computerexperten haben bislang kaum eine Chance, Unternehmen oder Behörden dauerhaft vor Netzwerkeinbrüchen zu schützen. Zu zahlreich und wenig aussagekräftig sind die Ereignisse, die auf mögliche Hacker-Angriffe hindeuten. Mit »PA-SIEM« bekommen IT-Verantwortliche ein effektives Werkzeug an die Hand. So können sie Datenklau schneller entlarven und Daten besser schützen.

Bundestag gehackt – diese Meldung sorgte im Jahr 2015 für Schlagzeilen. Das Bedenkliche dabei: Der Datenklau blieb geraume Zeit unbemerkt, nur durch Zufall wurde er entdeckt. 16 Gigabyte Daten, vor allem Dokumente, E-Mails und Tastatureingaben, waren zu diesem Zeitpunkt schon in unbefugte Hände gelangt. Gefahr droht auch Unternehmen und anderen Organisationen. Als Einfallstor dienen den Angreifern häufig Phishing-Emails, über die sie Zugriff auf die Computer der Empfänger erhalten, oder aber sie infizieren regelmäßig besuchte Webseiten. IT-Experten haben dem momentan noch wenig entgegenzusetzen. Zwar laufen in vielen Organisationen Ereignismeldungen in SIEM-Systemen zusammen, kurz für »Security Information and Event Management«. Diese enthalten jedoch riesige Mengen von Meldungen über den täglichen Betrieb – etwa darüber, welche Benutzer sich angemeldet haben oder welche Internetseiten geöffnet wurden. Für die Computerexperten ist es ein Ding der Unmöglichkeit, in der nicht enden wollenden Datenflut die auf einen Einbruch hindeutenden Meldungen zu finden. Ergo: SIEM-Systeme gleichen oft einem Datengrab.

Hinweise in Ereignismeldungen erkennen und korrelieren

Künftig ist es möglich, Netzwerkangriffen schneller auf die Spur zu kommen. Möglich macht es die Software »PA-SIEM«, kurz für »Profilbasierte Anomalieerkennung für SIEM-Systeme«. Entwickelt wird sie von Forschern vom Fraunhofer FKIE gemeinsam mit der Ostbayerischen Technischen Hochschule OTH Regensburg und der NETZWERK GmbH im gleichnamigen Projekt des Bundesministeriums für Bildung und Forschung.

»Statt Angriffe lediglich durch vorher festgelegte Regeln zu erkennen, berechnet ›PA-SIEM‹ typische Angriffsmuster auch aus unvollständigen oder schwachen Hinweisen«, sagt Rafael Uetz, von der Abteilung »Cyber Analysis & Defense« (CA&D) am Fraunhofer FKIE. »Auf diese Weise lassen sich Netzwerkeinbrüche deutlich effektiver und schneller erkennen.«

Die Forscher setzen dabei auf einen dreistufigen Prozess: Zunächst sammelt die SIEM-Software wie bisher die Ereignismeldungen der einzelnen Arbeitsplatz-PCs und Server. Im zweiten Schritt durchsuchen spezielle Algorithmen diese Ereignismeldungen auf bekannte Hinweise sowie auf Anomalien, also auf Abweichungen vom üblichen Verhalten. Die Suchergebnisse können auf einen Einbruch hinweisen, müssen dies aber nicht zwangsläufig. Sendet ein PC beispielsweise plötzlich auffällig viele Daten ins Internet, so kann es sich dabei um einen Einbruch handeln – oder aber der Mitarbeiter schickt lediglich außergewöhnlich große Dokumente an einen Kunden. Systeme, die solche Anomalien erkennen, gibt es bereits. Allerdings haben sie meist eine hohe Falsch-Positiv-Rate. Selbst wenn diese nur bei einem Promille liegt – also eine von hundert Meldungen fälschlicherweise als Bedrohung gesehen wird – laufen bei den Computerexperten je nach Größe des Unternehmens schnell mehrere Tausend Alarme pro Tag auf.

Ereignisketten sind der Weg zum Ziel

»Der Clou liegt quasi im dritten Schritt: Wir kombinieren die Hinweise und können die Fehlerrate somit stark senken«, erläutert Uetz. Ein vereinfachtes Zahlenbeispiel erläutert das: Bei einem Ereignis, das zu 90 Prozent durch einen Angriff ausgelöst wurde, läge die Falsch-Positiv-Rate bei zehn Prozent. Reiht man zwei solcher Meldungen hintereinander – kommt also etwa eine E-Mail mit einem PDF-Anhang an und steigt später die ins Internet gesendete Datenmenge – sinkt diese Rate bereits auf ein Prozent – also auf zehn Prozent von zehn Prozent –, bei einer Dreier-Verknüpfung gar auf 0,1 Prozent. Eine solche Ereigniskette, Experten sprechen von der »Intrusion Kill Chain«, gab es auch im Bundestag: Eine Spear-Phishing-E-Mail installierte Schadsoftware, die anschließend Benutzernamen und Passwörter von Administratoren ausspähte und den Angreifern somit den Weg bereitete, um Daten zu klauen, zu löschen oder zu manipulieren. Mit »PA-SIEM« wäre dies deutlich schneller aufgefallen.

KONTAKT
Rafael Uetz
Telefon +49 228 50212-593
rafael.uetz@fkie.fraunhofer.de

CLOUD COMPUTING

FORSCHEN FÜR DEN KOMPETENZAUFBAU

Die digitale Revolution verändert die Gesellschaft. Riesige Datenmengen, Big Data, sind inzwischen Standard, doch für ihre Verarbeitung sind enorme Rechenleistungen erforderlich. Hier kommt das Thema Cloud Computing als Enabler-Technologie ins Spiel. Seit Ende 2016 arbeitet die Abteilung »Informationstechnik für Führungssysteme« (ITF) des Fraunhofer FKIE gruppenübergreifend am Aufbau einer eigenen Cloud-Infrastruktur.

Zwar ist Cloud Computing kein neues Thema, doch gewinnt es zunehmend an Relevanz – im zivilen, vor allem aber auch im militärischen Bereich. Welche enormen Umwälzungen mit der Nutzung von Cloud-Technologien einhergehen, zeigt sich schon bei der Softwareentwicklung. Hätten Programmierer früher lediglich ihren Quellcode in ein Repository gestellt, werden heute komplexe, vorkonfektionierte Services, sogenannte »Container-Images«, zentral verfügbar gemacht und könnten auf Knopfdruck in der Cloud gestartet werden, so der FKIE-Mitarbeiter Dr. Timm Heuss. »Die Softwarerelease-Zyklen haben sich erheblich verkürzt. Dies erfordert neue Entwicklungsprozesse«.

Cloud Computing für die Bundeswehr

»Unser militärischer Kontext schließt die Nutzung von auf den zivilen Markt ausgerichteten Produkten weitgehend aus. Wir haben daher im letzten Jahr eigene Hard- und Software beschafft, um die Technologie an sich, aber auch ihren Einsatz für verschiedene Anwendungen zu untersuchen«, fasst Dr. Michael Wunder, Leiter der Abteilung, das Bestreben von ITF zusammen. Thomas Kudla, der die Cloud-Arbeiten koordiniert, führt weiter aus: »Gerade die Automatisierung ist in einer immer komplexer werdenden IT-Landschaft von großer Bedeutung. Nur so lassen sich Services mit vertretbarem Administrationsaufwand verwalten, und der Nutzer kann zeitnah auf neue Anforderungen reagieren. Wir können hier wertvolle Erkenntnisse für die von der Bundeswehr benötigten Fähigkeiten sammeln, um diese dann weiterzugeben«. Auch im Hinblick auf die Zusammenarbeit in internationalen Einsätzen sind noch wichtige Fragen ungeklärt: etwa der Aspekt der IT-Sicherheit ebenso wie die Integration von Cloud-Diensten sowie Betrieb und Synchronisation dezentraler Cloud-Services.

Test-Infrastruktur weckt wissenschaftliche Neugier

Fahrettin Gökgöz zum Beispiel hat – in der Zeit, die ihm zum freien Forschen zur Verfügung steht – untersucht, inwiefern eine Spracherkennung mit Deep-Learning-Methoden zu realisieren wäre, um damit ein Führungsinformationssystem (InfoSys) zu steuern. »Deep Learning« erfordert gerade in der Anlernphase enorme Rechenkapazitäten. Mit einer Cloud-Lösung und entsprechender Spezialhardware lässt sich der Rechenaufwand von mehreren Wochen auf wenige Stunden reduzieren.

Jede der fünf Forschungsgruppen der Abteilung verfolgt mit der Cloud ihre eigenen Ziele. Die Wissenschaftler der Forschungsgruppe »Informationsanalyse« von Prof. Dr. Ulrich Schade ergänzen die Analyse großer Datenbestände durch eine robuste Cloud-Lösung so, dass Speicher- und Analyselasten ausgelagert sind. Den Anwendungskontext stellen große Datenbestände textlichen Inhalts, z. B. Twitter-Nachrichten mit den zugehörigen Metadaten dar.

Die Gruppe »Interoperability & Testing« von Dr. Michael Gerz wiederum entwickelt den Prototyp eines interoperablen, hochskalierbaren Führungsinformationssystems. »Die Softwarearchitektur beruht auf denselben Prinzipien und Technologien, die auch Netflix einsetzt. Durch die Microservice-Architektur haben wir die Grundlage geschaffen, um zukünftig den Demonstrator um intelligente Funktionen zu erweitern, z. B. um ontologiebasierte Suchverfahren, die sowohl strukturierte Daten als auch Freitextmeldungen auswerten«, führt Dr. Gerz aus. Eine erste Version konnte im Juni 2017 bei einer internationalen Großübung erfolgreich getestet werden.

Synergien und Wissenstransfer

Auch die Vernetzung der Forschungsergebnisse der einzelnen Gruppen wird mit der Cloud vorangebracht. »Was uns eint, ist ein über alle Nutzer abgestimmtes Vorgehen. Indem jeder seine ›Services‹, also die Ergebnisse seiner Entwicklungsarbeit, verfügbar macht, schaffen wir gruppenübergreifende Synergien«, erklärt Dr. Hanna Geppert, Forschungsgruppenleiterin »Architektur verteilter Führungsinformationssysteme«. Bereits jetzt nutzt ihre Gruppe Lösungen der Sprachverarbeitung aus der Gruppe »Informationsanalyse« für ein intelligentes Anforderungsmanagement. Im Gegenzug unterstützen ihre Mitarbeiter dabei, Services cloud-fähig zu machen und den Deploy-Prozess zu automatisieren.

KONTAKT
Dr. Michael Gerz
Telefon +49 228 9435-414
michael.gerz@fkie.fraunhofer.de

FACT

DIE OFFENE TÜR ZUM UNTERNEHMENSNETZWERK

Computer, Smartphones, Tablets, Server – sie alle werden aufwendig in Unternehmen (mehr oder weniger erfolgreich) geschützt und mit komplexen Sicherheitskonzepten und -richtlinien belegt. Übersehen wird in vielen Firmen und Behörden allerdings oftmals ein Gerättypus, der sich als offene Tür zu dem internen Unternehmensnetzwerk entpuppen kann: der Drucker.

Die Sicherheitsbedrohung durch Drucker mit Netzwerkverbindung ist enorm groß. Das mussten im April 2016 gleich mehrere deutsche Universitäten schmerzlich erfahren, als ihre Drucker Ziel eines Hackerangriffs wurden und rassistische Hetzschriften in zahlreichen Ausgabefächern entdeckt wurden. Allerdings stellt das Drucken bösartiger Inhalte nicht die größte Gefahr von Druckern mit Netzwerkverbindung dar. Vielmehr können Drucker komplett lahmgelegt und sogar gesperrt werden. Hacker können zudem Daten bei der elektronischen Weiterleitung an den Drucker abfangen und sich Zugriffsmöglichkeiten auf Dokumente in der Druckerwarteschlange verschaffen. Haben sie die Kontrolle über den Drucker gewonnen, können die Hacker auch schwerwiegende Angriffe auf das gesamte Unternehmensnetzwerk durchführen und sensible sowie vertrauliche Daten einsehen, manipulieren, stehlen.

FKIE entlarvt Drucker als wunden Punkt in der Unternehmenssicherheit

Exemplarisch hatte Fraunhofer FKIE im Jahr 2016 eine Sicherheitslücke in verschiedenen Xerox-Drucker-Modellen nachgewiesen und damit die Netzwerkdrucker als wunden Punkt in der Unternehmenssicherheit vieler Firmen entlarvt. In bestimmten Konstellationen konnte die neueste Firmware in den Geräten angegriffen werden. Außerdem demonstrierten die Wissenschaftler aus der Abteilung »Cyber Analysis & Defense« (CA&D), dass manipulierte Konfigurationsdateien eingespielt werden konnten, obwohl dies durch ein Administrator-Passwort verhindert werden sollte. Die Firma reagierte und zusätzliche Sicherheitsstandards bei den neuen Geräten wurden eingeführt – nicht betroffen von den Schutzmaßnahmen sind allerdings alle älteren Modelle, was auch für viele Geräte anderer Hersteller gilt. Aber ein Appell der IT-Wissenschaftler geht auch in Richtung der Nutzer: »Deswegen ist es umso wichtiger, dass die Sicherheitskonzepte in der IT-Infrastruktur auch die Druckumgebung umfassen müssen«, so Peter Weidenbach, Experte aus der Abteilung CA&D.

Erpressungstrojaner legt Netzwerkdrucker lahm

Denn auch in den neuesten Modellen wurden wieder Schwachstellen analysiert. »Wir konnten einen Erpressungstrojaner in einem Drucker implementieren, der sich selbst verbreitet«, berichtet Weidenbach von der Suche nach den nächsten Sicherheitslücken, die bei vielen Herstellern in dieser Form existieren. Danach war dieser Drucker nicht mehr nutzbar, und er hat die Schadsoftware über das Netzwerk an die nächsten Geräte weitergeleitet und gleichzeitig ein Lösegeld für die Freischaltung gefordert. »Das betrifft dann nach kürzester Zeit alle Drucker innerhalb eines Unternehmens«, schildert Weidenbach das Szenario, das er mit Hilfe eines entwickelten Demonstrators präsentiert. Der Vorteil für die Hersteller der Geräte sei an dieser Stelle übrigens, dass Experten des Fraunhofer FKIE diese Schwachstellen in ihren Systemen detektieren und die Bedrohungslage offenlegen. Weidenbach: »Viel dramatischer wäre es doch, wenn Kriminelle oder Geheimdienste die Sicherheitslücken entdecken, Unternehmen ausspionieren bzw. lahmlegen und einen großen wirtschaftlichen Schaden anrichten.«

KONTAKT
Peter Weidenbach
Telefon +49 228 50212-563
peter.weidenbach@fkie.fraunhofer.de

EIDI

SCHUTZ VOR DIGITALEM IDENTITÄTSDIEBSTAHL

Identitätsdiebstahl kann heute jeden treffen – und kommt häufiger vor, als man meint: Digitale Identitätsdaten wie Konto- oder Kreditkarteninformationen als auch E-Mail-Adressen und Passwörter werden in großen Mengen von (Cyber-) Kriminellen gesammelt. In den meisten Fällen bemerken betroffene Personen nicht einmal, dass sie Opfer einer Straftat geworden sind. Je nach krimineller Aktivität erfahren sie erst sehr viel später davon, dass sich die Täter unter Verwendung ihrer persönlichen Daten bereichert haben. Bisher gibt es keine erprobte oder standardisierte Methode, mit der Opfer zuverlässig und proaktiv über den Missbrauch ihrer Daten informiert werden können. Reaktive Systeme, wie z. B. der BSI-Sicherheitstest, wurden zwar gut angenommen, setzen aber das Interesse und die Aktivität eines jeden Einzelnen voraus. Das Projekt »EIDI«, an dem FKIE-Wissenschaftler der Abteilung »Cyber Security« (CS) beteiligt sind, soll hier Abhilfe schaffen.

