Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

JAHRESBERICHT 2019/20

SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

JAHRESBERICHT 2019/20

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

Ursula Fuchs
Stellvertretende Institutsleiterin
und Verwaltungsdirektorin

Prof. Dr. Peter Martini
Institutsleiter

Dr. Markus Antweiler
Stellvertretender Institutsleiter
und Leiter der Abteilung
Kommunikationssysteme (KOM)

VORWORT

Liebe Freunde und Partner des Fraunhofer FKIE,

funktionierende Infrastrukturen sind für eine Gesellschaft lebenswichtig. Dies gilt erst recht für Kritische Infrastrukturen (KRITIS), die für die Aufrechterhaltung zentraler Belange des sozialen und wirtschaftlichen Wohlergehens der Bevölkerung – wie der Energie-, Wasser- oder medizinischen Versorgung – essentiell sind. Sie sind besonders schützenswert, denn ihr Ausfall hätte sehr schnell dramatische Folgen für jeden einzelnen Bürger.

Wie alle Bereiche unserer modernen Gesellschaft unterliegen auch KRITIS dem Wandel einer fortschreitenden Digitalisierung. Neben großen Chancen für die Sicherung und Zukunftsfähigkeit des Wirtschaftsstandortes Deutschland birgt dies jedoch auch erhebliche Risiken: Unterschiedlichste Systeme und Strukturen sind immer stärker vernetzt und dadurch anfälliger für Störungen. Und bereits der Ausfall einer einzelnen Komponente kann in diesem komplexen Zusammenspiel kaskadenartig auf angeschlossene Strukturen übergreifen. Mit der Abhängigkeit der Gesellschaft von funktionierender IT steigen somit auch ihre Gefährdung und Verwundbarkeit.

Sicherheit für Kritische Infrastrukturen zu schaffen, ist daher ein öffentlicher Kernauftrag an Forschung, Industrie und Lehre. Und gemäß unserem Mission Statement »Wir arbeiten jeden Tag daran, die Welt sicherer zu machen« kommt das Fraunhofer FKIE dieser Aufgabe Tag für Tag in zahlreichen spannenden Forschungsprojekten nach. Sie vorzustellen, und damit das beeindruckende Portfolio unseres Instituts, haben wir zum Schwerpunkt dieses Jahresberichts gewählt. Die zugehörigen Beiträge finden Sie mit einem Spotlight-Symbol markiert.

Freuen Sie sich auf einen Blick hinter die Kulissen und in die Labore unserer neun Forschungsabteilungen, die an so herausfordernden Aufgabenstellungen arbeiten wie dem Cyber-Schutz unserer Stromversorgung, an CBRNE-Robotik zur Unterstützung bei Unfällen in Atomkraftwerken, an KI-Tools zur Enttarnung von Fake News in den Sozialen Medien, an Systemen zur Erkennung und Abwehr von Drohnen in terroristischen Szenarien, an Sensor-Lösungen für die Zutritts- und Sabotageüberwachung von Hochrisiko-Forschungsflächen und vielem mehr.

Die vergangenen zwei Jahre waren erneut – wissenschaftlich wie wirtschaftlich – besonders erfolgreiche Jahre für unser Institut. Der Dank hierfür gebührt allein den engagierten FKIE-Mitarbeiterinnen und -Mitarbeitern, die sich Tag für Tag mit Begeisterung, Forscherdrang und großem Know-how den wachsenden Herausforderungen sicherheitskritischer Fragestellungen stellen. Mit Stolz möchten wir Ihnen daher auch in dieser Ausgabe wieder einige von ihnen und ihre besonderen Karrierewege vorstellen.
Ich wünsche Ihnen eine spannende Lektüre und freue mich schon jetzt auf zahlreiches Feedback und den persönlichen Austausch mit Ihnen, den ein Bericht wie dieser initiieren sollte!

Herzlichst, Ihr

Prof. Dr. Peter Martini
Institutsleiter

Spotlights

- Schwerpunkt »Sicherheit für Kritische Infrastrukturen«
- Sensorbasierte Zutrittsüberwachung
- Fake News-Klassifizierung
- Der Faktor Mensch in der Cybersicherheit
- Erkennung von Cyberangriffen
- Drohnenabwehr
- Cybersicherheit für maritime IT-Systeme
- Hafenüberwachung durch Passivradar
- Aufbau des Deutschen Rettungsrobotik-Zentrums

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

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE ist **der** strategische Partner für die Bundeswehr, Behörden und Organisationen mit Sicherheitsaufgaben sowie für Industrie und Dienstleister. Als führendes Institut für anwendungsorientierte Forschung und praxisnahe Innovation in der Informations- und Kommunikationstechnologie verfolgen wir gemeinsam das Ziel, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen.

Forschung für Verteidigung und Sicherheit ist für das Fraunhofer FKIE bei der Entwicklung von Technologien und Prozessen mehr als nur ein Auftrag. Die verlässliche und vertrauensvolle Unterstützung ziviler und wehrtechnischer Partner bei Führungs- und Aufklärungsprozessen bedeutet für die rund 490 Mitarbeiterinnen und Mitarbeiter des Instituts Herausforderung, Chance und Mission zugleich.

Als Forschungsinstitut leistet das Fraunhofer FKIE seinen aktiven Beitrag dazu, die Handlungsfähigkeit seiner Kooperationspartner und damit sämtliche Bereiche der Sicherheit in Deutschland zu gewährleisten: auf dem Boden, in der Luft, zur See, unter Wasser oder im Cyberspace. Hierbei haben die Wissenschaftlerinnen und Wissenschaftler die gesamte Verarbeitungskette von Daten und Informationen im Blick: vom Gewinn, der Übertragung und Verarbeitung über die nutzergerechte Anwendung bis hin zu ihrem zuverlässigen Schutz.

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

Dabei hat der »Faktor Mensch« stets zentrale Bedeutung: Bei der Entwicklung effektiver und effizienter Mensch-Maschine-Systeme bleibt er der Dreh- und Angelpunkt und als Entscheider letztlich verantwortlicher Akteur.

Schwerpunktmäßig forschen die Wissenschaftlerinnen und Wissenschaftler am Fraunhofer FKIE in fünf Themenfeldern, in denen sie umfangreiches Domänenwissen aufgebaut haben:

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

Die Forschungsleistungen erstrecken sich von Studien und Tests bis hin zur Entwicklung von Prototypen. Dank insgesamt neun 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.

Als verlässlicher, strategischer Partner für die Innere Sicherheit stellt sich das Fraunhofer FKIE Tag für Tag den aktuellen wissenschaftlich-technologischen Herausforderungen – mit Kompetenz in der Breite und Exzellenz im Detail.

ANSPRECHPARTNER

INSTITUTSLEITER

Prof. Dr. Peter Martini
Telefon 0228 9435-217
peter.martini@fkie.fraunhofer.de

STELLV. INSTITUTSLEITUNG

VERWALTUNGSDIREKTORIN

Ursula Fuchs
Telefon 0228 9435-886
ursula.fuchs@fkie.fraunhofer.de

STELLV. INSTITUTSLEITUNG

Abteilungsleiter
KOMMUNIKATIONSSYSTEME

Dr. Markus Antweiler
Telefon 0228 9435-810
markus.antweiler@fkie.fraunhofer.de

Abteilungsleiter
SENSORDATEN- UND INFORMATIONSFUSION

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

Abteilungsleiter
INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME

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

Abteilungsleiter
KOGNITIVE MOBILE SYSTEME

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

Leiter
STRATEGIE & MARKTERSCHLIESSUNG

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

Leiterin
WISSENSCHAFTS-KOMMUNIKATION

Anne Rindt
Telefon 0228 9435-734
anne.rindt@fkie.fraunhofer.de

IT-STANDORT BONN

ZENTRUM DER OPERATIVEN CYBER SECURITY
STRATEGISCHE PARTNER

ZENTRUM DER OPERATIVEN CYBER SECURITY

Das Fraunhofer FKIE befindet sich in prominenter Gesellschaft, wenn es in Bonn und der Region um das Thema Cyber Security geht: Das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR), die Bundespolizei, die Polizei NRW, die Deutsche Telekom, aber auch viele mittelständischen Unternehmen beschäftigen sich mit der Sicherheit im Cyberraum. Diese wichtigen Akteure haben sich im Cyber Security Cluster Bonn e.V. zusammengeschlossen und verfolgen gemeinsam das Ziel, sich der wachsenden Bedrohung durch Angriffe auf IKT-Systeme entgegenzustellen.

Bonn ist längst das Zentrum der operativen Cyber Security in Europa, betont Prof. Dr. Peter Martini, Fraunhofer FKIE-Institutsleiter, Lehrstuhlinhaber in der Informatik der Exzellenzuniversität Bonn und gleichzeitig auch stellvertretender Vorstandsvorsitzender des Clusters. Der Blick auf die lange Liste der Top-Player im Bereich der IT-Sicherheit in Bonn und der Region zeige, wie wichtig an dieser Stelle eine sinnvolle Vernetzung sei, denn Cyber Security stelle eine der größten Herausforderungen für die Zukunft der Gesellschaft dar. »Die fortschreitende sichere Digitalisierung kann nur als Gemeinschaftsprojekt umgesetzt werden. Deutlich wird das vor allem bei gravierenden Sicherheitsvorfällen im Cyberspace. Dann wendet man sich an die wirklich wichtigen Institutionen – und die arbeiten alle von Bonn aus.«

Höchstsicherheit als Alleinstellungsmerkmal

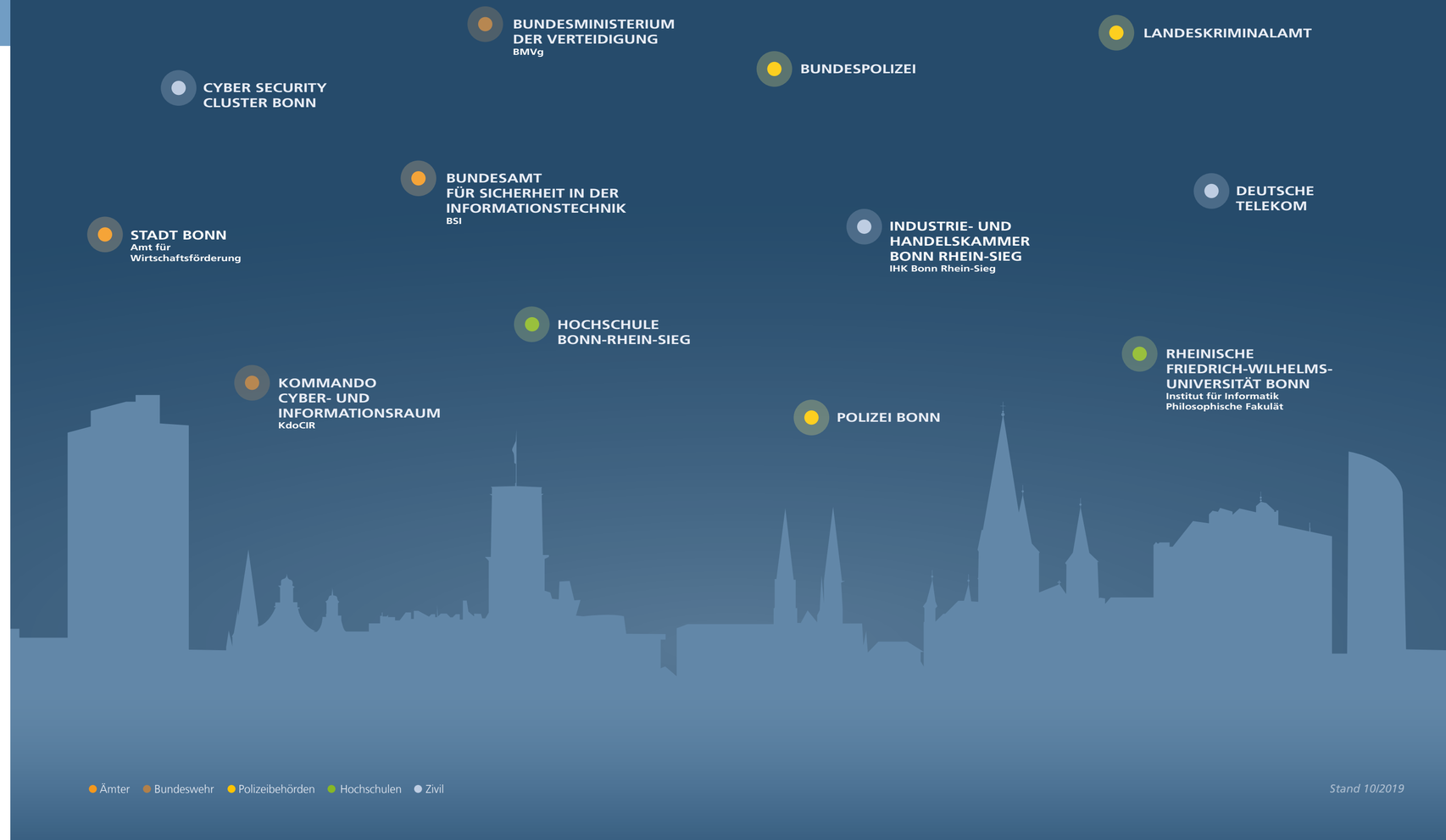
Unterstrichen wurde dies auch von Prof. Dr. Reimund Neugebauer, Präsident der Fraunhofer-Gesellschaft, der der persönlichen Einladung von Professor Martini zur Gründungsveranstaltung des Clusters im November 2018 gefolgt war: Bonn habe ein wichtiges Alleinstellungsmerkmal und stünde im Bereich Cyber Security für Höchstsicherheit. Dies werde auch an der Fokussierung des Lernlabors Cybersicherheit des Fraunhofer FKIE deutlich, das sich im Rahmen von Weiterbildungsmaßnahmen und Fortbildungen auf die Themenfelder »Hochsicherheit & Emergency Response« spezialisiert hat.

Wichtiger Baustein in der Arbeit des Cyber Security Cluster ist neben der Vernetzung der Akteure auch die Errichtung eines Weisenrates, dessen Aufgabe es künftig sein wird, Politik und Wirtschaft Empfehlungen in Sachen IT-Sicherheit zu geben. Auch in diesem Gremium, das insgesamt sechs Wissenschaftlerinnen und Wissenschaftler umfasst, ist das Fraunhofer FKIE deutlich sichtbar vertreten: mit Professor Dr. Matthew Smith, Informatik-Professor an der Universität Bonn und Leiter der Abteilung »Usable Security and Privacy« am Fraunhofer FKIE, sowie mit Prof. Dr. Delphine Reinhardt, aktives Mitglied des FKIE-Kuratoriums und frühere Abteilungsleiterin am Institut. Angelehnt ist dieses Gremium an die fünf Wirtschaftsweisen, die sich als Sachverständigenrat wissenschaftlich mit der Lage der wirtschaftlichen Entwicklung Deutschlands befassen und Empfehlungen aussprechen.

Bonn als das »Davos der Cyber Security«

Weitere Analogie zur Wirtschaft ist das Ziel des Cluster, Bonn langfristig als »das Davos der Cyber Security« zu etablieren. Durch den Schulterschluss der Akteure aus Wirtschaft, Politik und Forschung sowie der Zusammenführung von Kompetenzen, Netzwerken und High-End-Technologien könne sich hier »eine Armee der Guten mit der notwendigen Schlagkraft aufbauen, die sich der Armee der Bösen spürbar entgegenstellt«, erläuterte Dirk Backofen, Vorstandsvorsitzender des Clusters und Leiter der Telekom Security, anlässlich des Cyber Security Tech

STRATEGISCHE PARTNER



Stand 10/2019

Summit in Bonn im März 2019. Die zweitägige Veranstaltung mit mehr als 2.000 Teilnehmern im World Conference Center Bonn (WCCB) soll sich künftig zur jährlichen Flagschiff-Veranstaltung des Cluster entwickeln, bei der aktuellste Themen aus dem Bereich der Cybersicherheit auf der Agenda stehen werden.

Ziel: Mehr qualifizierte Arbeitnehmer

Auf die Fahnen geschrieben haben sich auch alle Cluster-Mitglieder, die Aus- und Weiterbildung im Bereich IT-Sicherheit zu stärken, da der Bedarf an qualifizierten Mitarbeitern aus dem IT-Sektor in allen Branchen groß ist – sei es Industrie, Verwaltung, Polizei oder Forschungseinrichtungen. Folgerichtig zählen natürlich auch die Universität Bonn, die Hochschule Bonn-Rhein-Sieg und die Industrie- und Handelskammer Bonn/Rhein-Sieg neben dem Fraunhofer FKIE, dem BSI, der Polizei Bonn und dem KdoCIR zu den Gründungsmitgliedern und Unterstützern des Clusters. Der hohen Nachfrage nach IT-Sicherheitsfachleuten vor allem am Standort Bonn kam die Universität Bonn mit der Einführung eines neuen Studiengangs »Cyber Security« entgegen. Zum Wintersemester 2019/2020 startet das Bachelor-Studienangebot, ab 2022 schließt sich der Master-Studiengang an. Mit Unterstützung der Partner aus dem Cyber Security Cluster will die Uni die essentiellen Grundlagen der IT-Sicherheit an ihre Studierenden vermitteln. Federführend mitgewirkt hat bei der Entwicklung des Studiengangs auch Prof. Dr. Michael Meier, Inhaber des Lehrstuhls für IT-Sicherheit am Bonner Institut für Informatik und Leiter der Abteilung »Cyber Security« am Fraunhofer FKIE.

Errichtung der Secure Digital City Bonn

Technologisch setzt das Cluster mit seinen Mitgliedern Akzente in Bonn und der Region: Unter dem Motto »Secure Digital City Bonn« gibt es konkrete Planungen, einen Bonner Stadtteil zum Schaufenster, Gestaltungs- und Erlebnisraum für sichere Digital-Technologie zu machen. Hier sollen sichere schlüssellose Zugangssysteme, intelligentes Parken, der hohe Stellenwert und auch die hohe Schutzbedürftigkeit digitaler Identität ebenso erlebbar gemacht werden wie autonomes Fahren oder digitales Bezahlen – nicht als Stückwerk bzw. Fleckenteppich, sondern in integrierten Gesamtkonzepten im lebendigen Zusammenspiel mit der analogen Welt. Bereits heute steht Bonn im Smart City Index, der im Auftrag des Digitalverbandes Bitkom in gründlicher Recherche erstellt wurde, unter den Top 10 der digitalen Städte.

SCHWERPUNKT »SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN«

INTERVIEW
MARITIME AWARENESS
ENERGIE-SEKTOR
CBRNE-SCHUTZ
SICHERHEIT FÜR EINSATZKRÄFTE

INTERVIEW

Gespräch mit **Peter Lauwe, Leiter des Referates »Risikomanagement KRITIS und Schutzkonzepte KRITIS« im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe**

Kritische Infrastrukturen werden oft als »die Lebensadern unserer Gesellschaft« bezeichnet. Mit zunehmender digitaler Vernetzung steigt jedoch auch hier das Gefährdungspotenzial durch unterschiedliche kriminelle Bedrohungen. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) hat die Aufgabe, den Schutz Kritischer Infrastrukturen zu koordinieren und hierbei ganzheitliche Schutzkonzepte zu etablieren.

Welche Bereiche zählen Sie zu den Kritischen Infrastrukturen?
Kritische Infrastrukturen werden zum einen in einer Definition grundsätzlich beschrieben. Zum anderen sind die Sektoren und Branchen festgelegt, in denen Kritische Infrastrukturen vorkommen. Definition und Sektoren sind in einer Nationalen Strategie zum Schutz Kritischer Infrastrukturen aufgeführt. Zu den Kritischen Infrastrukturen zählen die Energieversorgung, die Informations- und Kommunikationstechnik oder der Bereich Parlament, Regierung, öffentliche Verwaltung und Justizeinrichtungen. Daran kann man erkennen, dass sowohl Unternehmen als auch Behörden Kritische Infrastrukturen betreiben.

Welche davon sind besonders sensibel?
Alle Kritischen Infrastrukturen sind grundsätzlich wichtig bzw. bedeutsam. Sehr hohe Abhängigkeiten bestehen von der Stromversorgung, von Informations- und Kommunikationstechnik (IKT) und unmittelbar oder mittelbar von Transportleistungen. Diese drei Bereiche übernehmen damit in hohem Maße eine querschnittliche Funktion für alle Kritischen Infrastrukturen. Die Sensibilität bzw. Verwundbarkeit Kritischer Infrastrukturen hängt von unterschiedlichen Aspekten ab, beispielsweise von dem Stand der Notfallplanungsmaßnahmen in den Unternehmen und Behörden.

Wird in Deutschland genug unternommen, um Kritische Infrastrukturen vor Angriffen von außen zu schützen?
In Deutschland gibt es seit dem 19. Jahrhundert umfangreiche Vorgaben für den Bau und den Betrieb von Infrastrukturen. Der Aspekt »Sicherheit« spielt dabei von Anfang an auch eine Rolle. Dies beginnt mit Vorgaben, die von regionalen Industrievereinen und Vereinigungen im Zuge der Industrialisierung erlassen wurden. Im 20. Jahrhundert ist der Großteil der sektoralen Gesetze entstanden. Dazu zählt beispielsweise das Energiewirtschaftsgesetz, das ebenfalls Vorgaben zum sicheren Betrieb der Energieversorgung formuliert.

Das Thema »Schutz Kritischer Infrastrukturen« wurde in den 1990er Jahren als Annexthema verankert. Zusätzlich zu den sektoralen Vorgaben sollte ein querschnittlicher Blick auf solche Infrastrukturen gelegt werden, die für die Gesellschaft von besonders hoher Bedeutung sind. Neue Gefährdungen und Interdependenzen sollten erkannt sowie Ergänzungen zum Schutz vorgenommen werden. Das IT-Sicherheitsgesetz ist sicherlich ein gutes Beispiel für die Ergänzung des gesetzlichen Rahmens.

Wo sehen Sie den größten Handlungsbedarf?
Betreiber Kritischer Infrastrukturen sind in vielen Bereichen sensibilisiert und setzen viele Maßnahmen zur Sicherung ihrer Dienstleistungen um. Allerdings gibt es aus unserer Sicht auch noch viel Handlungsbedarf, da sich sowohl die Kritischen Infrastrukturen als auch die Risiken stetig verändern. An dieser Stelle kann ich nur Beispiele nennen. So sehen wir zum Beispiel großen Handlungsbedarf in der zunehmenden Systematisierung der Zusam-

INTERVIEW

menarbeit von staatlichen Akteuren und Betreibern Kritischer Infrastrukturen im Risikomanagement (Integriertes Risikomanagement). Die Zusammenarbeit von staatlichen Stellen und Betreibern Kritischer Infrastrukturen funktioniert in Teilen sehr gut. Eine stärkere Systematisierung dieser Zusammenarbeit wäre sinnvoll. Dabei geht es um den weiterreichenden Austausch von Erkenntnissen und die gemeinsame Bewertung von Risiken. Auch die zunehmende Umsetzung von Maßnahmen in geteilter Verantwortung können wir uns vorstellen. Eine in der Veröffentlichung befindliche DIN SPEC mit dem Titel »Integriertes Risikomanagement« bietet Anstöße, den Austausch zu intensivieren.