»Eine angemessene, proaktive Benachrichtigung und effektive Warnung betroffener Personen nach der Identifikation eines Diebstahls ist das Kernziel, auf das wir hinarbeiten«, erklärt Prof. Dr. Michael Meier, Abteilungsleiter »Cyber Security« (CS) und Professor am Institut für Informatik 4 der Universität Bonn. »Das erfordert zunächst eine technische Komponente, um die illegal angelegten Identitätsdaten-Sammlungen auf Aktualität und Validität überprüfen zu können. Dies genau ist der Beitrag, den wir mit unserem Team leisten.« Die Wissenschaftler erforschen zu diesem Zweck technische Verfahren, die Identitätsdaten analysieren, fusionieren und korrelieren.

Angemessene und rechtssichere Opfer-Warnung

Im Anschluss daran gilt es, die Betroffenen zu informieren. Die Herausforderung besteht zum einen in einer verständlichen Warnung, die es dem Empfänger ermöglicht, die Art des Missbrauchs seiner Daten zu verstehen und notwendige Schritte einzuleiten. Zum anderen dürfen solche Warnungen nicht zu häufig vorkommen, damit die nötige Aufmerksamkeit erhalten bleibt. Das richtige Maß ist hier entscheidend. Auch diesen Aspekt adressieren die FKIE-Forscher im Sinne der Institutsmaxime »Der Mensch im Mittelpunkt« und gestalten die Art und Weise der Warnung entsprechend nutzergerecht.

Ein dritter, wesentlicher Punkt ist die Rechtssicherheit solcher Warn- und Überprüfungssysteme. Die juristischen Partner im Projekt analysieren deshalb die Vereinbarkeit der Prozesse mit den rechtlichen Rahmenbedingungen und ihre Konformität mit den strengen Vorgaben des Datenschutzrechts der Bundesrepublik Deutschland.

Denkbar ist beispielsweise, dass die Warnung der Opfer digitaler Identitätsdiebstähle im Rahmen des öffentlichen Auftrags einer Behörde durchgeführt werden kann. Dafür ist aber auch zukünftig die Kooperation mit Identitätsdaten-Providern, wie Banken oder sozialen Netzwerken, notwendig. Nur so können die illegalen Datensammlungen zuverlässig bewertet und Betroffene über den Identitätsdiebstahl informiert werden – noch bevor ein Schaden entstanden ist.

Absicherung und Prävention dringend notwendig

Allein in der deutschen Wirtschaft verursacht Computerkriminalität jährlich Schäden von mehr als 10 Milliarden Euro. Eine Absicherung der IT-Systeme gegen Cyberangriffe und Cyberspionage ist daher für die Wirtschaft und Gesellschaft entscheidend, um die Fortschritte und Chancen der Digitalisierung nutzen zu können.

Das geförderte Vorhaben erforscht daher Verfahren, die mittels innovativer forensischer Aufklärungsmethoden Angriffsszenarien untersuchen und verstehen helfen. Gleichzeitig werden mit diesen Erkenntnissen neue Möglichkeiten geschaffen, solche Angriffe bereits im Vorfeld und in Echtzeit zu erkennen und zu verhindern.

KONTAKT
Prof. Dr. Michael Meier
Telefon +49 228 73-54249
michael.meier@fkie.fraunhofer.de

PROJEKTHIGHLIGHTS

THEMENFELD III

AVIATION AND SPACE

Die militärische und zivile Luftfahrt stehen für Spitzentechnologie und Innovation. Dabei spielt die Informations- und Kommunikationstechnologie sowohl für Systemhersteller als auch für Systemintegratoren und industrielle Dienstleister eine entscheidende Rolle. In diesem Themenfeld bündelt das Fraunhofer FKIE alle einschlägigen Aktivitäten der wissenschaftlichen Fachabteilungen mit Bezug zum Thema Luftfahrt und verknüpft spezifische technische Kompetenzen mit einem tiefen Verständnis des Anwendungsgebietes. Hier werden auch alle Aktivitäten zu Einsatz und Abwehr unbemannter fliegender Plattformen (Drohnen) dargestellt, die naturgemäß eine enge Verbindung zum Themenfeld »Information, Entscheidung und Führung« aufweisen.

Einen wesentlichen Schwerpunkt dieses Themenfeldes bildet das echtzeitnahe, interaktive Lagemanagement an Flughäfen. Hier gibt es aufgrund der heterogenen Systemlandschaft, komplexer Prozessabhängigkeiten und schwer vorhersehbarer Störfaktoren einen hohen Bedarf an Monitoring, Koordination und Management. Unter Einbindung verschiedener Abteilungskompetenzen und Technologien ist in diesem Kontext ein sehr leistungsfähiges prototypisches System zur Entscheidungsassistenz entstanden, das an einem großen internationalen Flughafen im Einsatz ist. Die enge Zusammenarbeit mit den Anwendern hat wesentlich dazu beigetragen, ein intuitiv bedienbares Interface mit geringem Schulungsbedarf zu entwickeln. Eine Stärke des Fraunhofer FKIE. Dem Dual-Use-Gedanken folgend arbeitet das Projektteam gegenwärtig daran, diese zivile Anwendung für die spezifischen Anforderungen militärischer Umgebungen zu adaptieren.

Ein weiteres zentrales Arbeitsgebiet dieses Themenfeldes befasst sich mit der Digitalisierung und Integration von Daten im Leistungsverbund Luftverkehr. Der Fokus liegt darauf, die Chancen der Digitalisierung für die Optimierung organisationsübergreifender Prozessketten zu nutzen. Konkret betrifft das beispielsweise die Zusammenarbeit von Airlines, Flughäfen, Bodenverkehrsdiensten sowie diversen IT- und Informationsdienstleistern. Das Fraunhofer FKIE bringt unter anderem seine umfassende Erfahrung und Methodenkompetenz zur Analyse komplexer Prozesse, zur Datenfusion, zur Systemintegration sowie zur Gestaltung von Benutzerschnittstellen ein.

Vor allem für die Bundeswehr relevant sind die Arbeiten des Fraunhofer FKIE zum Schutz von Hubschraubern gegen feindlichen Beschuss. Dabei geht es insbesondere um Sensornutzlast- und Fusionskonzepte zur frühzeitigen Erkennung der Bedrohung.

Das Institut wird seine Aktivitäten in diesem Themenfeld weiter ausbauen, da es neben den skizzierten Beispielen auch für die Bereiche Cybersicherheit und Anwendung von KI-Algorithmen großes Potenzial erkennt.

AMBOS

WENN DROHNEN DROHEN…

Dresden, 15. September 2013: Bei einer CDU-Wahlkampfveranstaltung stürzt eine etwa 40 Zentimeter große Drohne nur wenige Meter vor Bundeskanzlerin Angela Merkel ab. ### **Belgrad, 14. Oktober 2014:** Im EM-Qualifikationsspiel Serbien gegen Albanien zieht eine Drohne eine Flagge für die Gründung eines Groß-Albaniens durch das Stadion. Das Spiel wird wegen Tumulten abgebrochen. ### **Tokio, 22. April 2015:** Auf dem Amtssitz des japanischen Ministerpräsidenten wird eine Drohne mit radioaktivem Material entdeckt. Ihr Pilot möchte mit der Aktion gegen Atomkraft demonstrieren. ### **Zürich, 6. Mai 2017:** Ein vollbesetzter Swiss-Airbus entgeht beim Landeanflug nur knapp der Kollision mit einer viel zu hoch und ohne Genehmigung fliegenden Profi-Drohne.

Die Schlagzeilen über Vorfälle mit Drohnen häufen sich. Sie zeigen: Der einfache und immer preiswertere Zugang zu den ferngesteuerten Luftfahrzeugen konfrontiert Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit neuen Formen von Angriffen. Bedrohungsszenarien wie die von Drohnen, die Explosivstoffe oder gefährliche Chemikalien transportieren und diese über Stadien oder über Massenveranstaltungen zünden oder abwerfen, sind längst nicht mehr abstruse Science Fiction, sondern stellen eine Standard-Gefahrenlage dar. Zu ihrer Erkennung und Abwehr stehen den Sicherheitsorganen bislang jedoch nur unzureichende Forschungsergebnisse zur Verfügung. Um bei der Schließung dieser Sicherheitslücke zu unterstützen, entwickelt das Verbundprojekt »AMBOS« (Abwehr von unbemannten Flugobjekten für Behörden und Organisationen mit Sicherheitsaufgaben) seit Februar 2017 ein System, das Drohnen frühzeitig erkennt, meldet und im Bedarfsfall wirksam abwehrt.

Ziel: Schaffung einer zuverlässigen Abwehrlösung

Koordiniert wird das deutsch-österreichische Kooperationsprojekt durch das Fraunhofer FKIE und das Austrian Institute of Technology (AIT). Gefördert wird es durch das deutsche Programm »Forschung für die zivile Sicherheit« des Bundesministeriums für Bildung und Forschung (BMBF) und das österreichische »Förderungsprogramm für Sicherheitsforschung – KIRAS« des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT). »Durch die aktuell zunehmende Zahl terroristisch motivierter Straftaten besteht auf Seiten der Sicherheitsbehörden dringender Bedarf an rechtskonformen Aufklärungs- und Abwehrmitteln. Gerade vor diesem Hintergrund stellt die Nutzung unbemannter Luftfahrzeuge ein wachsendes Risiko für die öffentliche Sicherheit dar«, so Verbundkoordinator Hans Peter Stuch, Forschungsgruppenleiter am FKIE. »Benötigt werden zuverlässige Werkzeuge und rechtliche Rahmenbedingungen, um der von ihnen ausgehenden Gefahr wirksam zu begegnen. Im Rahmen von ›AMBOS‹ führen wir Expertisen aus Forschung, Industrie und Rechtswissenschaft zusammen, um in Abstimmung mit den Behörden ein solches Instrumentarium zu erarbeiten und unseren Sicherheitsorganen an die Hand zu geben.«

Angestrebtes System übertrifft bisherige Lösungen

Projektziel ist die Entwicklung eines Demonstrators, der über den Funktionsumfang derzeit am Markt verfügbarer Lösungen deutlich hinausgeht. Das System soll herannahende Drohnen mittels vier unterschiedlicher Sensormodalitäten – Funk, Akustik, Elektrooptik/Infrarot und Radar – zuverlässig detektieren. Die eingehenden Sensordaten werden fusioniert, analysiert und zu einem ergonomisch gestalteten Lagebild zusammengesetzt. Dieses unterstützt das Sicherheitspersonal bei der Entscheidung über die je nach Situation und Grad der Bedrohung auszuwählende aktive Maßnahme der Intervention. Die Optionen reichen hierbei vom Stören der Funkfernsteuerung, Satellitennavigation oder Bordelektronik der Drohne bis hin zu ihrem Abfangen mittels eines Netzes.

Wer haftet?

Welche Abwehrmaßnahme letztlich ergriffen wird und der Gefahrenlage angemessen ist, entscheidet der leitende Sicherheitsbeamte vor Ort. Wichtig ist es daher, den Behörden eine zuverlässige Abwehrlösung zur Verfügung zu stellen und ihnen Rechtssicherheit für ihre Entscheidungen zu verschaffen. Denn wer haftet, sollte eine Drohne im Zuge einer solchen Maßnahme abstürzen und Menschen verletzen oder Sachschäden anrichten? Um die Klärung solcher ethischer und rechtlicher Fragestellungen kümmert sich das Forschungsinstitut für öffentliche und private Sicherheit der Hochschule für Wirtschaft & Recht Berlin (FÖPS Berlin).

Enge Kooperation von Forschung, Industrie und Recht mit den künftigen Anwendern

Insgesamt gehören dem Projektkonsortium 16 Partner aus Deutschland und Österreich an. Als künftige Anwender der Lösung sind ihm sechs weitere Partner aus dem Bereich der BOS, darunter das Bundeskriminalamt und die Bundespolizei, assoziiert.

Das Fraunhofer FKIE arbeitet dem Projekt mit drei Forschungsabteilungen in den Forschungsfeldern »akustische Detektion«, »Sensordatenfusion«, »Lagedarstellung« und »Entscheidungsunterstützung« zu. Verbund-Koordinator Hans Peter Stuch: »Mit ›AMBOS‹ leisten wir nicht nur einen wichtigen Beitrag zur Stärkung der zukünftigen nationalen Sicherheit, sondern auch für die europäische Sicherheitsstruktur.«

KONTAKT
Hans Peter Stuch
Telefon +49 228 9435-850
hans-peter.stuch@fkie.fraunhofer.de

PROZESSOPTIMIERUNG

DIGITALISIERUNG FÜR MEHR EFFIZIENZ IN DER LUFTFAHRT

Die Air-Berlin-Insolvenz hat es deutlich gemacht: Luftfahrtunternehmen stehen zunehmend unter Druck. Sie sind einem harten, globalen Wettbewerb ausgesetzt und daher bemüht um effizientere Prozesse zum Erhalt ihrer Wettbewerbsfähigkeit. Voraussetzung dafür ist eine durchgängige Digitalisierung. Das Fraunhofer FKIE unterstützt hierbei mit breitem Know-how bei der Datenintegration, Lagedarstellung, Entscheidungsunterstützung, IT-Sicherheit und ergonomischen Gestaltung von Software.

Fluggesellschaften, Flughäfen, Boden-Abfertigung und andere in die Luftfahrtprozesse eingebundene Unternehmen agieren in einem komplexen Feld von Abhängigkeiten. Zusätzlich erschwert wird ihre effiziente Interaktion durch laufend erforderlich werdende Planänderungen. Diese sind häufig durch äußere Einflussfaktoren, wie z. B. das Wetter oder Verspätungen, bedingt und können bestenfalls prädiziert werden.

Durchgehende Digitalisierung

Voraussetzung für die Erkennung von Auswirkungen dieser Einflussfaktoren sowie für eine Umplanung zur effizienten Nutzung von eigenen und geteilten Ressourcen ist eine durchgehende Digitalisierung der Informationsprozesse. Diese scheitert in der Realität jedoch zumeist an zwei Stellen: Zum einen sind noch lange nicht sämtliche relevante Daten digital verfügbar, sondern werden an vielen Stellen immer noch über Funk, Telefon oder Papier übermittelt. Zum anderen liegen die Daten in unterschiedlichen technischen Systemen vor, die nur aufwendig zusammengeführt werden können.

Integrierte Entscheidungsunterstützung

Das Fraunhofer FKIE setzt an beiden Punkten an: Mittels Vorantreibens der Digitalisierung und der Integration von Daten wird die notwendige Basis für die Anwendung aktueller Methoden der Daten- und Prozessanalyse geschaffen. Erst hierdurch wird die genaue Ermittlung und Nutzung des Optimierungspotenzials möglich. Zusätzlich werden die digitalisierten Prozesse um eine integrierte Entscheidungsunterstützung ergänzt und gewinnen so an Effizienz.

In enger Kooperation mit Partnern aus unterschiedlichen Luftfahrtbereichen wie Herstellern von Teilsystemen, Software-Anbietern und weiteren Forschungseinrichtungen arbeitet das Fraunhofer FKIE an der Optimierung der Entscheidungsbasis für Airlines. Hier müssen beispielsweise Entscheidungen zum Crew- und Flottenumlauf getroffen werden, die sich auf das weltweite Netz einer Airline auswirken.

Die FKIE-Kompetenzen liegen hierbei in der

- Anforderungserhebung und Prozessanalyse
- Plattform- und Schnittstellenspezifikation
- Integration von Daten und Systemen
- Konzeption und Implementierung von IT-Sicherheit
- Datenverknüpfung und -analyse
- Lagedarstellung und Entscheidungsunterstützung
- ergonomischen Informationsdarstellung und Interaktion
- Implementierung von Prototypen

Ziel der Arbeiten ist es, der Luftfahrt deutliche Effizienzsteigerungen zu verschaffen: Neben möglichen Kosteneinsparungen betrifft dies auch die Optimierung von Faktoren wie beispielsweise der Sicherheit und/oder der Pünktlichkeit. Deutschland soll somit ein wichtiger Standortvorteil in der digitalen Transformation verschafft werden.