»Wir müssen lernen, mit den Veränderungen umgehen zu können, um auch zukünftig den Schutz Kritischer Infrastrukturen gewährleisten zu können.«

Von großer Bedeutung ist ebenso die Kommunikation zwischen staatlichen und nichtstaatlichen Akteuren im Krisenfall. Der Kommunikationsbedarf zwischen staatlichen Stellen und Betreibern Kritischer Infrastrukturen ist insbesondere im Krisenfall hoch. Fallen Kommunikationsmöglichkeiten wie Telefon oder Internet aus, muss auf Notsysteme zurückgegriffen werden. Diese bieten derzeit nur bedingt die Voraussetzungen für eine ausreichende Kommunikation. Es besteht ein Bedarf an ergänzenden Lösungen, um den Austausch zu gewährleisten.

Bei der Nutzung innovativer Technologien möchte ich beispielhaft die stärkere Nutzung von Modellen zur Auswirkungsprognose hervorheben. Im wissenschaftlichen Bereich liegen viele Forschungsergebnisse dazu vor. In der Praxis werden solche Modelle noch nicht umfänglich genutzt. Dabei spielt sicherlich der Zugang zu Daten eine Rolle. Aber auch die Komplexität der Modelle. Die Frage, wie man innovative Technologien verstärkt in der Praxis nutzen kann, ist sicherlich noch nicht umfassend beantwortet.

Insbesondere vor dem Hintergrund einer steigenden Komplexität in Kritischen Infrastrukturen müssen in stärkerem Maße einfache Rückfallebenen geschaffen werden. Auf sie kann zurückgegriffen werden, wenn Kritische Infrastrukturen in ihrer Funktionsfähigkeit erheblich beeinträchtigt sind. In der Frage, wie diese Rückfallebenen im 21. Jahrhundert aussehen sollten, sehen wir ebenfalls Handlungsbedarf.

Als letztes Beispiel möchte ich den spezifischen Bereich der Notfallplanung nennen. Vor dem Hintergrund möglicher langanhaltender und großräumiger Schadensszenarien wurden von Kommunen sowie von Länder- und Bundesseite in den letzten Jahren Maßnahmen angestoßen. Mögliche massive Stromausfälle wurden beispielsweise intensiv betrachtet. In Teilbereichen besteht noch Klärungs- und Handlungsbedarf. Beispielsweise bei der Verteilung wichtiger Güter wie Treibstoff oder Medikamente bei großen Schadenslagen.

Können Sie zahlenmäßig darstellen, wie viele Angriffe auf Kritische Infrastrukturen pro Jahr in Deutschland erfolgreich abgewehrt werden?
Angriffe aus dem Cyberraum in unterschiedlicher Qualität werden von Kritischen Infrastrukturen stetig abgewehrt.

Bedrohungsszenarien für Kritische Infrastrukturen werden in den Medien oft konkret dargestellt. Was bedeutet diese wachsende öffentliche Aufmerksamkeit für die Entwicklung von Schutzkonzepten oder für die Mitarbeiter, die für den Schutz der kritischen Systeme verantwortlich sind?
Mit der steigenden Sensibilisierung steigt natürlich auch der Handlungsdruck. Wichtig ist, diesen zu kanalisieren und erforderliche Ergänzungen zu erkennen und vorzunehmen. Das BBK hat in den letzten Jahren zahlreiche Empfehlungen herausgegeben und an Standards mitgearbeitet, deren Anwendung zur Schließung von Lücken im Risiko- und Krisenmanagement beitragen können.

Wie können Akteure im Risikomanagement besser zusammenarbeiten?
Akteure können Erkenntnisse und Ergebnisse aus ihrem jeweiligen Risikomanagement verstärkt austauschen. In einem Projekt, das wir begleiten durften, hat ein Betreiber Kritischer Infrastrukturen die Gebiete in einem Kreis gekennzeichnet, in denen bei Stromausfall seine Dienstleistung nicht mehr zur Verfügung steht. Für die Feuerwehren in diesem Kreis waren dies wertvolle Informationen für die Notfallplanung. Das ist ein gutes Beispiel für eine übergreifende Zusammenarbeit. Eine systematische Verknüpfung unterschiedlicher Akteure wird in der bereits erwähnten DIN SPEC vorgenommen. In der Umsetzung treten zukünftig sicherlich noch viele Fragen auf, die sukzessive geklärt werden müssen.

Welche Entwicklungen werden für die Zukunft angestrebt? Wo sehen Sie künftige Unterstützungsmöglichkeiten durch Forschungsinstitute wie zum Beispiel das Fraunhofer FKIE?
Die Komplexität der einzelnen Infrastrukturen und die Komplexität des Zusammenwirkens von Infrastrukturen werden stetig steigen. Auch die Risiken verändern sich und nehmen teilweise zu. Wir müssen lernen, mit den Veränderungen umgehen zu können, um auch zukünftig den Schutz Kritischer Infrastrukturen zu gewährleisten.

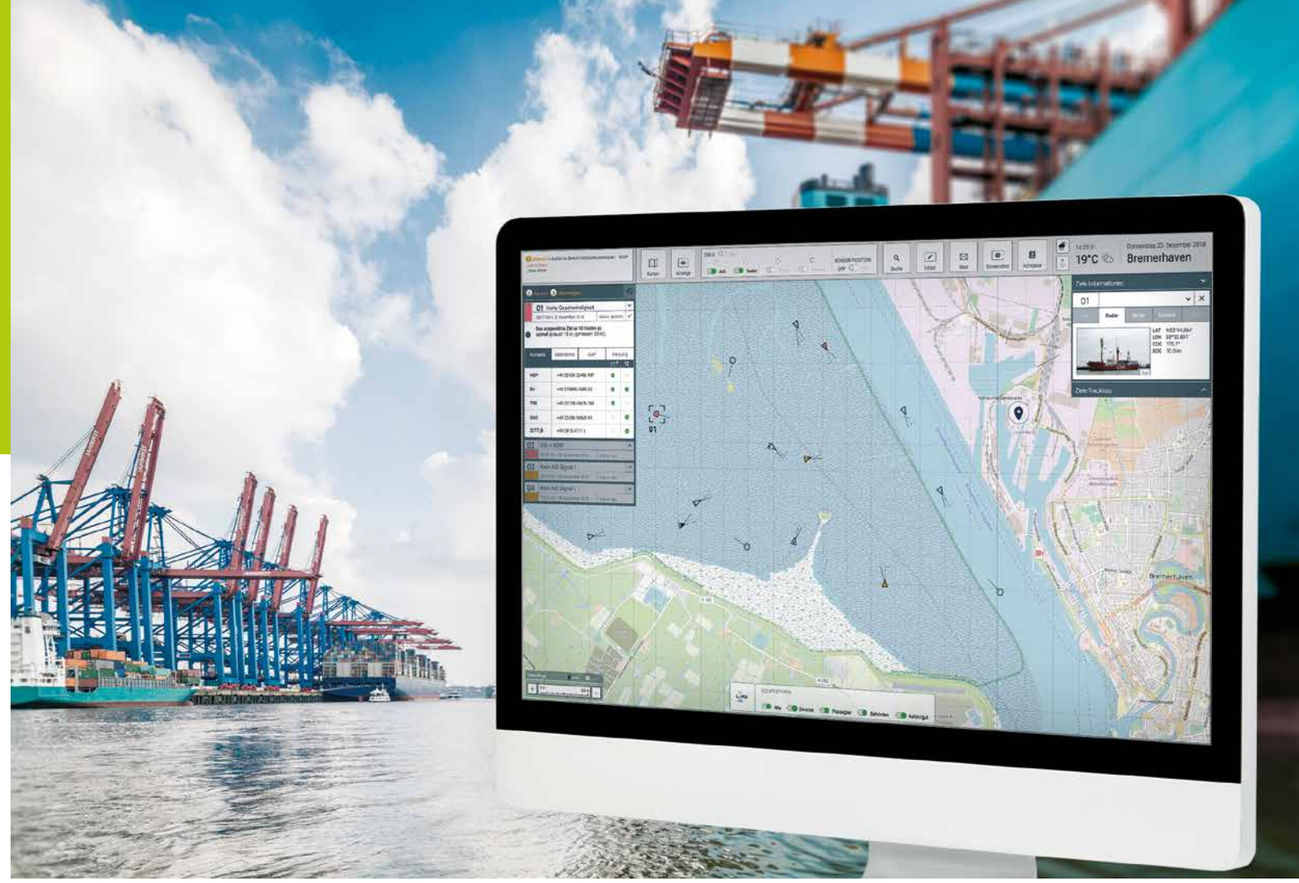
Dabei sind aus meiner Sicht zwei Entwicklungen wichtig: Zum einen sollten wir trotz oder wegen der Komplexität die Ausfallsicherheit der Systeme weiter ausbauen und dabei den Aspekt der Resilienz der Systeme von der Planungsphase an umfänglich mitdenken. Zum anderen benötigen wir einfache Rückfallebenen in den Kritischen Infrastrukturen, die im Fall schwerwiegender Störungen eine Aufrechterhaltung der Versorgung der Bevölkerung in Teilen ermöglicht. Es gibt sicherlich einen hohen Bedarf an Unterstützung bei allen Akteuren. Viele Fragen können auch nur mit wissenschaftlicher Unterstützung geklärt werden. Auch an dieser Stelle kann ich nur einige Fragen beispielhaft nennen, die für uns noch nicht ausreichend geklärt sind: Wie verändern sich Kritische Infrastrukturen in Zukunft? Welche Rolle spielt bei dieser Entwicklung Künstliche Intelligenz? Was bedeuten diese Veränderungen für die Versorgungssicherheit? Wie können Prognosefähigkeiten bezüglich potenzieller Auswirkungen in der Praxis verbessert werden? Welche zunehmende Rolle spielt die Datennutzung beim Schutz Kritischer Infrastrukturen? Wie müssen/sollten rechtliche Grundlagen weiterentwickelt werden? Wie müssen/sollten Standards weiterentwickelt werden?

Peter Lauwe
Leiter des Referates »Risikomanagement KRITIS und Schutzkonzepte KRITIS« im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

MARITIME AWARENESS

MARITIME AWARENESS

LAGEBILDOPTIMIERUNG FÜR DEN HAFENSCHUTZ



Hafenüberwachung auf, über und unter dem Wasser

Terroristische Anschläge, Drogenschmuggel, Wirtschaftskriminalität – denkbare Szenarien für illegale Machenschaften, die sich zu Wasser, an Land und in der Luft von Hafengebieten abspielen, gibt es zuhauf. Leider nicht nur fiktiv, sondern auch real, womit sie die Sicherheitslage gefährden. Im Rahmen eines durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Forschungsvorhabens entwickelt das Fraunhofer FKIE zusammen mit ATLAS Elektronik und Bremenports ein ziviles Hafenüberwachungssystem.

Ein Hafen ist eine komplexe Kritische Infrastruktur. Eine Vielzahl von Menschen und Technik ist an seiner Funktion und Organisation beteiligt. Die Gewährleistung der Hafensicherheit ist dabei ein wesentlicher Aspekt. Zur Überwachung des Hafens müssen zahlreiche Informationen über und unter dem Wasser vorliegen, die beispielsweise durch Kamera-, Radar- und Sonarsensoren erfasst werden können. Um ein zuverlässiges Lagebild zu generieren, müssen diese Daten zusammengeführt und weiterverarbeitet werden. Mit dieser Aufgabe befasst sich das Projekt LOMA, kurz für »Lagebildoptimierung für Maritime Awareness«. Es ist das erste Projekt, das vom Bundesministerium für Wirtschaft und Energie (BMWi) im Rahmen seines Förderschwerpunkts »Echtzeittechnologien für maritime Sicherheit« bewilligt wurde.

Ausgangsszenario: Angriff von Wasserseite

Ziel des Mitte 2017 gestarteten, dreijährigen Forschungsvorhabens für die zivile Hafensicherheit ist die Entwicklung eines umfassenden Hafenüberwachungssystems. Umgesetzt wird es in einem Konzept, das neben einem integrierten Lagebild eine Anomalie-Detektion mit Frühwarnsystem und adaptiver Entscheidungsunterstützung vorsieht. »Prinzipiell könnte diese Lösung überall eingesetzt werden, wo es Kritische Infrastrukturen zu schützen gilt«, hebt FKIE-Wissenschaftlerin Christina Seimetz das mögliche Einsatzspektrum des künftigen Systems hervor. »Ausgangsszenario in diesem Projekt ist der gezielte Angriff eines Hafens von der Wasserseite.« Angesichts einer zunehmenden terroristischen Bedrohung stellt diese Art von Vorfall eine der Gefahrenlagen dar, mit der Hafenbetreiber und -behörden rechnen müssen. Sie möchten daher gerüstet sein.

Frühzeitige Alarmierung bei verdächtigen Bewegungen

LOMA soll dabei unterstützen, auffällige Bewegungen auf und unter dem Wasser frühzeitig zu detektieren, das Objekt zu identifizieren und die Nutzer zu alarmieren. Hierzu fasst das System Daten und Informationen aus unterschiedlichen Quellen zu einer Informationslage zusammen und stellt sie den Sicherheitsverantwortlichen zur Verfügung. Eine Besonderheit des Projekts ist, dass dabei auf unterschiedlichste Sensoren zurückgegriffen wird, deren Daten durch Fusion valide nutzbar gemacht werden: Neben dem Automatic Identification System (AIS), einem Transpondersystem zum Austausch von Navigations- und anderen Schiffsdaten, integriert und bewertet das System die Daten von Radar-, Kamera- und Sonarsensoren sowie Schiffsmeldedaten. Ein weiterer Fokus des Projekts ist auf die integrative Darstellung, Alarmierung und Entscheidungsunterstützung gerichtet. Schwerpunkte des Arbeitsanteils des Fraunhofer FKIE in dem Verbundprojekt sind das Informationsmanagement in Form von Sensordatenintegration, Anomaliedetektion, Objektbewertung und -klassifikation sowie die ergonomische Darstellung aller fusionierten Informationen. »Da es sich um ein ziviles Projekt handelt, werden Gegenmaßnahmen nur in Form von Handlungsoptionen betrachtet«, erläutert Seimetz. »Ziel ist es, ein verdächtiges Objekt möglichst früh zu erkennen, seine Route zu tracken und die Bedrohung zu analysieren, um basierend auf Systemvorschlägen adäquat reagieren zu können. So soll ein potenzieller Anschlag im Idealfall verhindert werden.«

Interaktive Karte als zentrales Element des Lagebilds

Zur möglichst nutzungsfreundlichen Aufbereitung des fusionierten Lagebilds entwickelte das FKIE-Team ein Human Machine Interface, dem die Parameter Übersichtlichkeit, Einfachheit und Situationsbewusstsein zugrunde liegen. Es basiert auf praktischen Nutzungsanforderungen, die durch Befragungen, Usability-Untersuchungen, Experimenten und Experten-Reviews ermittelt wurden. Seimetz: »Entstanden ist eine adaptive und intuitive, aufgeräumte Oberfläche, deren zentraler Bestandteil eine große Karte ist. Mit dieser können die Nutzer vielfach interagieren, sich zum Beispiel Informationen bedarfsgerecht ein- oder ausblenden lassen. Zudem werden automatisch Warnmeldungen und Entscheidungshilfen angezeigt. Diese sollen dabei unterstützen, Entscheidungen möglichst sicher und effizient zu treffen. Ziel ist, zu diesem Zweck alle vom System bewerteten, relevanten Informationen möglichst auf einen Blick zu bieten.«

Testkampagne mit realen Szenarien in Bremerhaven

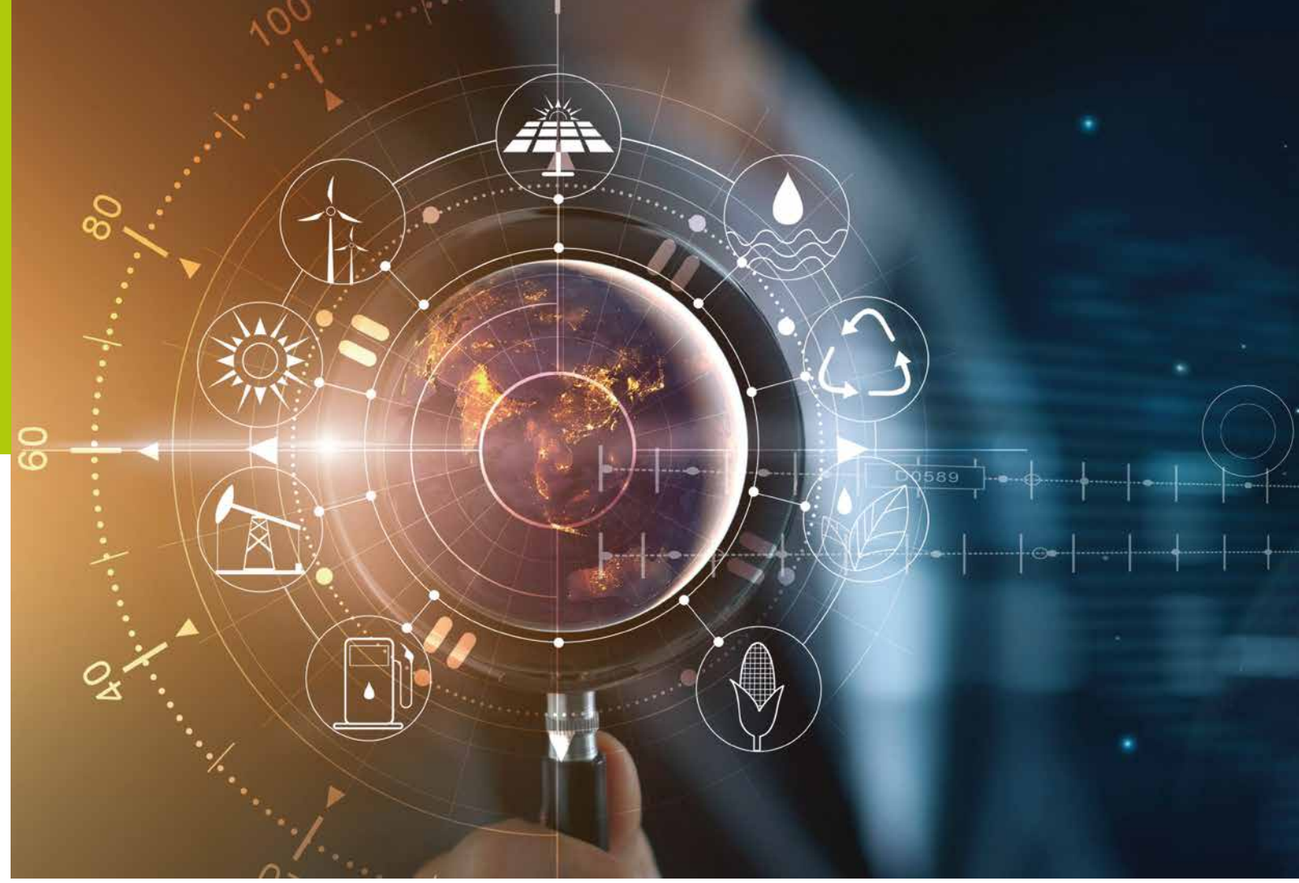
Betreut wird das bis Mitte 2020 laufende Forschungsvorhaben durch den Projektträger Jülich, die Projektleitung im Verbund obliegt der ATLAS Elektronik GmbH. Weiterer Projektpartner ist der Hafeninfrastruktur-Dienstleister Bremenports GmbH, der den Kontakt zu den Stakeholdern sowie die Testkampagnen koordiniert und mit Fachexpertise unterstützt. Nächster Meilenstein des Verbundprojekts ist eine große Testkampagne unter realen Bedingungen und mit realen Szenarien in Bremerhaven. Hier soll das System seine Leistungsfähigkeit unter Beweis stellen.

KONTAKT
Christina Seimetz
Telefon +49 228 9435-474
christina.seimetz@fkie.fraunhofer.de

ENERGIE-SEKTOR

ENERGIE-SEKTOR

CYBERSICHERE STROMVERSORGUNG



Das Stromnetz – die kritischste aller Kritischen Infrastrukturen

Eine gesicherte Stromversorgung ist für unsere Gesellschaft längst zu einer Selbstverständlichkeit geworden: Energiesicherheit 24/7 an 365 Tagen im Jahr wird vorausgesetzt. Ohne Strom finden Produktion, Mobilität, Kommunikation und Handel nicht statt. Dementsprechend gilt eine zuverlässige, bezahlbare und dauerhaft verfügbare Energieversorgung als das Rückgrat heutiger Industrienationen. Die fortschreitende Digitalisierung der Energiebranche bringt allerdings neben großen Chancen für die Sicherung des Wirtschaftsstandorts auch erhebliche Risiken mit sich: Die Verwundbarkeit der Energiesysteme steigt.

Ein erfolgreicher Angriff auf Stromnetze und Kraftwerke, der wohl kritischsten aller Kritischen Infrastrukturen, hätte nicht nur weitreichende Folgen für das betroffene Land, sondern für den gesamten Wirtschaftsraum der Europäischen Union. Derartige Angriffe sind jedoch keine Fiktion mehr, sondern für Unternehmen der Energiebranche schon lange Alltag. Auch handelt es sich dabei nicht mehr nur um einzelne Hackerangriffe, sondern längst haben sich diese zu ganzen Angriffskampagnen ausgewachsen, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) immer wieder betont. Die Notwendigkeit cybersicherer, resilienter Energiesysteme zeigt sich deutlich.

Bedrohung aus dem Cyberraum

Um die fortschreitend digitalisierte Energieversorgung also möglichst zielführend, anwendungsnah und verantwortungsvoll zu schützen und weiterzuentwickeln, ist eine Neuausrichtung der darauf spezialisierten Forschungs- und Industriezweige erforderlich. Ziel ist dabei die Schaffung einer zuverlässigen, effizienten und resilienten Energieversorgung, auch oder vielmehr gerade vor dem Hintergrund der Energiewende. Denn der Energiesektor vollzieht aktuell einen tiefgreifenden Wandel: Historisch gewachsene, unabhängige Infrastrukturen transformieren zu einem wechselwirkenden, digitalisierten und automatisierten Gesamtsystem, das unterschiedliche Sektoren und Stakeholder eng miteinander verbindet. Um in Zukunft Versorgungszuverlässigkeit zu gewährleisten, Digitalisierung und Automatisierung als Wirtschaftsfaktor weiter voranzutreiben, Planung und Betrieb von Energieversorgungssystemen durch digitale Abbilder zu verbessern und der Bedrohung aus dem Cyberraum adäquat begegnen zu können, bedarf es eines konzertierten Vorgehens aller verantwortlichen Akteure.