»Die Arbeiten zur Entwicklung einer Entscheidungsunterstützung für Airlines resultieren aus den Bemühungen, Projekte im Bereich der Digitalisierung und Entscheidungsunterstützung in komplexen Prozessumgebungen weiter auszubauen«, so Arne Schwarze, Leiter der Forschungsgruppe »Systems for Situational Awareness«. »Dabei ist das Potenzial in der Domäne Luftfahrt groß. Auf europäischer Ebene gibt es langjährig entwickelte Konzepte, die nun ihren Weg in die Umsetzung finden. Die Kompetenzen des FKIE ermöglichen dabei, die Lücke zwischen Theorie und praktischer Umsetzung zu schließen und die aus der steigenden Digitalisierung resultierenden Chancen zu nutzen.«

KONTAKT
Arne Schwarze
Telefon +49 228 9435-897
arne.schwarze@fkie.fraunhofer.de

PASSIV

NEUARTIGES RADARSYSTEM FÜR DEN LUFTVERKEHR

Wenn es um die Überwachung des Luftraums geht, eignet sich keine Technologie besser als Radar. Diese aber hat zwei entscheidende Nachteile: Sie ist kostenintensiv und wenig umweltfreundlich, da Radarsysteme elektromagnetische Wellen abstrahlen. Im Rahmen des Projekts »Passivradar zur Steigerung der Sicherheit im Luftverkehr« haben Wissenschaftler des Fraunhofer FKIE in Zusammenarbeit mit der HENSOLDT Sensors GmbH, der Deutschen Flugsicherung und dem Fraunhofer FHR nun eine Alternative untersucht.

Gemeinsam haben sich die Projektpartner der Frage angenommen, inwiefern sich die »grüne« Technologie »Passivradar« für den operativen Einsatz im kritischen Bereich der zivilen Luftraumüberwachung eignet. Hierzu zählen nicht nur die weitreichende Luftraumüberwachung (mögliche Ergänzung des »Air Traffic Managements«), sondern auch die lokale Überwachung für kleine Flughäfen bzw. -plätze, deren finanzielle Ausstattung bisher keine Radare zuließ. Ein weiteres Anwendungsfeld stellt die lokale Überwachung im Falle eines Katastropheneinsatzes dar.

Ziel der Forscher ist es daher, in dem durch das BMWi und dem im Rahmen des fünften zivilen Luftfahrtforschungsprogramms (LuFo V-2) geförderten Vorhaben ein kostengünstiges und modular aufgebautes Passivradarsystem zu entwickeln. Durch das modulare Konzept erhält das System die Flexibilität, um ein breites Einsatzspektrum in der Luftraumüberwachung abzudecken. Um Erkenntnisse zu sammeln und die Technologie zu bewerten, planen die Wissenschaftler den Aufbau eines »hybriden« Systems und seine Erprobung unter realen Bedingungen.

Die grüne Technologie Passivradar

Passivradar ist ein Radarsystem, das ohne eine dedizierte Sendeeinheit auskommt, also keine eigene Abstrahlung aufweist. Stattdessen werden sogenannte Gelegenheitsbeleuchter als Quellen verwendet (z. B. Rundfunk, Mobilfunk etc.). Hybrider Natur ist das geplante System, da es verschiedene Sendetechnologien (FM-Radio, DVB-T, DAB und GSM) verarbeiten kann. Dadurch können die Nachteile der einzelnen Sendearten kompensiert und die Vorteile optimal ausgenutzt werden. Die Wissenschaftler des Fraunhofer FKIE entwickeln im Rahmen des Vorhabens ein mobilfunkbasiertes Passivradar, dessen Fokus im Nahbereich liegt. Darüber hinaus bringen sie ihr Know-how im Bereich des multistatischen Trackings und der Datenfusion ein und sind an der Konzeptentwicklung sowie der Systemintegration beteiligt.

Weiterentwicklung bis zur Markteinführung geplant

Nach Projektabschluss ist geplant, die industrielle Produktentwicklung einer neuen Generation von Passivradaren anzuschließen, in die neben aktuellen Marktanforderungen die Erkenntnisse aus der Entwicklung und den Tests einfließen. Ab 2021 werden die abschließenden operationellen Tests an repräsentativen Flughäfen im In- und Ausland durchgeführt. Eine Markteinführung ist für 2021/2022 geplant.

KONTAKT
Dr. Christian Steffes
Telefon +49 228 9435-456
christian.steffes@fkie.fraunhofer.de

PROJEKTHIGHLIGHTS

THEMENFELD IV

MARITIME SYSTEMS

Seit vielen Jahren befassen sich Forscher des Fraunhofer FKIE mit wissenschaftlichen Fragestellungen zum Schutz und Einsatz maritimer Systeme und Infrastrukturen für militärische und zivile Anwendungen. Die vielfältigen Untersuchungen und Projekte sind im Themenfeld »Maritime Systeme« zusammengefasst. Im Einklang mit der Mission des Institutes sind die Arbeiten vorrangig auf sicherheitsrelevante Aspekte fokussiert. Dazu zählen beispielsweise Assistenzsysteme zur Evakuierung von Kreuzfahrtschiffen oder zur Bewältigung von Havarien auf Seeschiffen, integrierte Sicherheitskonzepte für Hafenanlagen, prototypische Lösungen für Leitzentralen von Fregatten oder Fragen der Cybersicherheit von IKT-Systemen für die Navigation und Steuerung.

Typisch für die Ergebnisse dieser Studien sind sehr realitätsbezogene, praxisrelevante Konzepte, die vielfach Eingang in Produktivsysteme, Prozessmodelle oder verbindliche Rechtsvorgaben gefunden haben. Von enormer Bedeutung sind auch hier Fragen der Cybersicherheit, da Digitalisierung und Vernetzung eine herausragende Rolle bei der Weiterentwicklung der Wertschöpfungsstrukturen in der maritimen Welt spielen. Aus der Perspektive des kompetenten, neutralen Experten haben Wissenschaftler des Fraunhofer FKIE diverse tiefgehende Analysen zur Verwundbarkeit konkreter Systeme durchgeführt. Diese Untersuchungen sind nicht auf technische Aspekte beschränkt, sondern adressieren in einem holistischen Ansatz auch prozessuale und organisatorische Gesichtspunkte.

Zunehmende Bedeutung erlangt sowohl im militärischen wie auch im zivilen Bereich der Einsatz unbemannter Plattformen. Dabei geht es beispielsweise um die Detektion und Beseitigung von Minen, die Kartographierung des Meeresbodens oder die Exploration von Lagerstätten. Das Fraunhofer FKIE entwickelt in diesem Kontext leistungsfähige Technologien zur ressourcenoptimierten Missionsplanung, kommunikativen Anbindung oder eigenständigen Navigation autonomer Systeme.

Neben der Erstellung von IT-Sicherheitsanalysen oder der Entwicklung anspruchsvoller Teilkomponenten für maritime Systeme befasst sich ein Team des Fraunhofer FKE in einem aktuellen Forschungsvorhaben auch mit den Potenzialen der Digitalisierung für die maritime Wirtschaft. Dabei geht es insbesondere um bruchfreie Informationsketten zwischen Frachtschiffen, Hafenbetreibern und Behörden, um die stark effizienzgetriebenen Logistikstrukturen noch wettbewerbsfähiger zu machen. Schließlich sei an dieser Stelle auch auf Forschungsarbeiten verwiesen, die die Möglichkeiten einer sicheren Nutzung der Nordwestpassage für die Schifffahrt unter Beachtung umweltbezogener Aspekte dieses sensiblen Ökosystems untersuchen.

Anhand dieser exemplarisch aufgeführten Arbeitsschwerpunkte lässt sich die Bandbreite dieses Themenfeldes erahnen. Das Fraunhofer FKIE ist aufgrund seiner breiten fachlichen Kompetenz und eines detaillierten Verständnisses dieses Anwendungsfeldes exzellent aufgestellt, eine führende Rolle bei der Bewältigung der anstehenden Herausforderungen zu spielen.

PASSAGES

NEUE ROUTEN SCHIFFBAR MACHEN

Im Jahr 2017, so meint man, sollten doch alle Seewege entdeckt, alle Kontinente der Welt erkundet sein. Wenn jedoch Dr. Wolfgang Koch, Abteilungsleiter »Sensordaten- und Informationsfusion« (SDF) am Fraunhofer FKIE, von dem Mitte 2016 abgeschlossenen Projekt »PASSAGES« spricht, denkt man unweigerlich an unerforschte Gegenden und die Entdeckungsreisen vergangener Jahrhunderte.

Der Hintergrund aber ist ein ganz aktueller: das Schmelzen des vermeintlich ewigen Eises verursacht durch den Klimawandel. Die globale Erderwärmung lässt Permafrostböden auftauen, Gletscher schmelzen und den Meeresspiegel ansteigen. Ein schleichender Prozess, der nicht zuletzt durch die Aufkündigung des Klimaabkommens durch US-Präsident Donald Trump wieder verstärkt in den Fokus der Öffentlichkeit gerückt ist.

Doch der Klimawandel bringt nicht nur extreme Wetterphänomene weltweit mit sich, auch die Landkarte verändert sich: So entstehen durch das Schmelzen des Eises am Nordpol zum Beispiel neue Seewege, die natürlich noch unerforscht und daher mit enormen Gefahren verbunden sind: sowohl für die Schifffahrt zum Beispiel durch Treibeis und unkartierte Untiefen als auch für die Umwelt etwa durch Verklappung oder illegalen Fischfang. Auf der anderen Seite aber locken die wirtschaftliche Erschließung dieses neugewonnenen Raums, kürzere Routen und der Zugang zu Rohstoffen wie Erzen und Mineralien.

Gut 5000 Kilometer sparen

Ein deutsch-kanadisches Forscherteam, darunter Dr. Wolfgang Koch vom Fraunhofer FKIE, hat den ersten Schritt in Richtung der Erschließung dieses neuen Seegebietes gemacht und somit auch technologisches Neuland betreten. Am Beispiel der Nordwestpassage, die den Seeweg nach Ostasien drastisch verkürzt und von Piraterie betroffene Gebiete vermeidet, wurde ein modulares System-Konzept erarbeitet, um das Gebiet zu überwachen und damit erst für den Schiffsverkehr nutzbar machen zu können. Im Projekt »PASSAGES« (Protection and Advanced Surveillance System for the Arctic: Green, Efficient, Secure) sehen sich die Forscher jedoch einigen Herausforderungen gegenüber: Die Größe der Fläche, die aufgrund geringer Besiedelung und fehlender Infrastruktur fast nicht vorhandenen Informationen und Daten zur lokalen Situation, kleinere Boote, die ihre Position bewusst verschleiern und das harsche, fast lebensfeindliche Klima.

Alle vorhandenen Daten durch Fusion nutzbar machen

»Die Schwierigkeit besteht darin, sehr heterogene, unvollständige und auch ungenaue Daten zusammenzuführen, um daraus z. B. Handlungsanweisungen für Kapitäne zu gewinnen, welche Route wann günstig ist«, so Koch. Die Lösung des Problems: Sensordaten- und Informationsfusion, das Fachgebiet von Koch. Unterschiedlichste Datenquellen werden dabei miteinander verknüpft: Satellitendaten, Radar- und Sonardaten, Daten, die dem Schiffsfunk entnommen werden, sowie solche aus geografischen Informationssystemen, aus Eis-, Fischerei- und Umweltdatenbanken – und: Informationen, die via Passiv-Radar gewonnen werden. Die clevere Technik ist für die Informationsgewinnung, was Recycling für Rohstoffe ist, und nutzt den Elektrosmog von Mobilfunkstationen in Küstennähe. Richtig analysiert liefert sie Informationen zu Position, Größe und Geschwindigkeit von Schiffen – und stellt somit eine der innovativsten Datenquellen des Konzepts dar.

Ziel dieses Informationssystems ist jedoch nicht nur die wirtschaftliche Nutzbarkeit für den Schiffsverkehr. Illegalen Aktivitäten wie Schmuggel, illegaler Fischerei oder auch Verklappung kann durch die Überwachung ein Riegel vorgeschoben werden. So leistet »PASSAGES« einen wichtigen Beitrag zum Schutz dieses riesigen ökologisch sensiblen Gebietes, das die Größe von Westeuropa hat.

KONTAKT
Dr. Martin Ulmke
Telefon +49 228 9435-524
martin.ulmke@fkie.fraunhofer.de

EFAS

DIGITALE INFORMATIONEN ZUR SCHIFFSBRAND-BEKÄMPFUNG

Feuer an Bord! Für die Besatzung ein Schreckensszenario. Und für die zuständigen Feuerwehren eine große Herausforderung. Denn Brandbekämpfung auf Schiffen ist nicht mit der an Land zu vergleichen: So unterscheiden sich die Begebenheiten aufgrund unterschiedlicher Schiffsgrößen mit ihren diversen Decks sehr stark. Zudem erschweren Wände aus Stahl den Funkverkehr zwischen Einsatzleitung und Einsatzkräften. Löschwasser kann nur begrenzt eingesetzt werden, da sonst das Schiff Schlagseite bekommen könnte. Enge und lange Korridore sowie schmale Luken lassen Feuerwehrleute oftmals nur langsam vorankommen oder sorgen für einen starken Kamineffekt, über den sich das Feuer schnell ausbreitet. Gerät allerdings ein im Hafen liegendes Schiff in Brand, kommt eine zusätzliche Problematik hinzu: Die Zuständigkeit liegt bei der landseitigen Feuerwehr, die für Brände auf Schiffen jedoch nicht umfangreich ausgebildet ist.

Um die Wehrleute bei einem solchen Großeinsatz im Hafen aktiv zu unterstützen, arbeitet das Fraunhofer FKIE an dem vom Bundesministerium für Bildung und Forschung geförderten Projekt »EFAS« als koordinierender Projektpartner mit: »EFAS« steht für »Einsatzunterstützungssystem für Feuerwehren zur Gefahrenbekämpfung an Bord von Seeschiffen«. Projektträger ist das VDI Technologiezentrum. Wissenschaftler aus dem Team um Dr. Daniel Feiser, stellvertretender Leiter der Forschungsgruppe »Organisationsergonomie« in der Abteilung »Mensch-Maschine-Systeme« (MMS) am Fraunhofer FKIE, erarbeiten in enger Kooperation mit verschiedenen Verbund- und assoziierten Partnern das System mit dem Ziel, die Sicherheit, die Effizienz und die Effektivität der Feuerwehr zu erhöhen. Hierzu sollen die Einsatzkräfte mit technologischen Neuentwicklungen für die Gefahrenbekämpfung an Bord optimal ausgestattet werden.

Sicheres Funksystem ermöglicht Kommunikation

Neben der Ortung der Feuerwehrleute im Inneren des Schiffes werden auch Körper- und Umgebungstemperatur an die Einsatzleitung übermittelt. So kann mithilfe von Sensoren, die sich in der Schutzkleidung der Einsatzkräfte an Bord befinden, die Temperaturverteilung unter Deck und daraus ggf. die Lage des Brandherdes lokalisiert werden. Hinzu kommt ein sicheres und robustes Funksystem, das die Kommunikation ins Schiffsinnere sicherstellt. Der Einsatzleiter an Land erhält über ein Darstellungssystem somit permanent ein elektronisches Lagebild angezeigt, das ihm Handlungsoptionen vorschlägt. Dies erfolgt über Brandmelde-, Brandbekämpfungs- und Sicherheitssysteme sowie über konkret ausgewählte Brandszenarien, die als Basis für das Entscheidungsunterstützungssystem zu Rate gezogen werden.

Gefahrgüter erschweren die Brandbekämpfung

Zusätzlich zu dem deutlich verbesserten Schutz für die Einsatzkräfte steht auch die Sicherheit für die unmittelbare Umgebung der im Hafen liegenden Schiffe im Fokus der Wissenschaftler. Ein Übergreifen des Feuers auf benachbarte Schiffe wie auch Infrastrukturen an Land und die Gefährdung von Menschen gilt es zu verhindern. So sich Gefahrgüter an Bord befinden, erschweren diese die Brandbekämpfung und Löscharbeiten ganz erheblich. Allerdings können allein schon die an Bord befindlichen Kraft- und Betriebsstoffe die Gefahrenlage für die Feuerwehrleute wie auch für die nähere Umgebung deutlich verschärfen.

Neben dem Szenario Feuer beschäftigt sich »EFAS« auch mit der Situation, dass ein Gefahrstoff an Bord austritt und die Feuerwehr ausrücken muss. Dafür werden Gefahrstoffsensoren von einem Projektpartner in die Bekleidung der Einsatzkräfte integriert. »Auch diese Informationen werden im Lagedarstellungssystem visualisiert und zur Entscheidungsunterstützung bereit gestellt«, erklärt Feiser das Vorgehen.