Gründung der Forschungskooperation »Digitale Energie«

Auf Grund der realen Bedrohungen des Energiesektors bedarf es neuer, praktischer Werkzeuge, Handlungskonzepte sowie interdisziplinärer IT-Sicherheitstools zur Unterstützung der Netzbetreiber. Das Ziel muss sein, dass alle Schutzmaßnahmen von Wirtschaft, Staat und Gesellschaft bestmöglich ineinander greifen. Um den Bedrohungen rechtzeitig zu begegnen, hat das Fraunhofer FKIE hierzu gemeinsam mit starken Partnern wie dem Fraunhofer-Institut für Angewandte Informationstechnik FIT und der RWTH Aachen das Fraunhofer-Zentrum für »Digitale Energie« als Forschungskooperation gegründet. Die Akteure arbeiten daran, die vielfältigen Herausforderungen im Bereich »Sicherung des Energiesektors« verstärkt gemeinsam und interdisziplinär anzugehen. Hier werden domänenübergreifende Kompetenzen in den Schlüsselbereichen Energietechnik, Digitalisierung, IT-Sicherheit und Wirtschaft gebündelt.

»Wir brauchen eine interdisziplinäre, unabhängige, sofort einsatzfähige Forschung, um die effiziente, resiliente Energieversorgung sicherzustellen«, so Dr. Elmar Padilla, Abteilungsleiter »Cyber Analysis and Defense« am Fraunhofer FKIE und einer der Initiatoren dieser Forschungskooperation. Dies gelinge allerdings nur, wenn dabei die Themen neue Technologien und Verfahren, Fachkräftemangel sowie Integration von Forschungsergebnissen zielgerichtet mittels der drei tragenden Säulen »Forschung und Entwicklung«, »Aus- und Weiterbildung« sowie »Test- und Prüfverfahren« adressiert werden.

Wohlstand, Wachstum und Frieden

Im Fokus des Beitrags des Fraunhofer FKIE stehen dabei Forschung und Entwicklung im Hinblick auf alle Aspekte der Cyber Security. Dies beinhaltet insbesondere die Punkte Prävention, Detektion und Reaktion bezüglich einzelner Systeme im Energieverbund. Dieser Dreiklang muss adressiert werden, um Cybersicherheit, Resilienz und Versorgungszuverlässigkeit für den Energiesektor realisieren zu können. Letztlich können nur so – zumindest an dieser Stelle – Wohlstand, Wachstum und Frieden in Europa gesichert werden.

KONTAKT
Raphael Ernst
Telefon +49 228 50212-562
raphael.ernst@fkie.fraunhofer.de

CBRNE-SCHUTZ

EINSATZUNTERSTÜTZUNG DURCH ROBOTIK

EnRicH – Roboter üben für den nuklearen Ernstfall

Unfall im Atomkraftwerk. Es hat eine Explosion nahe dem Reaktor gegeben. Wie sieht es in dem Gebäude jetzt aus? Droht Einsturzgefahr? Ist Strahlung ausgetreten? Menschen scheiden zur Aufklärung dieser zeitkritischen Fragen aus. Sie in die unbekannte Lage zu schicken, wäre viel zu gefährlich. Es sind Szenarien wie dieses, in denen alles an ihnen hängt: Robotern! Doch sind sie bereits soweit? Beim »European Robotics Hackathon (EnRicH)« haben Forschung, Universitäten, Industrie und Anwender die Gelegenheit, das zu testen.

Die Atomkatastrophe von Tschernobyl im April 1986, die aktuell dank einer TV-Serie bilderstark zurück ins öffentliche Gedächtnis gelangt, und der GAU in Fukushima 25 Jahre später, im März 2011, haben eines deutlich gemacht: Absolute Sicherheit gibt es bei Atomkraft nicht. Denn trotz jahrzehntelanger Erfahrung und stetig fortentwickelter Technologien kann es in jedem Atomkraftwerk (AKW) jederzeit zu einem Unfall kommen. Mit verheerenden möglichen Folgen für Menschen und Umwelt. Neben teils veralteten Anlagen, Naturkatastrophen und dem unberechenbaren »Faktor Mensch« hat sich die Lage durch das zunehmende Bedrohungsszenario terroristischer Angriffe noch verschärft. Dabei ist die Liste von Störfällen in kerntechnischen Anlagen Europas bereits heute lang – fast 40 seit dem Jahr 2000.

Doch nicht nur der Super-GAU, sondern bereits die geordnete Stilllegung alter kerntechnischer Anlagen oder der Abbau von Zwischenlagern rufen Roboter zur Unterstützung auf den Plan. »Die Einsatzszenarien für robotische Systeme im Bereich CBRNE sind sehr real, trotzdem wird bislang erstaunlich wenig konkret in diese Richtung geforscht«, erläutert Dr. Frank Schneider, stellvertretender Leiter der Abteilung »Kognitive Mobile Systeme« am Fraunhofer FKIE, die Situation. Um die Möglichkeit zu bieten, den aktuellen Stand von Forschung und Technik in realen Einsatzszenarien auf die Probe zu stellen, hat er im Jahr 2017 gemeinsam mit dem Amt für Rüstung und Wehrtechnik (ARWT) des österreichischen Heeres den »European Robotics Hackathon (EnRicH)« initiiert.

Reale Katastrophenszenarien

Der Wettbewerb findet seitdem alle zwei Jahre in dem nahe Wien gelegenen Kernkraftwerk Zwentendorf statt. Das AKW entspricht demselben Reaktortyp wie der Katastrophenmeiler in Fukushima. Seine Einschaltung wurde jedoch 1978, kurz nach seiner Fertigstellung, durch eine Volksbefragung gestoppt. Das niemals in Betrieb gegangene Kernkraftwerk bietet damit den idealen Austragungsort für die realitätsnahen Aufgaben, die unter anderem auf realen Einsatzszenarien vergangener Atomunfälle beruhen. »EnRicH ist zudem der einzige Wettbewerb in Europa, bei dem mit echter Strahlung geübt wird«, hebt ARWT-Leiter General Michael Janisch eine weitere, durch sein Amt ermöglichte Besonderheit des Hackathons hervor. »Hier zeigt sich, was die europäische Robotik im Fall der Fälle leisten kann.«

Und tatsächlich waren die zehn internationalen Teams und ihre Roboter, die sich bei der zweiten EnRicH-Ausgabe vom 1. bis 5. Juli 2019 messen konnten, stark gefordert. Gefragt waren Aufgaben in den Bereichen »Exploration«, Erkundung und Kartierung der Infrastruktur sowie der Messung und Kartierung ausgetretener Strahlung, »Manipulation«, das Szenario verlangte hier das Schließen von Ventilen, sowie »Search & Rescue«, dem Auffinden und Retten von Verletzten.

Herausfordernde Aufgabenstellungen

Der Parcours erstreckte sich rund um den Reaktor im Erdgeschoss des AKW bis in diesen hinein. Bei der ersten EnRicH-Ausgabe hatte sich das Szenario noch auf einer Reaktorebene in 40 Metern Höhe abgespielt, sodass die bis zu über eine Tonne wiegenden Roboter zunächst einmal mit einem Kran nach oben befördert werden mussten. Doch auch diesmal rang die Beschaffenheit eines AKW Teams und Robotern durch fehlendes Licht, enge Gänge, steile Treppen und massive, jede Funkverbindung erschwerende Betonwände einiges an Können ab.

Die Teilnehmer nahmen es sportlich. Nach ersten Testdurchläufen noch ohne radioaktive Strahlenquellen wurde in der »Pit Lane«, der Boxengasse, in der Teams und Roboter untergebracht waren, fieberhaft diskutiert, programmiert und geschraubt, um Software und Technik für den richtigen Wettbewerb optimal zu vorzubereiten. »Genau darum geht es bei einem Hackathon«, so Schneider, »vorrangig ist der Austausch unter den Teams, der Vergleich der Lösungen und das gemeinsame Lernen.« Für die anspruchsvollen Aufgabenstellungen erntete er daher auch viel positives Feedback seitens der Teilnehmer.

Langer Weg bis zu einsatzfähigen Lösungen

»EnRicH 2019 war aus unserer Sicht eine sehr erfolgreiche Veranstaltung mit bereits deutlich besseren Leistungen als noch bei der ersten Ausgabe 2017«, zieht Schneider positiv Bilanz. »Allerdings ist es bis hin zu Lösungen, die im Ernstfall wirklich zuverlässig und vielfältig Unterstützung bieten können, noch ein sehr weiter Weg.« So machen allein die Fortbewegung auf nicht ebener Fläche oder schwierige Kommunikationsbedingungen, mit denen im Katastrophenfall sicher zu rechnen ist, den meisten Robotern noch extrem zu schaffen. Wie die Erfahrungen der Teams umgesetzt werden, wird sich bei der dritten EnRicH-Ausgabe im Jahr 2021 zeigen. Schneider: »Auch anforderungstechnisch werden wir dann natürlich neue Maßstäbe setzen. Wir freuen uns auf einen weiteren spannenden Hackathon.«

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

SICHERHEIT FÜR EINSATZKRÄFTE

SCHIFFSBRANDBEKÄMPFUNG

Live-Informationen aus brennenden Schiffen

Schmale Gänge, enge Luken, sich schnell erhitzende Stahlwände – ein Brand an Bord eines Schiffes ist für die Feuerwehr eine besondere Herausforderung und birgt viele Risiken. So müssen sich die Einsatzkräfte bei einem Feuer im Maschinenraum mitsamt ihrer Ausrüstung und schwerem Schlauch in der Hand durch mehrere Decks, Rauch und Hitze bis ins tiefste Innere des Schiffes vorkämpfen. Eine schwierige Situation auch für die Führungskräfte: Denn sind die Kollegen erst einmal im Bauch des Schiffes verschwunden, kann es auch zu einem Ausfall des Funkkontakts kommen.

»Brennt ein Schiff in einem Hafen, ist dies noch einmal ein ganz spezieller Fall, denn die Zuständigkeit obliegt hier der landseitigen Feuerwehr«, erklärt FKIE-Wissenschaftler Dr. Daniel Feiser. Die Einsatzkräfte sind keine Nautiker und besitzen nur eine eingeschränkte Ausbildung für solche Einsätze. Unzählige Schiffstypen und ihr unterschiedlicher Aufbau sowie die Besonderheiten des Einsatzes auf dem Wasser stellen für sie seltene und daher schwierige Einsatzbedingungen dar. Ziel des durch das Bundesministerium für Bildung und Forschung (BMBF) mit 2,3 Millionen Euro geförderten Projekts EFAS, kurz für »Einsatzunterstützungssystem für Feuerwehren zur Gefahrenbekämpfung an Bord von Seeschiffen«, war vor diesem Hintergrund die Entwicklung eines Konzepts, das die Kommunikation und Übermittlung wichtiger Lagedaten bei Schiffseinsätzen sicherstellt. Denn je besser die Informations- und Datenlage, desto mehr Sicherheit für die Einsatzkräfte.

»Zum Projektstart wurden drei Fragestellungen als vorrangig identifiziert«, so EFAS-Verbundkoordinator Feiser. »Frage 1: Wie schaffen wir es, die Feuerwehrleute an Bord durchgängig zu orten? Frage 2: Wie stellen wir verlässlich fest, ob Gefahrstoffe ausgetreten sind und wie hoch die Temperatur in der Umgebung der Einsatzkraft ist, ohne dass die Trupps hierfür ein zusätzliches Messgerät mit sich führen müssen? Frage 3: Wie kann eine stabile Kommunikation zwischen den Einsatzkräften an Bord und an Land sichergestellt werden?«

Drei Jahre arbeiteten die Projektpartner, zu denen neben dem Fraunhofer FKIE auch das Institut für Sicherheitstechnik/Schiffsicherheit, das Institut für Textil- und Verfahrenstechnik, der Software-Hersteller MARSIG, der Sicherheitstechnik-Anbieter ATS Elektronik und der Feuerwehr-Schutzkleidungshersteller S-GARD zählten, an der Lösung. Von Anwenderseite war zur Bewertung der erarbeiteten Ansätze die Feuerwehr Wilhelmshaven eng in das Projekt eingebunden. Die Ergebnisse wurden im Rahmen einer großen Abschluss-Evaluation auf dem Traditionsschiff »Dresden« geprüft. Standortbedingt stellte sich hier die Berufsfeuerwehr Rostock für den Test in einem realen Einsatzszenario zur Verfügung. Ihr abschließendes Fazit: Begeistert!

Per Tablet immer mit Live-Daten versorgt

»Eine der wichtigsten Neuerungen von EFAS ist, dass Einsatz- und Abschnittsleiter Tablets mit einem Lagedarstellungssystem nutzen«, erklärt Feiser – und damit den Arbeitsanteil des Fraunhofer FKIE. In dieses System werden zu Einsatzbeginn die verpflichtend außen an Bord hinterlegten Schiffspläne eingespielt, als Grundlage für die per Software bereitgestellte digitale Lagedarstellung. Ebenfalls hier eingespeist werden ab diesem Zeitpunkt alle Informationen, die der Angriffstrupp auf seinem Weg zum Brand sammelt. Sowohl der Einsatzleiter, der sich mit dem Kapitän auf der Schiffsbrücke befindet, als auch der Abschnittsleiter, der sich in einem sicheren, d. h. gefahrstoff-, rauch- und feuerfreien, Bereich an Bord positioniert, sind so immer auf demselben Echtzeit-Informationsstand.

Sensoren in Schutzkleidung sammeln automatisiert Daten

Die Lagedaten werden durch Sensoren in der Schutzkleidung der Einsatzkräfte gesammelt und an das System übertragen. Feiser: »Die Kommunikation wurde durch die Firma ATS über eine LTE-Mobilfunkzelle realisiert.« Zur Ortung der Einsatzkräfte unter Deck wurden Beschleunigungs- und gyroskopische Sensoren in die Schuhe integriert, da GPS im Schiffsinneren nicht verfügbar ist. Ausgehend von einem Startpunkt kann das System die jeweils aktuelle Position der Einsatzkräfte berechnen und auf dem digitalen Schiffsplan markieren. Ergebnis im Live-Test: Mit einem kleinen Versatz von ein bis zwei Metern funktioniert auch dies sehr genau, was die Feuerwehr als großen Projekterfolg wertete.

Weitere Sensoren wurden zur Messung von Temperatur und Gefahrstoffen in die Kleidung der Einsatzkräfte eingebracht. Feiser: »Schutzkleidung ist heute oft so gut, dass Einsatzkräfte die Hitze gar nicht mehr spüren, sondern erst merken, dass sie sich in viel zu heißen Bereichen befinden, wenn ihre Kleidung zu schmelzen beginnt, was sehr gefährlich ist. Man könnte also sagen, die heutige Schutzkleidung ist ›zu gut‹.« Mithilfe der Sensoren und der neuen Lagedarstellungssoftware werden Einsatz- und Abschnittsleiter jetzt umgehend informiert, sollten sich die Trupps kritischen Bereichen nähern. Per Knopfdruck können sie ihre Leute dann zurückrufen. In diesem Fall leuchten an den Ärmeln der Schutzkleidung LED-Leuchten auf: der Befehl zum sofortigen Rückzug.

»Von Ablauf, Organisation und Ergebnissen her war die Evaluation ein großer Erfolg«, zieht Feiser Bilanz. »Einsatz- und Abschnittsleiter konnten die neue Lagedarstellungssoftware nach kurzer Einweisung nutzen und bewerteten sie als intuitiv, effizient und ansprechend. Das größte Lob für unsere Arbeit.«

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

PROJEKT-HIGHLIGHTS

INFORMATIONSGEWINNUNG, ENTSCHEIDUNG UND FÜHRUNG

Die Bewältigung militärischer Einsätze oder kritischer Situationen im zivilen Umfeld hängt entscheidend von echtzeitnahem Lagebewusstsein und effektiver Zusammenarbeit ab. Das Fraunhofer FKIE verfügt über alle erforderlichen Kompetenzen wie Sensordatenfusion, Kommunikation, Massendatenverarbeitung oder nutzerzentrierter Informationsdarstellung.

SENSORBASIERTE ZUTRITTSÜBERWACHUNG

Manipulation teurer Agrarforschung erkennen

Bis zum Jahr 2050 werden mehr als neun Milliarden Menschen auf der Erde leben. Ihre Ernährung stellt eine der größten globalen Herausforderungen dar. »Crop Science« bzw. die Forschung im Bereich Kulturpflanzen ist daher die Grundlage eines der wichtigsten Geschäftsfelder der Bayer AG. Sie ist der weltweit drittgrößte Anbieter für Pflanzenschutz (Crop Protection) und Saatgut (Seeds) in der Landwirtschaft. Im Projekt »SensFArM« entwickelt das Fraunhofer FKIE ein System zur Überwachung der Testfelder, auf denen der Konzern seine aufwendige und kostenintensive Forschung betreibt.

Auf weltweit angesiedelten Breeding und Crop Protection Fields züchtet, beobachtet und erforscht Bayer neu entwickelte resistente Getreidesorten und Pflanzenschutzmittel. »Oft handelt es sich hierbei um gepachtete, frei zugängliche Plantagen und Felder«, erläutert FKIE-Wissenschaftlerin und »SensFArM«-Projektleiterin Linda Nelles-Ziegler. »Immer besteht daher das Risiko, dass sich Unbefugte, zum Beispiel Umweltaktivisten oder Wettbewerber, Zutritt verschaffen, um Versuche zu manipulieren – wie durch das Einstreuen von Fremdsaatgut.« Da die Forschungsprojekte meistens über viele Jahre laufen und die Manipulationen nicht immer direkt entdeckt werden, bedeuten solche Vorfälle große Rückschritte und finanziellen Schaden für den Konzern. Bayer hat daher ein starkes Interesse daran, frühzeitig über unberechtigte Aktivitäten auf seinen Hochrisikofeldern informiert zu werden.

Neben der konzerneigenen Corporate Security hat Bayer mit Securitas einen namhaften Sicherheitsdienstleister an seiner Seite. Securitas ist bereits mit der Überwachung diverser Liegenschaften des Bayer-Konzerns betraut und leistet diese von sogenannten »Security Operation Centers« (SOC) aus. Eine 24/7-Kontrolle der geografisch weit verstreuten, vielfach abseits gelegenen und zudem ständig wechselnden Testfeld-Standorte kann jedoch bisher nicht gewährleistet werden.

Im Projekt »SensFArM«, kurz für »Sensor-Based Flexible Area Monitoring«, entwickelt das Fraunhofer FKIE aus diesem Grund seit Oktober 2018 eine verlegefähige technische Lösung zur sensorbasierten Liegenschaftsüberwachung. Sie soll die Detektion und Nachvollziehbarkeit unerwünschter Bewegungen innerhalb der fest definierten Bereiche der Bayer-Testfelder gewährleisten. Die Umsetzung innerhalb des 12-monatigen Projekts erfolgt dabei bis zur Ausbaustufe eines Funktionsdemonstrators. Ziel ist es, Bayer die Information bereitzustellen, ob, wann, wie und wo Unbefugte die Testfelder des Konzerns betreten haben.

Zutrittsdetektion durch optische und seismische Sensoren

Der technische Lösungsansatz, an dem insgesamt vier FKIE-Abteilungen mitgewirkt haben, basiert auf zwei Sensortechnologien zur Bewegungsdetektion: optischen (Tageslicht/Infrarot) und seismischen Sensoren. Die von ihnen übermittelten Daten werden via LTE von den Feldern zu den Servern übermittelt. Hier werden die generierten Alarme in einer übersichtlichen, visuell und kartografisch aufbereiteten Lagedarstellung angezeigt. Die als auffällig gemeldeten Testfelder können so gezielt angefahren und überprüft werden.

»Bei der Konzeption der Lösung galt es besondere projektspezifische Anforderungen zu berücksichtigen«, erklärt Nelles-Ziegler die Herausforderungen des Projekts. »So sind die Felder abgelegen und ohne Energieversorgung, was wir durch den Einsatz von spezieller Sensorik und Generatoren gelöst haben. Die eingesetzte Technik muss weiterhin sehr robust sein, da sie jeder Witterung ausgesetzt ist. Gleichzeitig muss sie möglichst unauffällig platziert werden. Bedingt durch die bei landwirtschaftlich bewirtschafteten Böden übliche wechselnde Fruchtfolge ändern sich die Standorte der Testfelder zudem im Jahresrhythmus, sodass das gesamte System verlegefähig sein muss.«