Zur besseren Visualisierung der Gefahrenlage erstellt das Team um Dr. Feiser zwei Typen von Systemen: Sämtliche Informationen zum Lagebild werden im stationären System des Einsatzleitwagens visualisiert. Mobile Systeme werden hingegen den Gruppenleitern und dem Einsatzleiter an Bord des Schiffes zur Verfügung gestellt. Via Tablets erhalten sie alle relevanten Angaben über das Vorankommen und die Brandbekämpfungsmaßnahmen ihrer Einheiten im Einsatz. Der Vorteil: »Die mobilen Systeme werden so konzeptioniert, dass Empfänger nur die für sie relevanten Informationen erhalten, wodurch die Einsatzkräfte weniger belastet werden«; erläutert Dr. Feiser.

Dem Projekt, das bis 2019 ausgelegt ist, steht die Feuerwehr Wilhelmshaven als assoziierter Partner zur Seite. Geplant ist allerdings, auch weitere Feuerwehren zu der Anwendung von »EFAS« zu befragen. Insgesamt sieht das Konzept sogar vor, Einsatzunterstützungssysteme auch auf andere Einsatzorte zu übertragen. Dr. Feiser: »Das langfristige Ziel ist, ›EFAS‹ nicht nur für Schiffe im Hafen anzuwenden, sondern zum Beispiel auch auf Schiffen auf hoher See, für die Brandbekämpfung in Stadien, Industrieanlagen oder in öffentlichen Gebäuden.«

KONTAKT
Dr. Daniel Feiser
Telefon +49 228 9435-403
daniel.feiser@fkie.fraunhofer.de

PROJEKTHIGHLIGHTS

THEMENFELD V

LAND SYSTEMS

Seine vielfältigen Forschungsarbeiten zu landbasierten Systemen führt das Fraunhofer FKIE im Themenfeld »Land Systems« zusammen. Wie auch in den Anwendungsfeldern Luft- und Schifffahrt geht es hierbei in erster Linie um die Entwicklung spezifischer Informations- und Kommunikationstechnologie, die einen effektiven Einsatz oder angemessenen Schutz beweglicher Plattformen auf der Straße, im Gelände oder auf der Schiene unterstützt.

Herausragend am Fraunhofer FKIE sind die sehr praxisorientierten Untersuchungen und Konzepte zur Steuerung autonomer, fahrender Systeme. Die Landroboter werden durch die Einbindung leistungsfähiger Sensorik und »intelligenter« Algorithmen befähigt, geplante Missionen in hoher Eigenständigkeit durchzuführen und sogar im Verbund zu handeln. Auf diese Weise unterstützen sie Einsatzkräfte bei gefährlichen Arbeiten (z. B. Bergung von Verletzten oder Bekämpfung von Bränden), übernehmen zeitaufwendige Routineaufgaben (z. B. Inspektion oder Monitoring) oder dienen als Transportmittel zur Beförderung von Lasten (z. B. Ausrüstung oder Ersatzteile). In diesem Bereich zählt das Fraunhofer FKIE zu den führenden Forschungseinrichtungen in Europa und erzielt in den einschlägigen Leistungsvergleichen wie ELROB regelmäßig überragende Ergebnisse.

Ein weiteres wichtiges Arbeitsgebiet in diesem Themenfeld widmet sich der Unterstützung des Nutzers bei der Interaktion mit den mobilen Systemen, beziehungsweise mit deren funktionalen Komponenten. Hier geht es beispielsweise um innovative Konzepte bei der Bedienung von Nutzfahrzeugen oder um die Einbindung optischer Sensorik zur Verbesserung der Sicht in gepanzerten Fahrzeugen. Dabei müssen auch physiologische und psychische Aspekte unter Dauerbelastung oder in Stresssituationen berücksichtigt werden. Zu diesem Zweck betreiben die entsprechenden Fachabteilungen des Fraunhofer FKIE verschiedene Labors und Testumgebungen zur Nachstellung realitätsnaher Anwendungsszenarien. In deren Mittelpunkt müssen nicht zwangsläufig angetriebene bewegliche Plattformen stehen. Vielmehr ist auch die Nutzung moderner Technologien wie Virtual Reality oder Augmented Reality als Teil der persönlichen Ausrüstung von Einsatzkräften ein wesentlicher Forschungsbereich mit hoher Bedeutung für militärische und zivile Einsatzumgebungen.

In Analogie zum Schutz schwimmender und fliegender Plattformen stellt auch der Schutz landbasierter Systeme und der damit verbundenen Verkehrsinfrastrukturen gegen physische Angriffe einen wesentlichen Forschungsschwerpunkt am Fraunhofer FKIE dar. Hier geht es unter anderem um den Betrieb heterogener Sensornetze zur Gefahrendetektion wie dem Aufspüren von Sprengstoffen oder radioaktivem Material an stark frequentierten Infrastrukturknoten (z. B. Bahnhöfe, Hafenanlagen oder Airports). Im militärischen Kontext spielen die Beschussdetektion oder die Unterdrückung improvisierter Sprengfallen eine wichtige Rolle. Wie auch in den anderen Themenfeldern arbeiten die Forschungsabteilungen des Fraunhofer FKIE bei der Bewältigung dieser Aufgaben eng zusammen, um praxisnahe und anwendungsorientierte Lösungen zu entwickeln.

PAA

INFORMATIONSÜBERLEGENHEIT DURCH TAKTISCHES TEAMING

Sie bilden ein Team mit den Soldaten und unterstützen sie im Einsatz: Unbemannte Systeme, die den Soldaten auf vielfältige Weise zur Seite stehen. In dem Forschungsprojekt »Prozesskette Automatisierte Aufklärungsunterstützung« am Fraunhofer FKIE wird gezeigt, wie perfekt abgestimmte »Künstliche Intelligenz« bei Unbemannten Systemen für eine Informationsübergelegenheit gegenüber Angreifern sorgt.

Dabei steht den Soldaten eine bestimmte Anzahl Unbemannter Systeme zur Seite, insbesondere um ihnen bei der Aufklärung gefährlicher Umgebungen zu assistieren. Das Fraunhofer FKIE hat als langjähriger strategischer Partner des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw), mit dessen Zuwendung dieses Projekt durchgeführt wurde, eine Unterstützungsarchitektur geschaffen, die durch zusätzliche Aufklärungsergebnisse den Schutz der Soldaten maßgeblich erhöht.

»KI« sorgt für eine spürbare Entlastung der Soldaten

Bei dem Projekt »PAA« werden neben Bodenrobotern (Unmanned Ground Vehicles, UGV) auch fliegende Systeme (Unmanned Aerial Vehicles, UAV) eingesetzt, die mithilfe der rückgemeldeten Informationen über das Lagebild den Soldaten eine erhebliche Informationsüberlegenheit garantieren. Der Einsatz »Künstlicher Intelligenz« führt an dieser Stelle zu einer deutlichen Ergänzung der Fähigkeiten und gleichzeitig zu einer spürbaren Entlastung der Soldaten. Voraussetzung hierfür ist, dass die Unbemannten Systeme mit geringem Aufwand eingesetzt werden können. Dies ermöglichen die vom Fraunhofer FKIE entwickelten, an den Bedarf der Soldaten angepassten Endgeräte sowie gleichzeitig die hohe Autonomie der Systeme.

Der simultane Einsatz verschiedener Roboter bringt ebenfalls einen großen Mehrwert für Missionen mit sich, da neben den übertragenen Aufklärungsdaten über die Umgebung auch mit Hilfe der Fusion der jeweiligen Sensordaten Personen und Fahrzeuge detektiert werden können. Zudem ermöglichen die Systeme eine akustische Schützendetektion und Schützenpeilung. Die Unbemannten Systeme sind als eigene Gruppe automatisiert in die Aufklärungsmission eingebunden und versorgen ein Führungsinformationssystem über die Battle Management Language (BML) mit den entsprechenden Informationen zur Einsatzlage in Echtzeit.

Kernkompetenzen aus sechs Abteilungen

Ein herausragendes Beispiel für ein Projekt am Fraunhofer FKIE ist »PAA«, bei dem unterschiedliche Forschungsbereiche ihre Kernkompetenzen in einem System zusammengefasst haben.

Koordiniert wird »PAA« von der Abteilung »Kognitive Mobile Systeme« (CMS). Ihr Forschungsschwerpunkt liegt auf dem »Teaming« (KI) mit heterogenen Mehr-robotersystemen. Durch CMS wurde auch die Steuerung der UGV entwickelt, die die Aufklärungsdaten aus der Bodenperspektive liefern. Die Abteilung »Sensordaten- und Informationsfusion« (SDF) hat die Einbindung der UAV übernommen. Bei ihnen

werden Tageslicht- und Infrarotsensoren eingesetzt, die Personen im Bild erkennen und ihre Position in einem Koordinatensystem bestimmen. Gleichzeitig werden alle erkannten Personen »getrackt« und zur Darstellung im Echtzeit-Lagebild gemeldet. Weiterhin ist SDF für die Schussdetektion und Peilung verantwortlich.

Die Kommunikationsinfrastruktur wurde von der Abteilung »Kommunikationssysteme« (KOM) konzipiert und realisiert. Hierfür wurde die LTE-Technologie ausgewählt. Mit dem Aufbau und Betrieb eines eigenen autarken mobilen LTE-Netzes wird gezeigt, dass die zivile LTE-Mobilfunktechnologie das Potenzial für einen solchen Einsatz besitzt. Die Abteilung »Informationstechnik für Führungssysteme« (ITF) hat für »PAA« ein mobiles Führungssystem entwickelt, das es mittels BML erlaubt, mit den Unbemannten Systemen im Sinne der Auftragstaktik zu kommunizieren. Dies hat den Vorteil, dass ein einzelner Soldat die gesamte Gruppe der Unbemannten Systeme führen kann, auch wenn sich die Zusammensetzung der Gruppe im Einsatz noch verändert.

»PAA« ermöglicht intuitive Nutzung der Geräte

Der Beitrag der Abteilung »Mensch-Maschine-Systeme« (MMS) lag darin, die Anforderungen der Nutzer zu erfassen, Benutzeroberflächen für verschiedene Endgeräte zu gestalten und die Qualität der Interaktion abschließend mit Nutzern durch Usability-Tests und Befragungen zu evaluieren. Ein besonderer Fokus lag dabei auf dem Fahrzeugarbeitsplatz. Dies erfolgte gemeinsam mit der Abteilung »Human Factors« (HF), die sich auf die Erstellung des Anzeige- und Bedienkonzeptes für die mobilen Endgeräte konzentrierte. Weiterhin wurden auch die Hardware-Aspekte wie Anbringung und Trageweise der Geräte betrachtet.

Der Erfolg von »PAA« zeigte sich unter anderem darin, dass die Soldaten die Geräte und damit auch die Unbemannten Systeme intuitiv und ohne große Einweisung direkt nutzen können. Die unterstützenden Möglichkeiten der Systeme wurden dabei unmittelbar deutlich.

KONTAKT
Dr. Bernd Brüggemann
Telefon +49 228 9435-364
bernd.brueggemann@fkie.fraunhofer.de

CBRNE-ROBOTER

AUF DER SUCHE NACH TÖDLICHEN GEFAHRSTOFFEN

Es war das stärkste Erdbeben in der japanischen Geschichte: Die Seismographen zeigen am 11. März 2011 den hohen Wert von 9,0 Mw an. Über eine Länge von 400 Kilometern reißt im Nordosten Japans die Erdkruste auf dem Meeresgrund auf. Teile der Küste verlagern sich um bis zu 50 Meter nach Osten. Im Atomkraftwerk Fukushima ereignen sich in der Folge gewaltige Explosionen in drei Reaktorgebäuden. Doch wie ist die Lage heute – mehr als sechs Jahre danach? Antwort: Erschreckend unklar. Denn die robotischen Systeme sind aktuell noch nicht auf dem technologischen Stand, den das Einsatzszenario des AKW in Fukushima erfordert. Dabei ist dieses nur eines von vielen realen und/oder möglichen Beispielszenarien, in denen autonome CBRNE-Aufklärung dringend gefragt ist.

Bereits seit einigen Jahren forschen die Wissenschaftler der Abteilung »Kognitive Mobile Systeme« (CMS) des Fraunhofer FKIE im Bereich der CBRNE-Aufklärung. CBRNE steht für »Chemical, Biological, Radiological, Nuclear and Explosive«. Darunter fallen beispielsweise auch aggressive Gefahrstoffe und radioaktive Verstrahlung, welche die Streit- und polizeilichen Sicherheitskräfte im Einsatzfall vor extreme Herausforderungen stellen. Eine Gefahr für Leib und Leben kann hierbei trotz richtiger Ausrüstung und intensiver Schulung nie vollkommen ausgeschlossen werden. Roboter, die mit CBRNE-Sensorik und autonomen Assistenzfunktionen ausgestattet sind, können hier unterstützen. Sie erfüllen Aufgaben, die Menschen aufgrund des hohen Risikos keinesfalls übernehmen können.

Präzise Detektion, Lokalisierung und Kartierung von Gefahrstoffen

Zu diesem Zweck verknüpfen und koordinieren die Wissenschaftler Sensordaten, die Erkundungsroboter im Hinblick auf die Erkennung von CBRNE-Gefahrstoffen liefern, mit Navigationsstrategien und Zusatzinformationen aus digitalen Geo-Datenbanken. Falls nicht alle Bereiche eines Areals vom Roboter erkundet werden können, steht basierend auf den gesammelten Daten ein geostatistisches Schätzverfahren zur Verfügung, das die Kontaminierung an fehlenden Stellen ergänzt. Gefahrenquellen können somit genauer detektiert, lokalisiert sowie – für die Einsatzkräfte besonders wichtig – präzise kartiert werden. Die unterschiedlichen Daten werden hierfür zu einem gemeinsamen Lagebild fusioniert.

Der Fokus der Tests lag bislang auf RN-Sensorik, das heißt auf Sensoren zur Erkennung radioaktiver und nuklearer Stoffe. Durch ein speziell entwickeltes gemeinsames Datenformat können jedoch jederzeit und mit überschaubarem Aufwand weitere Sensoren mit dem System verknüpft werden.

Nachhaltige Entscheidungsunterstützung des Operators

Sämtliche gesammelte und berechnete Daten werden dem Leitstand zur Verfügung gestellt. Dieser erhält so eine flächendeckende Kontaminierungskarte. Der verantwortliche Nutzer kann darin wählen, ob er alle verfügbaren Daten oder eine auf die einsatzbedingt relevanten Daten vorgefilterte Ansicht angezeigt erhalten möchte. »Der Operator hat so die Möglichkeit, einzelne Sensoren auszuwählen und sich die unterschiedlichen Kontaminierungs- und Geokarten transparent übereinander legen zu lassen«, erläutert Dr. Frank E. Schneider, stellvertretender Abteilungsleiter CMS, die flexiblen, nutzenfokussierten Funktionen des Systems. »Das sich daraus ergebende kartierte Lagebild kann somit beispielsweise zur Planung der schnellsten, sichersten und kontaminierungsärmsten Strecke durch das Areal genutzt werden. Der Operator wird dadurch nachhaltig in seinen Aufgaben entlastet.«

Neben der theoretischen Erforschung erfolgt dies mithilfe von Simulationen und Experimentaluntersuchungen mit einem Unmanned Ground Vehicle (UGV), das mit entsprechender Sensorik ausgestattet ist. Ebenfalls werden reale Testszenarien erprobt: so zum Beispiel beim europäischen Roboterwettbewerb »EnRicH« im österreichischen AKW Zwentendorf, bei dem ein Unfall in einem Kernkraftwerk simuliert wurde. Dem FKIE-Roboter gelang es hier als einzigem der teilnehmenden Systeme, autonom nach den mit radioaktivem Material gefüllten Zylindern zu greifen, diese zum Strahlendetektor zu führen und in dem dafür vorgesehenen Behälter abzulegen.