Erfolgreicher Systemtest

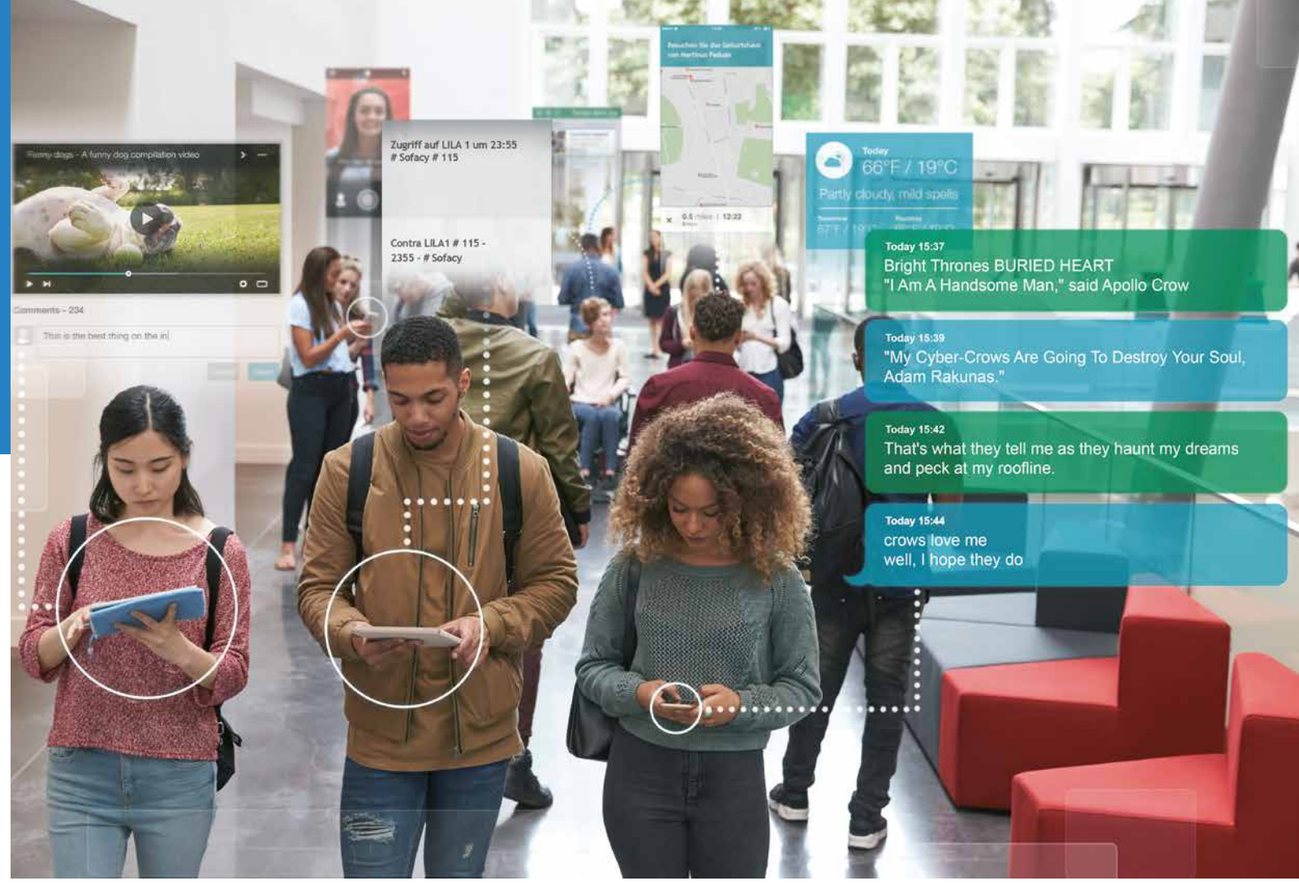
Auf dem Burscheider Versuchshof »Gut Höfchen« hat die Bayer AG ein Testfeld für die Durchführung von zwei Testkampagnen und die Abschlussdemonstration im Oktober 2019 zur Verfügung gestellt. Bereits bei der ersten Testreihe konnten der allgemeine Systemaufbau und die Datenübertragung von der Kamera-Sensorik zu den Clients, insbesondere die Übertragung eines Live-Streams, erfolgreich belegt werden. Auch die GPS-Eigenpositionsmeldung von Smartphones wurde bei dieser Gelegenheit untersucht. Sie soll später zur Unterscheidung von berechtigten und unberechtigten Zutritten auf die Felder eingesetzt werden. Ziel einer zweiten Testkampagne ist es, die per Datenfusion erstellten Tracks von der Sensorik über den Server bis in die Lagedarstellung zu übertragen. Ein Track beinhaltet dabei sowohl den Pfad (die Koordinaten) eines detektierten Objekts als auch seine Klassifikation (Mensch, Fahrzeug etc.).

Weitere Verwertung und Perspektiven des Projekts

Eine technische Überwachungslösung, die die spezifischen Anforderungen der Bayer-Hochrisikofelder erfüllt, ist bislang nicht am Markt verfügbar. Der im Rahmen des Projekts »SensFArM« entwickelte Demonstrator kann daher Ausgangspunkt für eine zur Produktreife gelangten, industrieseitig angebotenen und breit ausrollbaren technischen Lösung sein, die von Securitas als beauftragtem Sicherheitsdienstleister der Bayer AG betrieben wird. Der bei der Entwicklung des Demonstrators verfolgte generische Implementierungsansatz begünstigt dabei weitere anwendungsorientierte Ausbaustufen.

KONTAKT
Linda Nelles-Ziegler
Telefon +49 228 9435-114
linda.nelles-ziegler@fkie.fraunhofer.de

FAKE NEWS-KLASSIFIZIERUNG



Frühwarnsystem reduziert den Datenberg

Die öffentliche Meinungsbildung läuft heute zunehmend über die Sozialen Medien ab. Die Bedeutung von Twitter, Facebook und Co. als Medien politischer Kommunikation nimmt immer mehr zu und Fake News – erfundene Nachrichten oder verdrehte Fakten – verbreiten sich rasant im Netz und werden oft unbedacht oder gerade ganz gezielt geteilt. Prof. Dr. Ulrich Schade, Forschungsgruppenleiter am Fraunhofer FKIE, hat mit seinem Team ein Tool entwickelt, das als Frühwarnsystem zur automatisierten Erkennung von Fake News eingesetzt werden kann. Das System wertet Social Media-Daten aus und weist auf diejenigen hin, die Merkmale von Fake News tragen.

Fake News werden zur Stimmungsmache oder Hetze gegen einzelne oder mehrere Personen genutzt. Sie sollen die öffentliche Meinung zu bestimmten aktuellen Themen beeinflussen und manipulieren. Solche Falschmeldungen zu identifizieren, ist selbst für erfahrene Journalisten und Fakten-Checker schwierig. An dieser Stelle setzt das Klassifikationstool von Professor Schade an. Es scannt automatisiert Social Media-Nachrichten, filtert diejenigen heraus, die ganz spezifische Merkmale aufweisen und bereitet die Ergebnisse grafisch ergonomisch optimiert auf. Dabei führt das System keinen automatisierten Wahrheitscheck oder gar eine Zensur durch. Die letztendliche Bewertung der als potenzielle Fake News markierten Nachrichten liegt bei den Nutzern des Klassifizierungstools.

Auswertung und Beobachtung der Nachrichtenlage

Ziel ist es, auffällige Nachrichten frühzeitig zu erkennen und die Aufmerksamkeit auf sie zu lenken, sodass ihre Weiterverbreitung bei Bedarf beobachtet werden kann. Es handelt sich somit um ein Vorselektions- und Alert-System, das Nutzer bei der Auswertung und Beobachtung der Nachrichtenlage unterstützt. »Wir helfen bei der Suche nach der Nadel im Heuhaufen, indem wir den riesigen Daten-Heuberg maximal reduzieren«, beschreibt Schade die Vorteile seines Tools. Dabei fokussieren sich die Wissenschaftler aus der Abteilung »Informationstechnik für Führungssysteme« auf Twitter und Webseiten, also öffentlich zugängliche Datenquellen. »In den Tweets werden oftmals die Links veröffentlicht, unter denen die eigentlichen Fake News zu finden sind. Die sozialen Medien liefern sozusagen den Trigger. Manche Webseiten, auf die so verwiesen wird, sind denen von Nachrichtenagenturen nachempfunden und nur schwer von den Originalen zu unterscheiden. Oftmals liegen ihnen dpa-Meldungen zugrunde, die sprachlich einfach verändert oder um problematische Passagen ergänzt wurden«, erläutert Professor Schade.

Lernsets trainieren das System

Mithilfe zweier Korpora lernt das Tool, Nachrichten zu klassifizieren: Im ersten Schritt werden Bibliotheken aufgebaut, eine mit seriösen Beispielbeiträgen und eine mit solchen, die der Nutzer als Fake News ansieht. Mithilfe dieser Lernsets wird das System trainiert. Dabei wenden die Forscherinnen und Forscher »Machine Learning«-Verfahren an, sowohl klassische Verfahren als auch solche mit »Deep Learning«. Letztere erlernen die Erkennungszeichen (genannt »Merkmale«), nach denen sie zwischen seriösen Beiträgen und den Fake News unterscheiden aus dem Lernset. Das ist mit hohem Rechenaufwand verbunden. Für die klassischen Verfahren werden Merkmale vorgegeben, aus denen die relevanten Kombinationen mit weniger Aufwand erlernt werden.

Hinweise auf Bots

Als mögliche Erkennungszeichen werden sowohl sprachliche Daten, etwa die Wortwahl oder der Satzbau, aber auch Metadaten in die Analyse einbezogen. Diese spielen eine wichtige Rolle, wenn es darum geht, richtige von falschen Meldungen zu unterscheiden: Wie häufig wird gepostet, wann wird ein Tweet abgesetzt und um welche Uhrzeit. Aufschlussreich ist auch der Zeitpunkt eines Posts. Er kann darauf hinweisen, aus welchem Land bzw. aus welcher Zeitzone der Sender Meldungen absetzt. Eine hohe Sendefrequenz deutet auf Bots hin, was die Wahrscheinlichkeit einer Fake News erhöht. Auch die Vernetzung der Accounts und deren Follower-Strukturen können für die Analyse von großer Bedeutung sein. Prinzipiell müssen stets mehrere Merkmale zusammen auf Fake News hinweisen, um eine entsprechende Klassifikation auszulösen.

Insbesondere durch die grafische Darstellung dieser Einsortierung bietet das System den Nutzern ein hilfreiches Instrument zur Früherkennung von Fake News. Sowohl Behörden als auch Unternehmen nutzen das Tool bereits, um gezielt Desinformation aufzudecken und umfassend zu bekämpfen. »Unsere Software lässt sich für jeden Kunden individuell anpassen. Die Bedienung ist leicht, sodass Kunden auch ihre eigenen Beispielbibliotheken anlegen und die Klassifikation mit diesen trainieren können«, sagt Schade.

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

LOKALISIERUNG VON MENSCHEN

Lebensrettung, die Wände überwindet

Erdbeben, Lawinen, Feuer – wenn der Auftrag lautet: »Schnell alle Überlebenden finden und befreien!«, sind Rettungskräfte im Kampf gegen die Zeit oft mit vielfältigen Hindernissen konfrontiert, z. B. verschütteten, nicht begeh- oder einsehbaren Räumen. Abhilfe schaffen kann hier einmal mehr die Technik – der Einsatz von UWB-Sensoren, um genau zu sein. Denn mithilfe eines Systemverbunds dieser Ultrabreitband-Radartechnologie können, wie FKIE-Wissenschaftlerin Snezhana Jovanoska erforscht hat, Personen durch Wände, Schutt, Rauch oder Schnee hindurch geortet werden.

Für ihre Dissertation, die sie sowohl an der TU Ilmenau als auch am Fraunhofer FKIE geschrieben hat, untersuchte die Wissenschaftlerin den Einsatz von Radar-Sensoren für die Lokalisierung und Verfolgung mehrerer Personen. Verwendet wurde hierfür ein Ultrabreitband-Radar (UWB-Radar), weil dieses im Gegensatz zum schmalbandigen Radar gerade im Nahbereich sehr präzise ist. Dabei ging es ihr nicht darum, einen einzelnen Sensor zu verbessern, sondern darum, die Fähigkeiten eines Sensorverbundes zu erforschen und so zu optimieren, dass sie die Positionen von mehreren Personen möglichst genau bestimmen können.