KONTAKT
Dr. Frank E. Schneider
Telefon +49 228 9435-481
frank.schneider@fkie.fraunhofer.de

UNIMOG

OPTIMIERTES INTERAKTIONS-KONZEPT FÜR DEN UNIMOG

Der allradgetriebene Geräteträger von Mercedes-Benz Special Trucks ist im öffentlichen Bild omnipräsent. Kein anderes Fahrzeug setzen Kommunen so gerne für Grünflächenarbeiten oder den Winterdienst ein wie ihn. Im Auftrag der Daimler AG hat sich im Jahr 2017 auch ein Team der Abteilung »Human Factors« (HF) des Fraunhofer FKIE fünf Monate lang intensiv mit dem Nutzfahrzeug befasst. Da aktuell neue, innovative Technologien auch für den Unimog verfügbar werden, sollte das Bedienkonzept zur Inbetriebnahme und Steuerung der Anbaugeräte einer umfassenden Effizienzüberprüfung unterzogen werden. Im Juli 2017 wurde das Projekt erfolgreich abgeschlossen. Zusammen mit Mercedes-Benz wurden Handlungsempfehlungen festgelegt, die die nächste Generation des Fahrzeugs sowohl bedientechnisch als auch ergonomisch noch einfacher und komfortabler werden lassen sollen.

»Die besondere Herausforderung lag darin, dass bei diesem Fahrzeug sehr, sehr viele Faktoren ineinandergreifen, die berücksichtigt werden mussten«, erklärt Projektleiter Björn Nord, Senior Systems Engineer beim Fraunhofer FKIE in Bonn. Denn der Unimog, kurz für Universal-Motor-Gerät, wird für seine Arbeitseinsätze in der Regel mit Anbaugeräten bestückt, wie zum Beispiel einem Mäh- oder Mulchgerät, einer Astschere für Lichtraumprofilschnitt oder einem Schneepflug. Die zugehörigen Steuergeräte für diese Funktionen kommen zu dem ohnehin bereits umfangreichen Arsenal an Schaltern im Cockpit noch hinzu.

Weiterhin hat der Fahrzeugführer für jeden einzelnen Einsatz zu Beginn eine Vielzahl von Bedienschritten durchzuführen (z. B. die Aktivierung von Hydraulikkreisen), die nach Ende des Arbeitsvorgangs in umgekehrter Folge erledigt werden müssen. So auch bei jeder einzelnen Pause.

Automatisierung von Bediensequenzen

Um sich für die Analyse von Nutzerkontext und -anforderungen ein maximal praxisnahes Bild zu verschaffen, hat Nord zunächst umfangreiche Interviews mit Mitarbeitern verschiedener Straßen- und Autobahnmeistereien geführt. Zudem ist er etliche Arbeitseinsätze der Straßenmeistereien mitgefahren. »Neben den Befragungen haben wir mithilfe von Kameras die Arbeitsabläufe im Fahrzeug gefilmt und später genau analysiert«, erklärt der Ingenieur das Vorgehen.

Bei der gemeinsamen Auswertung der Daten mit dem Auftraggeber ergab sich dann die Idee, immer wiederkehrende Sequenzen von Bedienschritten zu automatisieren. Die Bedienelemente im Cockpit, die größtenteils in der Mittelkonsole untergebracht sind, könnten auf diese Weise reduziert und die Bedienung des Fahrzeugs nochmal deutlich vereinfacht werden. Auch Mitarbeiter, die nicht jeden Tag auf dem Unimog arbeiten, könnten so noch flexibler für den Dienst mit dem Allzweckfahrzeug eingesetzt werden.

Verbesserte Ergonomie

Unter ergonomischen Gesichtspunkten fiel bei der Analyse unter anderem auf, dass die Elemente für die Bedienung der Funktionen der Anbaugeräte aufgrund der Wechsellenkung in der Mitte der Unimog-Kabine angebracht sind – aus Fahrerperspektive entsprechend weit außen. Der Führer des Wagens muss aus diesem Grund, egal ob er links oder rechts sitzt und steuert, was durch die Wechsellenkung des Unimog problemlos möglich ist, jeweils in Richtung Fahrzeugmitte greifen. Nach ergonomischen Kriterien wäre es besser, die Bedienelemente näher am Fahrer anzubringen, am besten noch abhängig von der jeweiligen Schulterbreite. Dies ist insbesondere für längere Dienste in Stoßzeiten vorteilhaft.

Die Projektergebnisse wurden den Mercedes-Benz-Entwicklungsingenieuren mittels Workshops in regelmäßigen Intervallen vorgestellt und diskutiert. Der Daimler AG liegt nun seit Abschluss des Projekts Ende Juli 2017 ein Konzeptansatz zur Optimierung sowie eine Liste von Empfehlungen für das weitere Vorgehen vor. Das Unternehmen hat bereits angekündigt, dass es auch bei künftigen Nutzeranalysen und -tests gern auf die Unterstützung des Fraunhofer FKIE zurückgreifen würde.

KONTAKT
Björn Thorsten Nord
Telefon +49 228 50212-439
bjoern.thorsten.nord@fkie.fraunhofer.de

MEILENSTEINE

JAHRESHIGHLIGHTS

FKIE präsentiert sich erfolgreich auf der DWT »Angewandte Forschung für Verteidigung und Sicherheit 2016«

Alle zwei Jahre findet mit der DWT-Konferenz eine der wichtigsten Veranstaltungen im Bereich der wehrtechnischen Forschung in Bonn statt. So auch vom 23. bis 25. Februar 2016.

Hoher Besuch am Messestand: Konteradmiral Thomas Jugel, Amtschef des Planungsamtes der Bundeswehr, informierte sich zu aktuellen Entwicklungsergebnissen des Instituts und ließ sich von FKIE-Wissenschaftlern das Projekt »Prozesskette automatisierte Aufklärung« (PAA) vorstellen.

Der Amtschef des Planungsamtes der Bundeswehr zeigte sich von dem Projekt beeindruckt und lobte insbesondere den gemeinsam mit der Bundeswehr durchgeführten Test des Systems unter Realbedingungen.

Fast jede der zehn, fachlich sehr unterschiedlich ausgerichteten Abteilungen des Fraunhofer FKIE war an dem Projekt beteiligt, sodass im Ergebnis eine systemische Lösung entstanden ist, die die Automatisierung über die gesamte Prozesskette hinweg gewährleistet. »Ziel des Projektes war, mehrere heterogene Robotersysteme in die Lage zu versetzen, ihre Sensordaten untereinander auszutauschen, ihre Informationen mit einem Führungsinformationssystem zu teilen und Daten zu aggregieren«, erklärte Projektleiter Dr. Bernd Brüggemann. »Durch das Zusammenspiel mit den Soldaten sollen bei einer Aufklärungsmission höherwertige Informationen gewonnen werden«, so Brüggemann. Dadurch sei es möglich, das System in einen Infanteriezug zu integrieren und die Zusammenarbeit von Menschen und Robotern optimal zu gestalten.

Neuer Standort des Fraunhofer FKIE in Bonn

Prominent war die Riege der Redner, die anlässlich der feierlichen Eröffnung des neuen Institutsstandortes des Fraunhofer FKIE erschienen waren. Der Bürgermeister der Bundesstadt Bonn Reinhard Limbach, der Rektor der Universität Bonn Prof. Dr. Dr. h.c. Michael Hoch, und Dr. Beate Wieland Abteilungsleiterin im Ministerium für Innovation, Wissenschaft und Forschung des Landes NRW, hielten Grußworte bei der Feier am 25. Mai 2016 im neuen Gebäude in der Zanderstraße 5 in Bonn.

»Seit wir im Jahr 2009 Teil der Fraunhofer-Gesellschaft wurden, hat sich die Anzahl der Mitarbeitenden von annähernd 200 auf etwa 400 verdoppelt«, erklärte Institutsleiter Prof. Dr. Peter Martini. Dieser Umstand habe es notwendig gemacht, mit einigen Abteilungen und Forschungsgruppen an einen weiteren Institutsstandort umzuziehen. »Wir bleiben dadurch attraktiv für unsere Mitarbeitenden«, begründete der Institutsleiter seine Entscheidung weiter, »und bringen auch unser Bekenntnis zum Standort Bonn als Zentrum der IT-Sicherheitsforschung zum Ausdruck.«

Denn mit dem neuen Standort rückt das Fraunhofer FKIE näher an die Stadt Bonn und bereichert sie um einen weiteren Player im Bereich IT und Sicherheit. »Die hochkarätigen Redner, die bei der Eröffnungsfeier gesprochen haben, sind für uns auch ein Zeichen der Wertschätzung und Anerkennung unserer Arbeit«, freute sich Martini. Referatsleiter vom BMVg und BMBF, der Vizepräsident des BSI und ein hochrangiger Vertreter der Deutschen Telekom unterstrichen in ihren Redebeiträgen die guten und engen Beziehungen des FKIE zu den einschlägigen Organisationen und Unternehmen in Bonn.

Technologieforum 2016

Als hervorragendes Veranstaltungsformat für extern geladene Gäste hat sich 2016 erneut das Technologieforum erwiesen. Rund 200 hochrangige Besucher folgten der Einladung zur dritten Auflage der Veranstaltung und lieferten damit einen Beweis dafür, dass die Inhouse-Messe des Fraunhofer FKIE großes Ansehen beim Fachpublikum genießt.

Nach der Eröffnungsrede durch Institutsleiter Prof. Dr. Peter Martini in der voll besetzten FKIE-Robotikhalle und einem Grußwort von Generalleutnant Ludwig Leinhos, Inspekteur des neuen Bundeswehrkommandos »Cyber- und Informationsraum« (CIR), hatten die Gäste Gelegenheit, sich an 27 Ständen über aktuelle Forschungsergebnisse zu informieren. Die vorgestellten Demonstratoren und Exponate waren dabei in fünf Themenbereiche unterteilt: »Aufklärungsunterstützung für mobile Einheiten«, »Mobile Kommunikation, Aufklärung und Störung«, »Sicherheit im Informationsraum«, »Informationsgewinnung und Entscheidungsunterstützung« sowie »Sicherheit für und durch Luftsysteme«.

Parallel zur Ausstellung wurde den Gästen ein Begleitprogramm von Vorträgen zu ausgewählten Forschungsprojekten geboten, das die große Bandbreite der wissenschaftlichen Arbeit des Instituts widerspiegelte. Und auch das Netzwerken kam nicht zu kurz: Strahlender Sonnenschein und ein entsprechend im Außenbereich serviertes Catering boten beste Rahmenbedingungen für einen regen Austausch.

MEILENSTEIN

JAHRESHIGHLIGHTS

Der Takedown von »Avalanche«

Mit der Zerschlagung der Botnet-Infrastruktur »Avalanche« am 30. November 2016 ist nach vierjähriger Ermittlungsarbeit einem internationalen Team, dem auch das Fraunhofer FKIE mit seiner Abteilung »Cyber Analysis & Defense« (CA&D) angehört, ein wichtiger Schlag gegen die organisierte Cyberkriminaltiät gelungen. »Avalanche« galt als die weltweit größte Infrastruktur zum Betrieb sogenannter Botnetze und hat hunderttausendfach private und geschäftliche Computersysteme und Mobilgeräte mit Schadsoftware infiziert. Pro Woche wurden mehr als eine Million Spam- oder Phishing-Mails mit schädigendem Anhang oder Link versendet. Damit hat »Avalanche« Schäden in Millionenhöhe angerichtet.

Bei der Zerstörung der komplexen Infrastruktur kamen verschiedene Bausteine parallel zum Einsatz, die erstmals eine solch konzertierte Aktion gegen ein weltweit agierendes Botnetz-System ermöglicht haben. Fraunhofer FKIE hat durch technische Unterstützung im Rahmen eines vom Bundesamt für Sicherheit in der Informationstechnik (BSI) beauftragten Projekts maßgeblich zu der Zerschlagung von »Avalanche« beigetragen. Neben der Analyse und massiven Störung der Strukturen sowie der Identifizierung der einzelnen Server auf Führungsebene als erstem Schritt standen die Identifizierung und Sicherstellung der Täter im Vordergrund. Dank der Analyse der Schadsoftware konnten über durch das FKIE entwickelte Systeme die Opfer der Angriffe identifiziert und benachrichtigt werden. Diese Kontaktmöglichkeit über die Provider führte als Teil der Schadensabwehrstrategie zur Bereinigung der infizierten Systeme.

FKIE eröffnet Lernlabor Cybersicherheit

51 Milliarden Euro Schaden entstehen der deutschen Wirtschaft jährlich durch Datendiebstahl: Wirtschaftsspionage und Cyberkriminalität nehmen so rasant zu, dass dringend Handlungsbedarf besteht. Aus diesem Grund hat das Fraunhofer FKIE in Kooperation mit der Hochschule Bonn-Rhein-Sieg ein Lernlabor Cybersicherheit eröffnet, in dem Führungs- und IT-Fachkräfte eine kompakte Qualifizierung zu den Themenfeldern Erkennung und Analyse von sowie Reaktion auf Cybersicherheitsvorfälle erhalten.

Am 23. Mai 2017 wurde das FKIE-Lernlabor »Hochsicherheit und Emergency Response« feierlich in der Hochschule eröffnet. Mit dabei waren BMBF-Staatssekretär Thomas Rachel (2.v.r.) und Prof. Dr. Georg Rosenfeld (l.) aus dem Fraunhofer-Vorstand. Rosenfeld betonte die Notwendigkeit, Technologien nicht nur zu entwickeln, sondern auch anzuwenden und

JAHRESHIGHLIGHTS

als Lernangebote bereitzustellen. Als Impulsredner hatte FKIE-Institutsleiter Prof. Dr. Peter Martini (r.) den BSI-Vizepräsidenten Dr. Gerhard Schabhüser sowie Thomas Tschersich, Senior Vice President Internal Security & Cyber Defense der Telekom, gewinnen können. Beide lobten die Initiative des Fraunhofer FKIE und der Hochschule, am Standort Bonn das Lernlabor als einen neuen, zentralen Baustein innerhalb des IT-Sicherheitsstandortes zu errichten.

Gastgeber FKIE: Weltweites DHM-Symposium fand in Bonn statt

Das jährliche, weltweite Treffen der Digitalen Mensch-Modell-Experten, das »Digital Human Modeling Symposium« fand 2017 erstmals in Deutschland statt. Das Fraunhofer FKIE mit Dr. Thomas Alexander und seiner Abteilung »Human Factors« (HF) hatte die Veranstaltung nach Bonn geholt. An dem dreitägigen Symposium haben rund 50 Vertreter aus unterschiedlichen Forschungseinrichtungen, Universitäten sowie Mitarbeiter aus Entwicklungsabteilungen der Automobil- und der Luftfahrtindustrie aus aller Welt in den FKIE-Räumlichkeiten an der Zanderstraße teilgenommen und sich über die neuesten Entwicklungen rund um das Thema Digital Human Modeling ausgetauscht. Als Keynote-Speaker hatte Dr. Alexander den renommierten Arbeitswissenschaftler Prof. Dr. Heiner Bubb, langjähriger Professor für Ergonomie an der TU München und einer der bedeutendsten Forscher auf dem Gebiet der Fahrzeugergonomie, gewinnen können.

Insgesamt fanden bei dem Symposium sechs Sessions statt, in denen unter anderem Themen wie »3D-Animation von Modellen«, »Erfassung und Simulation von Bewegungen«, »Anthropometrie und Biomechanik«, »Validierungsmethoden für digitale Menschmodelle« sowie die »Industrielle Anwendung von digitalen Menschmodellen« diskutiert wurden. Drei Monate nach dem äußerst erfolgreichen Symposium hat die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) als Mitorganisator des Symposiums, einen Tagungsband unter dem Titel »Proceedings of the 5th International Digital Human Modeling Symposium« veröffentlicht. Er enthält insgesamt 26 wissenschaftliche Beiträge aus den verschiedenen Schwerpunktbereichen des Themengebietes »Digitale Menschmodelle«. Der 300 Seiten starke, englischsprachige Bericht vermittelt einen vollständigen Überblick über den aktuellen Forschungsstand im Bereich der digitalen Menschmodelle.

Bonner Dialog für Cybersicherheit: Diskussionsreihe mit Global Playern

Die Digitalisierung hat die Industrienationen grundlegend verändert. Aus diesem Grund wurde das Thema »Cyber- und IT-Sicherheit« auf staatlicher und industrieller Ebene längst zur Chefsache erklärt. Am Standort Bonn wird die Cybersicherheit durch unterschiedliche Akteure entwickelt und gestaltet. Um den Dialog über dieses Thema zu intensivieren, veranstalten das Fraunhofer FKIE unter der Federführung von Prof. Dr. Meier (o. l.), die Deutsche Telekom, die Stadt Bonn und die IHK Bonn/Rhein-Sieg seit 2013 den »Bonner Dialog für Cybersicherheit« (BDCS).

Das kurz zuvor in Dienst gestellte Kommando Cyber- und Informationsraum (CIR) der Bundeswehr stand im Mittelpunkt des **9. BDCS** (u.). Als »Glücksfall für Bonn und für Deutschland« bezeichnete FKIE-Institutsleiter Prof. Dr. Peter Martini, dass die Bundeswehr diesem Thema eine so zentrale Bedeutung beimesse und den Cyber- und Informationsraum als eigenen Organisationsbereich definiere. Gefragter Diskussionspartner des Abends war insofern der stellvertretende Inspekteur des Kommandos CIR, Generalmajor Michael Vetter, der über die Abwehr von Cyber-Angriffen und die Cyberstrategie der Streitkräfte berichtete.

»Cybersicherheit zum Schutz der Demokratie« lautete das Thema des **10. BDCS** (o. r.), bei dem Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), als Keynote-Speaker hervorhob, dass Deutschland in Sachen Cyberabwehr gut aufgestellt sei. Es gebe jedoch keine Gewähr dafür, dass dies so bleibe: Wichtige Voraussetzung hierfür sei, dass sich die Bürger entsprechend beteiligen, denn: »Cybersicherheit ist eine gesellschaftliche Gemeinschaftsaufgabe.«

KARRIEREWEGE

GELUNGENER ABSCHLUSS DER ERSTEN FÜHRUNGSAKADEMIE

»Zwei Jahre sind seit dem Start ins Land gezogen, ich kann es kaum glauben«, begann Institutsleiter Prof. Dr. Peter Martini seine Begrüßung anlässlich des feierlichen Abschlusses der ersten FKIE-Führungsakademie. 2014 war Dr. Eva Kneise, Leiterin der Personalentwicklung am Fraunhofer FKIE, angetreten, um aus jungen FKIE-Wissenschaftlerinnen und Wissenschaftlern Nachwuchsführungskräfte zu machen. Im Mai 2016 nahm der erste Abschlussjahrgang seine Zertifikate entgegen.

Die Idee zu einer Führungsakademie gab es bereits seit 2012, doch erst Kneise hatte 2014 die Feinplanung des aus drei Bausteinen bestehenden Programms übernommen und den Prozess gestartet. Die zwölf Teilnehmer, die aus 30 Bewerbern ausgewählt worden waren, durchliefen ein Seminarprogramm aus acht Modulen und arbeiteten gemeinsam an Zukunftsprojekten. Zudem suchte sich jeder Teilnehmer einen Mentor aus Wirtschaft oder Forschung, der ihn begleitete und in der persönlichen Entwicklung unterstützte.

Individuelle Weiterentwicklung und partizipatives Führungsverständnis

Die Ziele, die das neue Programm adressieren soll, sind vielfältig: Natürlich geht es um die individuelle Förderung und Weiterentwicklung der einzelnen Teilnehmer. Jeder von ihnen soll seine eigenen Stärken erkennen und sich auf diese fokussieren. Wichtig ist Professor Martini zudem, das Programm nicht als Vorgesetzten-, sondern als Führungsakademie verstanden zu wissen.

Zentraler Bestandteil der Qualifizierung ist jedoch, die Teilnehmer im Sinne der gewünschten Kulturentwicklung am Institut zu sensibilisieren und zu schulen: So ist es Ziel, die abteilungsübergreifende Zusammenarbeit zu verbessern. Auch das Verständnis von »Führung« soll sich wandeln und das FKIE-Führungsleitbild mit Leben gefüllt werden. »Wir sind ein komplexes Institut «, so Professor Martini zu den Absolventen, »deshalb brauchen wir Mitarbeiter wie Sie, die zusätzliche Verantwortung übernehmen, mit und ohne Vorgesetztenfunktion.« Gerade angewandte Wissenschaft, so Martini weiter, erfordere Freiheiten und ein partizipatives Führungsverständnis.

Durch das zweijährige Programm ist innerhalb des Fraunhofer FKIE ein starkes Netzwerk entstanden, das nicht zuletzt auch abteilungsübergreifende Projekte wie »PAA« begünstigt hat. Sich miteinander über wissenschaftliche Ergebnisse und Projekte auszutauschen sei wichtig, sind sich die Akademie-Absolventen Dr. Elmar Padilla, Alex Höck und Dr. Bernd Brüggemann einig. Denn, so bringt es Brüggemann, inzwischen Forschungsgruppenleiter, auf den Punkt: »Das Thema Kommunikation, das das Institut im Namen trägt, darf nicht nur Forschungsgegenstand sein.« Vielmehr sei es von enormer Bedeutung, den Begriff auch im Alltag mit Leben zu füllen und sich auszutauschen, damit Synergien entstehen und Verständnis wachsen kann.

Fazit: Ziele erreicht!

»Sie haben viel Zeit und Lebenskraft eingebracht«, schloss der Institutsleiter, »doch es hat sich gelohnt – für Sie und für das ganze Institut.« Aus der gemeinsamen Arbeit an den Zukunftsprojekten ist eine Projektlandkarte hervorgegangen, die den Überblick über die Entwicklungsergebnisse des gesamten Instituts fördert und neue Synergien schafft. 92 Prozent der Teilnehmerinnen und Teilnehmer haben seit Abschluss der Akademie eine erweiterte führende Funktion. Sie sind so Vorbild und Motivation für die strukturierte Weiterbildung am FKIE.

VON LINKS NACH RECHTS:
I Vorne I ***Sandra Noubours, Dr. Bernd Brüggemann, Dr. Hanna Geppert, Dr. Eva Kneise*** *I Mitte I* ***Arne Schwarze, Dr. Daniel Feiser, Dr. Felix Govaers, Alexander Höck*** *I Hinten I* ***Daniel Ota, Christian Plegge, Sylvia Käthner***
NICHT IM BILD:
Dr. Elmar Padilla, Dr. Marek Schikora

Dr. Hanna Geppert

FORSCHUNG UND FAMILIE IM EINKLANG

Sind die Leidenschaft für anwendungsorientierte Forschung und eine Großfamilie miteinander vereinbar? Die Wissenschaftlerin Dr. Hanna Geppert beweist: Ja, sind sie! In jedem Fall bei Fraunhofer FKIE. Seit Dezember 2016 leitet die vierfache Mutter die Forschungsgruppe »Architektur verteilter Führungssysteme« in der Abteilung »Informationstechnik für Führungssysteme« (ITF). Ihr Lebenslauf bis dorthin liest sich so beeindruckend wie diszipliniert. Doch die engagierte Informatikerin gibt offen zu: »Ohne die Unterstützung des Fraunhofer FKIE wäre mir dieser Weg so nicht möglich gewesen.«

Die Karrierestationen von Dr. Hanna Geppert zeugen von Zielstrebigkeit und Leidenschaft für die Forschung: Dank eines sogenannten Anfänger-Stipendiums der Technischen Universität Kaiserslautern startet die 19-Jährige im Jahr 2000 ihr Studium der Informatik. Nach zwei Jahren wechselt die Studentin an die Universität in Bonn, wo sie 2004 ihr Studium als Diplom-Informatikerin abschließt. Am Lehrstuhl für Lifescience-Informatics, der in das Bonn-Aachen International Center for Information Technology (b-it) integriert ist, arbeitet sie anschließend als wissenschaftliche Mitarbeiterin. Dort schließt sie auch im Jahr 2008 ihre Promotion ab. Drei weitere Jahre bleibt sie am b-it, forscht, publiziert und hält im Rahmen einer Postdoc-Stelle Lehrveranstaltungen zu ihren Forschungsthemen. Währenddessen werden im Abstand von einein-halb Jahren 2009 und 2010 ihre beiden Töchter geboren. Geppert wechselt von Voll- auf Teilzeit.

Verstärkt anwendungsorientiert forschen

Zwar hat bereits ihre Arbeit für das b-it einen Anwendungsbezug, da dieses mit der klassisch universitären Lehre und Forschung auch Kollaborationen wie zum Beispiel mit der Chemie- und Pharma-Industrie verbindet. Geppert aber möchte noch stärker für die Industrie forschen. »Und bei anwendungsorientierter Forschung kommt man an dem Namen ›Fraunhofer‹ einfach nicht vorbei«, so die begeisterte Wissenschaftlerin. 2011 wechselt sie erfolgreich als Wissenschaftliche Mitarbeiterin ans Fraunhofer FKIE und steigt zunächst ebenfalls mit 20 Stunden pro Woche ein.

Flexible Aufgabenanpassung

2012 und 2014 kommen ihre beiden Söhne auf die Welt. »Ohne die Unterstützung meiner Kollegen, der flexiblen Arbeitsgestaltung und der Tatsache, dass meine Vorgesetzten sich ohne Vorurteile darauf eingelassen haben, wäre es nicht möglich gewesen, den Spagat zwischen der Betreuung von vier Kindern und der anspruchsvollen wissenschaftlichen Arbeit zu bewerkstelligen«, resümiert die Wissenschaftlerin dankbar. So räumt die Abteilung ITF der vielversprechenden und beliebten Kollegin beispielsweise die Möglichkeit ein, für die Zeit, in der die Kinder noch sehr klein und aus diesem Grund planbare und regelmäßige Arbeitszeiten hilfreich sind, Forschungsaufgaben größtenteils in Wachtberg zu übernehmen und Dienstreisen auf ein absolutes Minimum zu reduzieren. »Die große Aufgabenvielfalt und die Gestaltungsmöglichkeit, waren von großem Vorteil für mich.«

Karrierezeit
Mit der Teilnahme an der institutsinternen Führungsakademie, ergeben sich für Geppert neue Aufgabenfelder im Bereich Projektleitung und zunehmend in der Vertretung des Forschungsgruppenleiters. Nach dessen Berufung an die Hochschule für Technik und Wirtschaft des Saarlandes (htw saar) übernimmt Geppert Ende 2016 schließlich die offizielle Leitung der ITF-Forschungsgruppe »Architektur verteilter Führungssysteme«.

»Die Führungsakademie war für mich eine wichtige Chance und hat mich wirklich weiter gebracht – auch wenn man erst im Nachhinein, im Alltag, feststellt, wie es nachwirkt. Der Mentoring-Baustein beispielsweise war sehr wichtig, um mir über meine Persönlichkeit und Wünsche klar zu werden, und das umfangreiche Seminarprogramm für die Handhabung der Führungstools.«

Wissenschaft für den Kunden
Über die Frage, was ihre Arbeit bei Fraunhofer FKIE besonders präge, muss Geppert nicht lange nachdenken: »Da ist zuallererst die beratende Position, die man für den Auftraggeber einnimmt. Wir machen Wissenschaft für den Kunden, man muss dessen Anforderungen und Probleme genau verstehen. Andersherum bietet Fraunhofer FKIE auch die Möglichkeit, Themen, an denen man Spaß hat, weiter voranzutreiben, vorausgesetzt natürlich, der Bedarf von Kundenseite ist gegeben.«

Ein weiterer Punkt, den sie besonders schätze, sei der hohe Grad an Interdisziplinarität, der am Institut herrsche: »Man kann hier Experten aus so unterschiedlichen Bereichen wie der Ergonomie, der Linguistik und Softwareentwicklung zusammenbringen.« Und schließlich habe man bei Fraunhofer FKIE die Gelegenheit, sich in kürzester Zeit in neue Themen einarbeiten zu dürfen: »Es gibt ein ständiges Lernen und Neu-Erarbeiten. Das schätze ich sehr.«

Dr.-Ing. Emre Özyurt

AUFSTIEG IN DER INDUSTRIE DANK PROMOTION

Dr.-Ing. Emre Özyurt, ehemaliger wissenschaftlicher Mitarbeiter der Abteilung »Mensch-Maschine-Systeme« (MMS) des Fraunhofer FKIE, ist in Istanbul. In seiner Position als Executive Product Manager von T-Systems führt der promovierte Diplom-Informatiker dort gerade Sondierungsgespräche für eine Kooperation mit den ansässigen Universitäten. Ziel der angestrebten Zusammenarbeit ist es, gut ausgebildete Fachkräfte nach Deutschland zu holen. T-Systems benötigt sie in Stuttgart dringend zur Verstärkung seiner sogenannten Scrum-Teams, welche derzeit vorrangig Softwareapplikationen für Automobilhersteller entwickeln. Die Initiative, dem Fachkräftemangel in Deutschland durch das Direkt-Anwerben guter Leute aus dem Ausland zu begegnen, stammt von Özyurt selbst. Dass er diese so schnell auch federführend in die Tat umsetzen konnte, hat der Manager seinem schnellen Aufstieg beim neuen Arbeitgeber zu verdanken. Die Weichen dafür wurden bereits in seiner Zeit bei Fraunhofer gestellt.

»Ohne die Möglichkeit, bei Fraunhofer FKIE neben der Projektarbeit zu promovieren, hätte ich den Aufstieg nicht so schnell geschafft«, ist Özyurt überzeugt. Dadurch, dass er am Fraunhofer-Institut in Projekten arbeiten konnte, die eng an seinem Promotionsthema lagen, und ihm auch ausreichend Freiraum für die Arbeit an seiner Dissertation eingeräumt wurde, konnte er diese in kurzer Zeit abschließen.

Der Doktorgrad sei eine gute Ausgangslage für den Start in der Industrie gewesen. »Natürlich hat der Zeitpunkt auch einfach gut gepasst und das Glück ein bisschen mitgespielt«, gibt Özyurt zu. Denn schon Anfang nächsten Jahres steht eventuell der nächste Schritt auf der Karriereleiter an, in Form eines Assessment-Centers für die Position des Fachgebietsleiters.

Doch zurück zum Anfang: Özyurt kam 2001 nach seinem Abschluss des Gymnasiums aus Istanbul nach Aachen und studierte dort zunächst Informatik an der RWTH. Parallel zum Studium arbeitete er als studentische Hilfskraft am Institut für Arbeitswissenschaft (IAW) bei Prof. Dr. Christopher Schlick. Durch dessen Tätigkeit sowohl an der RWTH als Leiter des IAW als auch bei Fraunhofer FKIE, seinerzeit als stellvertretender Institutsleiter, entstanden erste Berührungspunkte mit dem Institut in Wachtberg.

»Schicksalhafte Karrierefügung«
Dass dieses nach Abschluss seines Diploms im Jahr 2008 zufälligerweise gerade einen Spezialisten für Simulation suchte, war eine schicksalhafte Fügung, die Özyurt direkt nach dem Studium eine Stelle als wissenschaftlicher Mitarbeiter in der Abteilung »Mensch-Maschine-Systeme«

(MMS) bescherte. Zusammen mit anderen Wissenschaftlern entwickelte er hier unter anderem die Operationszentrale der Zukunft für schwimmende Plattformen sowie weitere Konzepte und Prototypen für Benutzungsschnittstellen für Fregatten/Korvetten der Deutschen Marine.

In dieser Zeit schrieb er parallel seine bereits erwähnte Dissertation zum Thema »Konzeption und Entwicklung eines kognitiven und kooperativen Assistenzsystems zur interaktiven Unterstützung bei sicherheitskritischen Aufgaben« als Abstraktion der stark anwendungsorientierten Projektarbeit unter der Betreuung von Prof. Dr. Frank Flemisch, Prof. Dr. Schlick und Prof. Dr. Bernhard Döring.

Diese Möglichkeit der Verknüpfung zwischen Projektarbeit und wissenschaftlicher Promotionsarbeit beschreibt Özyurt noch immer als Glückssituation, ebenso wie die Tatsache, dass er dank der Kontakte seiner Abteilung zur Marine Operateure aus diesem Bereich für die Evaluation des Systems, das aus seiner Doktorarbeit entstand, gewinnen konnte.

Wechsel in die Industrie

Im Januar 2016 schloss er seine Promotion an der RWTH Aachen erfolgreich ab. Auch das von ihm mitentwickelte Systemkonzept konnte im Rahmen eines Kooperationsprojektes erfolgreich in die Führungs- und Waffeneinsatzsysteme (FüWES) eines Industriepartners integriert werden. Bereits im April 2016 brach er dann auf zu neuen Ufern: Özyurt wechselte in die Wirtschaft und stieg als Produktmanager im Bereich Sales / After Sales bei T-Systems in Stuttgart ein. Das Unternehmen entwickelt Software für mittelständische Unternehmen und Großkonzerne und ist an diesem Standort auf die Automobilbranche ausgerichtet. So erarbeitet Özyurt mit seinem Team verschiedene Softwareprodukte für einen namhaften deutschen Automobilhersteller, beispielsweise ein Monitoring-/Reportingsystem, mit dessen Hilfe der Zustand bereitgestellter Applikationen im Sales-Bereich überwacht werden kann. Zwei Teams unterstehen bei T-Systems seiner Leitung, eines in Deutschland und eines in Rumänien. Zu seinen Zuständigkeiten zählen die Bereiche Projektmanagement, Vertrieb und Kundenpflege.

Freude am Lösen von Problemen

Wenn Özyurt an seinen ehemaligen Arbeitgeber Fraunhofer FKIE denkt, fällt ihm als erstes die große und schnelle Hilfsbereitschaft seiner Kollegen und Vorgesetzten ein. Der Umgang bei MMS sei sehr freundschaftlich gewesen. Noch heute habe er Kontakt zu seinen ehemaligen Kollegen. Die Freude am Lösen von Problemen sei tief in der Kultur des Instituts verankert. Auch methodisch habe er viel mitgenommen: vor allem wissenschaftlich zu arbeiten, also Problemstellungen klar zu strukturieren, den aktuellen Forschungsstand zu eruieren, vom spezifischen Anwendungsfall zu abstrahieren und Lösungen zu transferieren sowie umgekehrt auch andere Technologien oder Ideen für das eigene Problem adaptieren zu können.

»Durch die starke Anwendungsorientierung bei Fraunhofer habe ich gelernt, Ideen bis hin zum Prototypen oder zum einsatzfähigen Produkt umzusetzen und voranzutreiben – und diese Ergebnisse dann anhand selbst gesetzter, sinnvoller Kriterien zu evaluieren«, führt Özyurt weiter aus. »Die Forschung für die Industrie, wie sie bei der Fraunhofer-Gesellschaft betrieben wird, ist für diejenigen, die später ohnehin in die Wirtschaft wollen, sehr von Vorteil«, lautet sein dankbares Fazit, »weil sich in dieser Zeit bereits sehr wertvolle Kontakte ergeben.«

Dr.-Ing. Emre Özyurt

Jessica Conradi

EXZELLENZFÖRDERUNG MIT »FRAUNHOFER TALENTA«

»Es erfüllt mich mit Freude, so engagierte Mitarbeiterinnen wie Sie am Institut zu haben. Und das sage ich nicht, weil Sie eine Frau sind, die erfolgreich Karriere in der Wissenschaft macht, sondern weil Sie wirklich eine tolle Mitarbeiterin meines Instituts sind.« Institutsleiter Prof. Dr. Peter Martini zeigte sich anlässlich der Übergabe der »Fraunhofer TALENTA«-Urkunde an FKIE-Wissenschaftlerin Jessica Conradi sichtlich stolz. Bis Mai 2017 hat die stellvertretende Leiterin der Abteilung »Human Factors« (HF) zwei Jahre lang das exklusive Programm der Fraunhofer-Gesellschaft zur Förderung herausragender Wissenschaftlerinnen absolviert.

Ihre »TALENTA-Karrierezeit« hat die diplomierte Ingenieurin für Sicherheitstechnik für mehrere Projektleitungsfortbildungen, darunter die PMP (Project Management Professional)-Zertifizierung, sowie für die Fertigstellung ihrer Promotion genutzt. In der Arbeit befasst sich die Wissenschaftlerin mit der Fragestellung, wie sich unterschiedliche Button- und Schriftgrößen auf die Bedienung von Smartphones in der Bewegung auswirken, also beispielsweise im Gehen. Ein brandaktuelles und maximal anwendungsorientiertes Forschungsfeld.

Durch das Förderprogramm steht die Doktorarbeit kurz vor ihrem Abschluss. Conradi: »Es ist toll, dass einem diese Zeit gegeben wird, die man für seine Karriere nutzen kann und muss. TALENTA ermöglicht es einem, sich diese Zeit von dem täglichen Projektgeschäft freizuschaufeln.«

ZIEL
Die Fraunhofer-Gesellschaft als die größte Organisation für anwendungsorientierte Forschung hat es sich zur Aufgabe gemacht, Wissenschaftlerinnen aus den MINT-Fächern zu fördern.

Das TALENTA-Programm bietet ausgewählten Wissenschaftlerinnen auf drei verschiedenen Karrierestufen Networking, Weiterbildung und Unterstützung bei der Karriereplanung:

I. **TALENTA start** für alle Hochschulabsolventinnen, die ihre Karriere mit Fraunhofer in der angewandten Forschung gerade erst beginnen
II. **TALENTA speed up** für berufserfahrene Wissenschaftlerinnen mit Motivation und Potenzial zur Übernahme von Führungs- oder Fachverantwortung
III. **TALENTA excellence** für etablierte Wissenschaftlerinnen in Führungspositionen

AUSZEICHNUNGEN

ERC-Grant

»Die Technik muss sich dem Menschen anpassen und nicht umgekehrt«, das ist der Leitspruch von **Prof. Dr. Matthew Smith**, Leiter der Abteilung »Usable Security and Privacy« (USP) am Fraunhofer FKIE. »Nur wenn IT-Sicherheit bedienbar ist, wird sie auch angewendet.« Der Europäische Forschungsrat teilt seine Meinung und bewilligte Smith's Forschungsprojekt »Frontiers of Usable Security« eine fünfjährige Förderung in Gesamthöhe von 1,5 Millionen Euro. Smith, der parallel zu seiner Funktion bei Fraunhofer einen Informatik-Lehrstuhl an der Rheinischen Friedrich-Wilhelms-Universität in Bonn innehat, möchte damit einen umfassenden Lösungsansatz für diese weltweit relevante Problematik erforschen.

Bereits seit vielen Jahren befasst sich Smith mit dem »Faktor Mensch« und der möglichst ergonomischen Darstellung und Handhabung sicherheitsrelevanter Informationen und Funktionen. Im Fokus seiner Forschungsarbeit steht dabei das Spannungsfeld zwischen komplexen Sicherheitstechnologien einerseits und der einfachen Bedienbarkeit andererseits. »Mithilfe der Förderung möchte ich die Grenzen der Forschung erweitern und Entwicklern und Administratoren helfen, sichere Systeme zu bauen«, so Smith. Dafür ist zunächst einmal umfassende Ursachenforschung unter der engen Einbindung von Entwicklern und Administratoren erforderlich. Im Anschluss daran werden konkrete Lösungen zu insgesamt sieben Fragestellungen erforscht. Der offizielle Startschuss für das Projekt fiel am 1. August 2016.

ATHENA

Im November 2016 wurde das Projekt »ATHENA« nach einer Laufzeit von drei Jahren nicht nur erfolgreich beendet, sondern seitens der EU zusätzlich für seine stringente Durchführung und seine Ergebnisse, welche die vorab definierten Ziele noch deutlich übertrafen, als »exzellent« ausgezeichnet.

Ziel des Kooperationsprojekts unter der Leitung von **Dr. Kellyn Rein**, wissenschaftliche Mitarbeiterin der Abteilung »Informationstechnik für Führungssysteme« (ITF), war die Entwicklung und Testung einer App für mobile Endgeräte und eines Führungssystems (Command and Control). Im Zusammenspiel sollen App und Führungssystem in den ersten Minuten einer Krisensituation, der sogenannten »goldenen Stunde«, dabei unterstützen, Informationen von Zivilisten in Echtzeit zu erfassen und den Einsatzkräften, die sich zum Zeitpunkt noch nicht vor Ort befinden, zeitnah und in einer konsolidierten Form zuzuführen. Diese erhalten mittels der aufbereiteten Daten sehr schnell ein möglichst genaues Lagebild, welches sie zur optimalen Einsatzplanung nutzen können. Das System wurde in mehreren Großübungen, unter anderem in Slowenien und England, erfolgreich getestet.

AFCEA Studienpreis 2016

Der zweite und dritte Platz des renommierten AFCEA Studienpreises wurde im Jahr 2016 an Masterarbeiten vergeben, die von zwei FKIE-Mitarbeitern wissenschaftlich begleitet wurden: **Jun.-Prof. Dr. Delphine Reinhardt** und **Prof. Dr. Frank Kurth** forschen für das Fraunhofer FKIE und haben gleichzeitig einen Lehrauftrag am Institut für Informatik 4 der Universität Bonn inne. Thematisch befassen sich die von ihnen für die Auszeichnung vorgeschlagenen Arbeiten mit ihren jeweiligen FKIE-Forschungsschwerpunkten.

So bewertet Professorin Reinhardt die Ergebnisse der mit dem zweiten Preis ausgezeichneten Masterarbeit von **Ilya Manyugin** als »einen Meilenstein zur Erhöhung der Privatsphäre bei der Nutzung von Smartphones«. Die wissenschaftliche Arbeit des Bonner Studenten befasst sich mit der Frage, wie partizipative Sensornetze (engl. Participatory Sensing) zur Verbesserung der Privatsphäre von Nutzern beitragen können, und belegt einen innovativen Weg für die dezentrale Verschlüsselung von Daten.

Den dritten Platz des AFCEA Studienpreises erzielte **Sebastian Urrigshardt**, mittlerweile wissenschaftlicher Mitarbeiter der Abteilung »Kommunikationssysteme« (KOM), mit seiner Forschungsarbeit über Methoden zur robusten Sprachsignalverarbeitung. Er wurde von Professor Kurth betreut, der die Praxisnähe der Arbeit seines Studenten lobt: »Spracherkennung für Diktierfunktionen oder Sprachsteuerung halten immer weiter Einzug in den Alltag.« Die Verleihung des AFCEA Studienpreises fand am 1. September 2016 in Koblenz statt. Die seit 2008 jährlich vergebene Auszeichnung ist mit insgesamt 15.000 Euro dotiert.

Locked Shields 2017

»Für die ausgezeichnete Zusammenarbeit und Unterstützung« durch **Harald Schmidt,** wissenschaftlicher Mitarbeiter der Abteilung »Kommunikationssysteme« (KOM), bei der »Locked Shields 2017«, der mit 800 Teilnehmern aus 25 Nationen größten und komplexesten internationalen Cyber-Defence-Übung, hat sich das Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) mit einem offiziellen Schreiben bei der Institutsleitung des Fraunhofer FKIE bedankt.

In seiner Funktion als Firewall-Administrator habe Schmidt, so ZCSBw-Leiter Hans-Ulrich Schade, »eine Schlüsselposition« innegehabt. Schmidt habe durch »großartige Einsatzbereitschaft« und »herausragende Fachkenntnisse« überzeugt und damit maßgeblich zu dem »sehr guten Gesamtergebnis« des nationalen »Blue Teams« beigetragen.

AUSZEICHNUNGEN

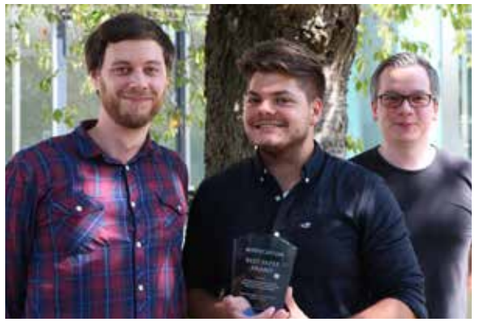
EnRicH

In dem niemals in Betrieb gegangenen österreichischen Kernkraftwerk Zwentendorf hat vom 19. bis 23. Juni 2017 der erste »European Robotics Hackathon« (EnRicH) stattgefunden. Das Fraunhofer FKIE fungierte bei dem Wettbewerb nicht nur als Organisator, sondern gewann als Teilnehmer sogar in zwei von drei Kategorien.

Elf internationale Teams und ihre Robotersysteme stellten sich der Herausforderung des realen Störfallszenarios. Nur sieben Teams, darunter auch das FKIE, traten in allen Kategorien – »3D-Lagekarte«, »Strahlungskarte« und »Manipulation« – an. Als einzigem Teilnehmer gelang es den Wissenschaftlern um **Dr. Bernd Brüggemann**, ihren Roboter ganz autonom nach den Zylindern mit radioaktivem Material greifen und diese auf Strahlung prüfen zu lassen sowie abzutransportieren. Eine Leistung, die ihm den Sieg in der Kategorie »Manipulation« einbrachte.

Und auch mit seiner Strahlungskarte konnte das Institut punkten. Den ersten Platz teilt es sich hier mit Team Hector der TU-Darmstadt. FKIE-Wettbewerbsleiter **Dr. Frank E. Schneider**: »Der erste Durchlauf des Hackathons war so erfolgreich, dass wir eine Fortsetzung des Formats in 2019 planen. Dann werden wir den Schwierigkeitsgrad erhöhen und noch realere Einsatzbedingungen schaffen.«

Best Paper Award



Ein Forschungsbeitrag der Abteilung »Cyber Analysis & Defense« (CA&D) hat den Best Paper Award des Digital Forensik Research Workshops USA, einer der wichtigsten internationalen Konferenzen im Bereich »Digitale Forensik« gewonnen. Mit der Einreichung »Extending the Sleuth Kit and its Underlying Model for Pooled Storage File System Forensic Analysis« setzte sich das Autorenteam **Jan-Niclas Hilgert** (M.), **Martin Lambertz** (r.) und **Daniel Plohmann** (l.) im August 2017 gegen zwölf internationale Beiträge durch.

Ihre Arbeit befasst sich mit der »File System Forensic Analysis« des US-Sicherheitsexperten Brian Carrier. Die Veröffentlichung von 2005 bietet bis heute die umfassendste Übersicht über verbreitet genutzte Dateisysteme, wurde jedoch nie aktualisiert. Eine Aufgabe, der sich nun die drei FKIE-Wissenschaftler angenommen hatten. Bereits im März 2016 zählten Hilgert und Lambertz zu den Gewinnern eines Forensik-Rodeos, das im Rahmen der EU-Ausgabe der Veranstaltung durchgeführt wurde.

BERUFUNGEN

Dr. Steffen Wendzel
Bereits in seiner Dissertation sowie auch in seiner Zeit in der Abteilung »Cyber Security« (CS) am Fraunhofer FKIE forschte Dr. Steffen Wendzel zum Thema »Sicherheit von Netzwerken«. Hierbei beschäftigte ihn zuletzt vor allen Dingen der Bereich »Smart Homes & Smart Buildings«. Zum Wintersemester 2016/2017 erhielt der Wissenschaftler einen Ruf an die **Hochschule Worms**, wo er seitdem eine Professur für »IT-Sicherheit und Netzwerke« innehat.

Dr. Markus Esch
Der Leiter der Forschungsgruppe »Architekturen Verteilter Systeme« in der Abteilung »Informationstechnik für Führungssysteme« (ITF) wurde zum 1. Dezember 2016 auf eine Professur für das Lehrgebiet »Softwarearchitektur, Verteilte Systeme und Grundlagen der Informatik« an die **Hochschule für Technik und Wirtschaft des Saarlandes** (htw saar) berufen. Seine Forschungsschwerpunkte, die in den Bereichen »Selbstorganisation in Verteilten Systemen« und »Cloud-Computing-Architekturen« liegen, wird er an der htw saar fortführen und vertiefen.

Jun.-Prof. Dr. Delphine Reinhardt
Auch die Leiterin der Abteilung »Privacy and Security in Ubiquitous Computing« verlässt das Fraunhofer FKIE und die Rheinische Friedrich-Wilhelms-Universität Bonn. Hier widmete sie sich der Erforschung des Themas Schutz der Privatsphäre im Cyberspace. Doch Delphine Reinhardt geht nicht ganz: Zwar folgt sie dem Ruf an die **Georg-August-Universität Göttingen** zum 31. Dezember 2017, doch bleibt sie dem Institut in Zukunft als Kuratorin erhalten und auf diese Art eng verbunden.

Prof. Dr. Matthew Smith
Erfolgreich abgewehrt werden konnten einige attraktive Rufe an Prof. Dr. Matthew Smith, Leiter der Abteilung »Usable Security and Privacy« am Fraunhofer FKIE sowie der gleichnamigen Arbeitsgruppe am Institut für Informatik 4 der Universität Bonn. Möglich war dies nur dank des engen Schulterschlusses der Rheinischen Friedrich-Wilhelms-Universität Bonn und des Fraunhofer FKIE. Durch seinen Verbleib in Bonn wird der Schwerpunkt IT-Sicherheit in Forschung und Lehre weiter verstärkt.

SERVICE

FKIE VERNETZT

KURATORIUM

VORSITZENDER DES KURATORIUMS
Prof. Dr. Gerd Ascheid
RWTH Aachen, Aachen

Victoria Appelbe
Amt für Wirtschaftsförderung, Bonn

Ralf Brümmer*
Securitas GmbH, Berlin

BrigGen Dr. Michael Färber
BMVg – Bundesministerium der Verteidigung, Berlin

Prof. Dr. Stefan Fischer
Universität zu Lübeck, Lübeck

Prof. Dr. Uwe Hanebeck
Karlsruher Institut für Technologie KIT, Karlsruhe

Dr. Vera Kamp
Plath GmbH, Hamburg

Prof. Dr. Reinhard Klein
Rheinische Friedrich-Wilhelms-Universität, Bonn

Dr. Jens Bodo Koch-Kusenberg
ATLAS ELEKTRONIK GmbH, Bremen

Herbert Rewitzer
ROHDE & SCHWARZ GmbH & Co. KG, München

Prof. Dr. Axel Schulte
Universität der Bundeswehr München, Neubiberg

Prof. Dr. Walter Tötsch
Ehemals Evonik Industries AG, Marl

Thomas Tschersich
Deutsche Telekom AG, Bonn

Joost Verton
Airbus Defence and Space GmbH, Taufkirchen

MR Norbert Michael Weber
BMVg – Bundesministerium der Verteidigung, Bonn

Prof. Dr. Klaus Wehrle
RWTH Aachen, Aachen

Dr. Thomas Weise
Rheinmetall AG, Düsseldorf

Prof. Dr. Claudia Wich-Reif
Rheinische Friedrich-Wilhelms-Universität, Bonn

Bolko Wietrzynski
Diehl BGT Defence GmbH & Co. KG, Überlingen

**Kurator ab 01.01.2018*

KOOPERATIONEN

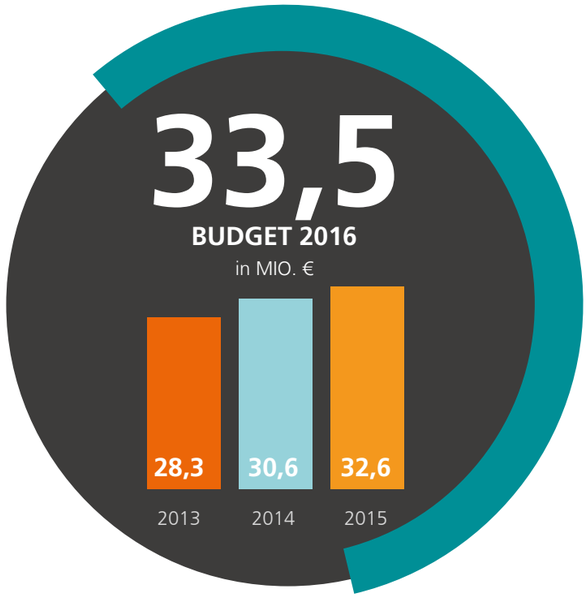
FRAUNHOFER-VERBÜNDE
Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung **VVS**
Fraunhofer-Verbund **IUK-Technologie**

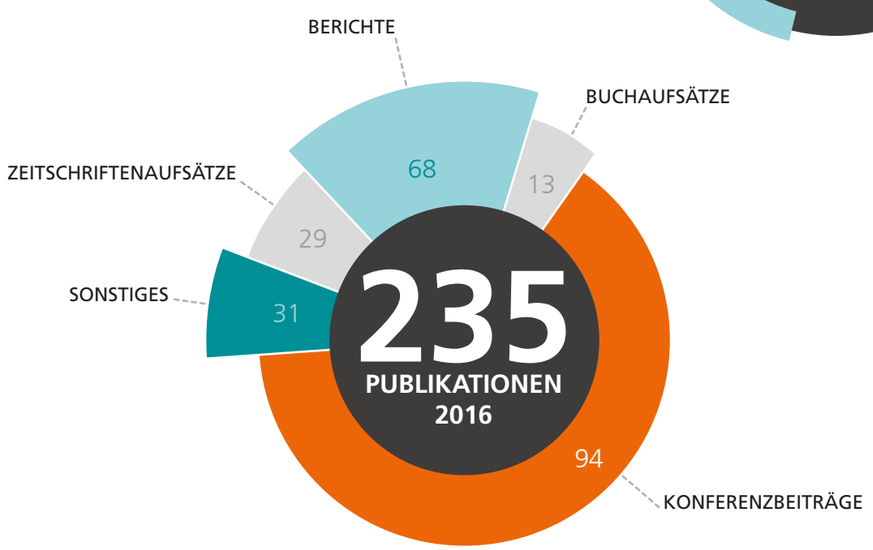
FRAUNHOFER-ALLIANZEN
Big Data
Space
Embedded Systems

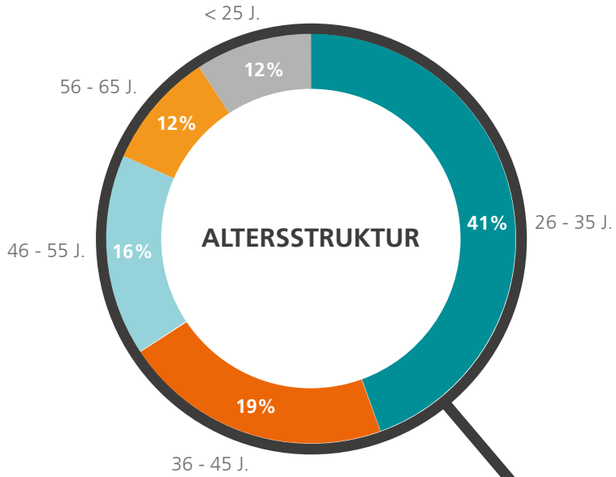
UNIVERSITÄTSKOOPERATIONEN
Rheinische Friedrich-Wilhelms-Universität Bonn
Rheinisch-Westfälische Technische Hochschule Aachen
Hochschule Bonn-Rhein-Sieg

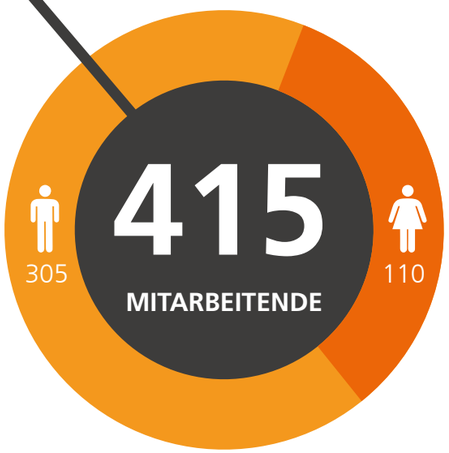
PARTNER
Allianz für Cybersicherheit

ZAHLEN UND FAKTEN









Computerlinguistik
Elektrotechnik
Informatik
Maschinenbau/Verfahrenstechnik
Mathematik
Physik
Psychologie
Sicherheitstechnik

STUDIENRICHTUNGEN (HÄUFIGSTE)

Stand 04.10.2017

SERVICE

FRAUNHOFER-GESELLSCHAFT

Forschen für die Praxis ist die zentrale Aufgabe der Fraunhofer-Gesellschaft. Die 1949 gegründete Forschungsorganisation betreibt anwendungsorientierte Forschung zum Nutzen der Wirtschaft und zum Vorteil der Gesellschaft. Vertragspartner und Auftraggeber sind Industrie- und Dienstleistungsunternehmen sowie die öffentliche Hand.

Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit 69 Institute und Forschungseinrichtungen. 24 500 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 2,1 Milliarden Euro. Davon fallen 1,9 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Mehr als 70 Prozent dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Knapp 30 Prozent werden von Bund und Ländern als Grundfinanzierung beigesteuert, damit die Institute Problemlösungen entwickeln können, die erst in fünf oder zehn Jahren für Wirtschaft und Gesellschaft aktuell werden.

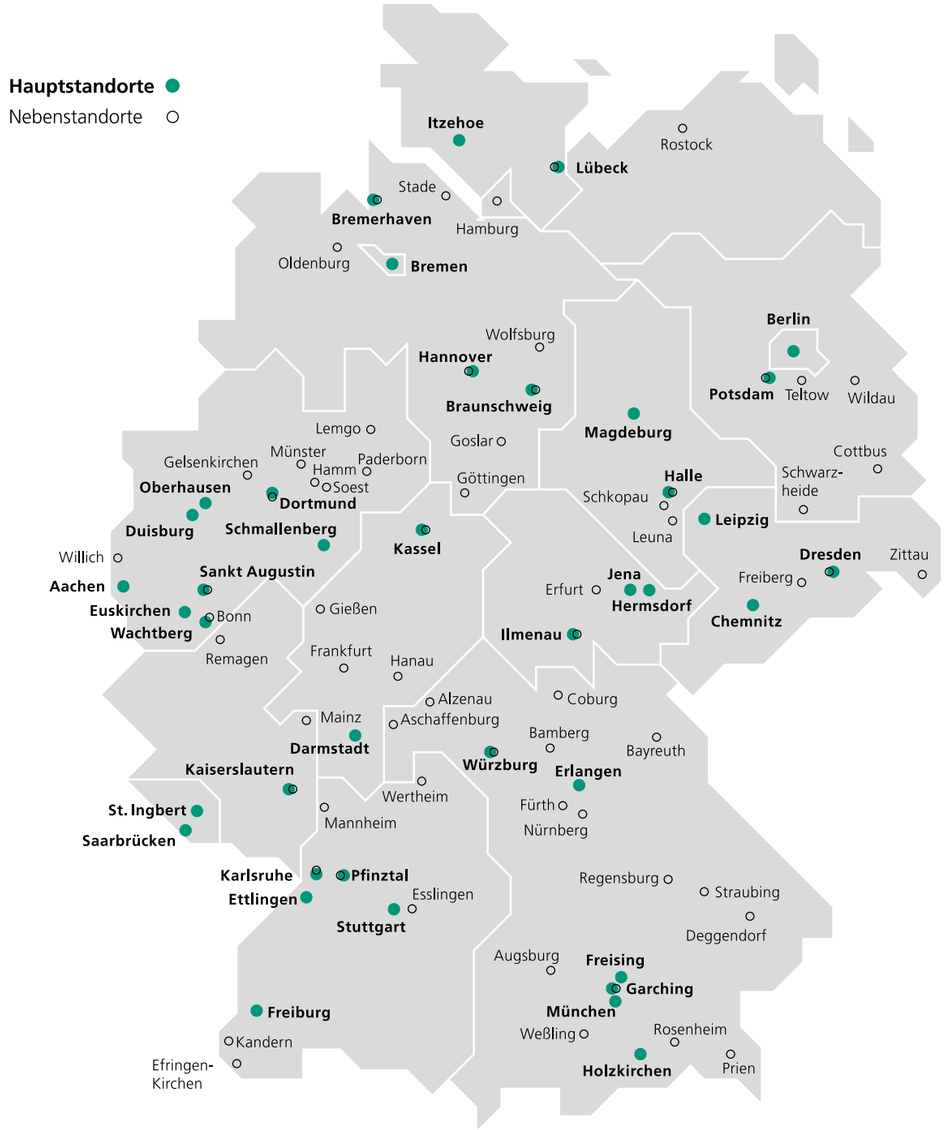
Internationale Kooperationen mit exzellenten Forschungspartnern und innovativen Unternehmen weltweit sorgen für einen direkten Zugang zu den wichtigsten gegenwärtigen und zukünftigen Wissenschafts- und Wirtschaftsräumen.

Mit ihrer klaren Ausrichtung auf die angewandte Forschung und ihrer Fokussierung auf zukunftsrelevante Schlüsseltechnologien spielt die Fraunhofer-Gesellschaft eine zentrale Rolle im Innovationsprozess Deutschlands und Europas. Die Wirkung der angewandten Forschung geht über den direkten Nutzen für die Kunden hinaus: Mit ihrer Forschungs- und Entwicklungsarbeit tragen die Fraunhofer-Institute zur Wettbewerbsfähigkeit der Region, Deutschlands und Europas bei. Sie fördern Innovationen, stärken die technologische Leistungsfähigkeit, verbessern die Akzeptanz moderner Technik und sorgen für Aus- und Weiterbildung des dringend benötigten wissenschaftlich-technischen Nachwuchses.

Ihren Mitarbeiterinnen und Mitarbeitern bietet die Fraunhofer-Gesellschaft die Möglichkeit zur fachlichen und persönlichen Entwicklung für anspruchsvolle Positionen in ihren Instituten, an Hochschulen, in Wirtschaft und Gesellschaft. Studierenden eröffnen sich aufgrund der praxisnahen Ausbildung und Erfahrung an Fraunhofer-Instituten hervorragende Einstiegs- und Entwicklungschancen in Unternehmen.

Namensgeber der als gemeinnützig anerkannten Fraunhofer-Gesellschaft ist der Münchner Gelehrte Joseph von Fraunhofer (1787–1826). Er war als Forscher, Erfinder und Unternehmer gleichermaßen erfolgreich.

Stand der Zahlen: Januar 2017
www.fraunhofer.de



IMPRESSUM

HERAUSGEBER
Fraunhofer-Institut für Kommunikation,
Informationsverarbeitung und Ergonomie FKIE

Fraunhoferstraße 20
53343 Wachtberg-Werthhoven

Tel.: +49 (0)228 9435-0
Fax: +49 (0)228 9435-685

kontakt@fkie.fraunhofer.de
www.fkie.fraunhofer.de

REDAKTION UND LEKTORAT
Anne Rindt

TEXTE
Christina Haberland, Anne Rindt, Silke Wiesemann,
Mitarbeiterinnen / Mitarbeiter des Fraunhofer FKIE

LAYOUT | SATZ | FOTOMONTAGE
Petra Kaiser

BILDQUELLEN
Bilder © Fraunhofer FKIE

Wachtberg-Werthhoven, Dezember 2017

AUSNAHMEN
Cover majkot + valex / 123RF® *Fotomontage*
Seite 10 iloveotto + somartin / 123RF® *Fotomontage*
Seite 11 Uwe Bellhäuser / das bilderwerk
Seite 14 - 15 Hans-Jürgen Vollrath / Ahr-Foto
Seite 31 viteethumb + szefei / 123RF® *Fotomontage*
Seite 33 erikona / iStock *Fotomontage*
Seite 35 nexusplexus / 123RF®
Seite 38 Uwe Bellhäuser / das bilderwerk
Seite 43 cooldesign / 123RF®
Seite 48 Uwe Bellhäuser / das bilderwerk
Seite 51 alphaspirit / 123RF®
Seite 53 bagotja / 123RF®
Seite 55 missisya / 123RF® *Fotomontage*
Seite 57 stevanovicigor / 123RF®
Seite 58 Uwe Bellhäuser / das bilderwerk
Seite 61 aneese / 123RF®
Seite 63 hxdyl / 123RF®
Seite 65 jirsak / 123RF®
Seite 66 Uwe Bellhäuser / das bilderwerk
Seite 69 oversnap / iStock
Seite 71 Yuri_Arcurs / iStock *Fotomontage*
Seite 79 Daimler AG
Seite 83 Vollrath (l.), Bellhäuser (r.)
Seite 84 Hans-Jürgen Vollrath / Ahr-Foto
Seite 85 Hans-Jürgen Vollrath / Ahr-Foto
Seite 87 Hans-Jürgen Vollrath / Ahr-Foto
Seite 90 Hans-Jürgen Vollrath / Ahr-Foto
Seite 104 - 105 Tawng / 123RF®