Fusion Engine für sinnvoll interpretierbare Informationen

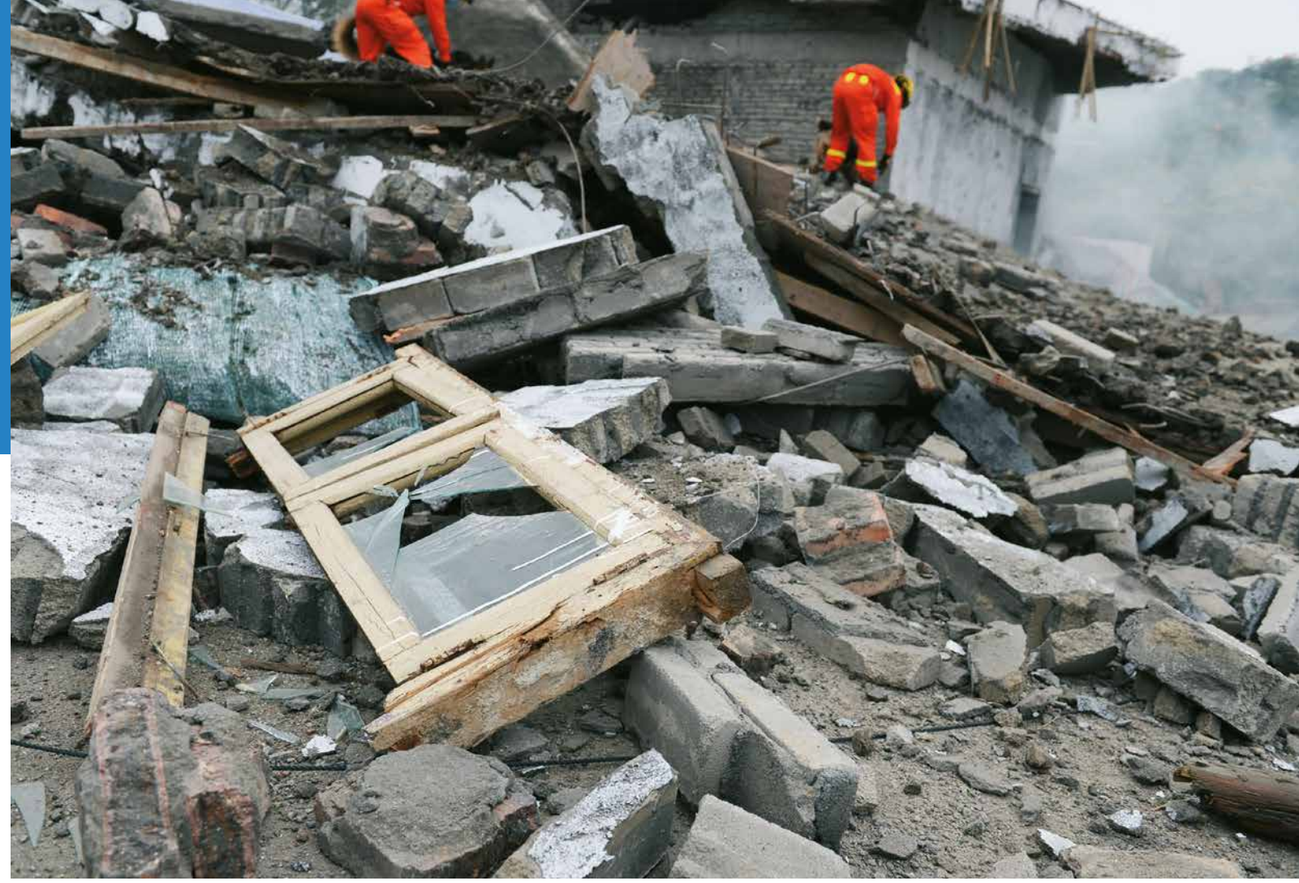
Hierzu kam eine Fusion Engine zum Einsatz, ein Schwerpunkt der Abteilung »Sensordaten- und Informationsfusion« (SDF), in der Jovanoska arbeitet. Dabei handelt es sich um sehr spezifisch nach dem jeweiligen Anwendungszweck ausgerichtete Algorithmen, welche die durch die Sensoren gesammelten Daten fusionieren und zu Informationen zusammenführen. Dann erst sind die Daten auch durch den Menschen interpretierbar. Als universales Werkzeug kann Fusion unterschiedlichste Aufgaben erfüllen und ist damit für vielfältige Zwecke einsetzbar: So kann man etwa Objekte detektieren, tracken oder klassifizieren sowie Ressourcen gemäß Bedarf und Abhängigkeiten zuteilen, die komplexer sind, als ein Mensch sie verarbeiten kann. Damit bildet die Fusion von Sensordaten die Basis einer Vielzahl von Technologien, die gemeinhin unter dem Begriff der Künstlichen Intelligenz zusammengefasst werden.

Unterstützung der Einsatzkräfte bei Rettungsaktionen

Was sehr theoretisch klingt, verfolgt ein ganz praktisches Ziel: Einsatzkräften – sei es bei einer Naturkatastrophe wie einem Erdbeben, einem Industrieunfall, etwa einem Feuer in einer Werkshalle mit hoher Rauchentwicklung, oder auch bei einer Geiselnahme – aufzuzeigen, wie viele Personen sich in Räumen aufhalten und wo diese sich befinden. Und das ganz ohne die Notwendigkeit, diese Räume betreten zu müssen und ebenso ohne die Kooperation der Person. Schließlich sind Verschüttete, Verletzte oder Geiseln in den seltensten Fällen in der Lage, irgendwie auf sich aufmerksam zu machen. Rettungsaktionen können so deutlich zielgerichteter durchgeführt werden. In vielen Messungen konnte bereits gezeigt werden, dass die gelieferten Ergebnisse sehr präzise sind. Trotz unterschiedlicher Signaldurchlässigkeit der Wand- oder auch Bodenmaterialien: Die Ortungsergebnisse bleiben gut und sind brauchbar. Dies ist möglich, weil die unterschiedlichen Materialeigenschaften durch eine Anpassung der Fusionsalgorithmen ausgeglichen werden.

Auch den Datenschutz im Blick

»Im nächsten Schritt haben wir uns dann die Frage angeschaut, wie wir die Sensoren reduzieren können und dennoch gleichbleibend gute Ergebnisse erhalten«, so Jovanoska. »Wie können die fehlenden Informationen durch die Algorithmen ausgeglichen werden?« Die Idee der FKIE-Wissenschaftlerin: Kontextwissen wie die zeitliche Dimension und geometrische Informationen hinzuzunehmen. Wenn ein einzelner Sensor über eine gewisse Zeit zwei Personen detektiert und dann mit einem Mal nur noch eine Person, muss der Algorithmus der Fusion Engine schlussfolgern, dass sich die zweite Person nun hinter der ersten befindet und daher verdeckt wird. »So kann der Algorithmus immer weiter angepasst werden und ist auf viele Szenarien anwendbar«, fasst Jovanoska zusammen. Was Radartechnologie außerdem vor dem Hintergrund des Datenschutzes aktuell so relevant macht: »Die Sensorensammeln keine personenbezogenen Daten, wie etwa Kameras, die durch Gesichtserkennung Personen identifizieren können. Das ist ein großer Vorteil!«

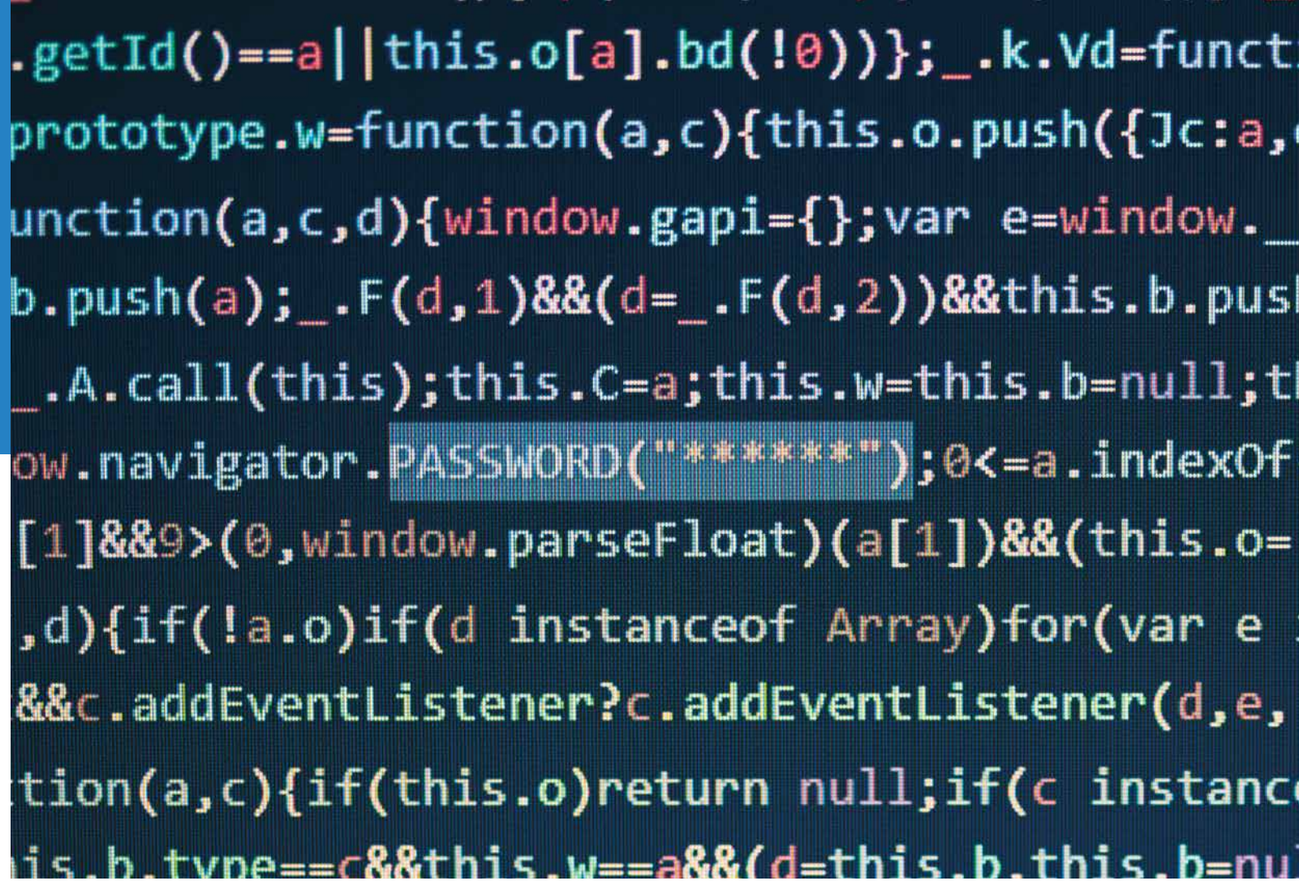


KONTAKT
Snezhana Jovanoska
Telefon +49 228 9435-305
snezhana.jovanoska@fkie.fraunhofer.de

CYBER- UND INFORMATIONSRAUM

Digitalisierung und Vernetzung durchdringen nahezu alle Lebens- und Arbeitsbereiche. Das bietet Chancen und Potenziale, aber erzeugt auch neue Risiken und Angriffsvektoren. Das Fraunhofer FKIE widmet sich dieser Thematik mit höchster fachlicher Kompetenz in den Bereichen Prävention, Detektion, Repression, Reaktion und Usability.

USABLE SECURITY



Mehr Sicherheit für User-Daten

Kennen Sie die Seite Sportsnapshare.com? Nein? Gut so! Denn bei dieser Website handelt es sich um einen Fake. Der Hintergrund aber ist weder Meinungsmache noch kriminelle Täuschung wie etwa Betrug. Ein Wissenschaftler-Team von der Uni Bonn und dem Fraunhofer FKIE hat sie zu Studienzwecken erstellt. Was sie damit herausfinden wollen? Unter welchen Umständen Entwickler Webservices so programmieren, dass die User-Passwörter sicher abgelegt werden – oder kurz: Es geht um entwicklerfreundliche Sicherheit.

Das Problem ist nicht unbekannt: Immer wieder geraten Passwörter im Klartext an Unbefugte oder gar an die Öffentlichkeit. Und dabei sind es nicht nur die kleinen Software-Firmen, die wenig Geld für die Entwicklung sicherer Systeme haben oder gar für ganze Teams von Sicherheitsexperten. Sondern dieses Problem betrifft auch die Tech-Giganten wie Google, Facebook und Yahoo.

Daten-Lecks durch Unachtsamkeit

Es gibt viele mögliche Gründe, warum Passwörter nicht sicher gespeichert werden. Es wird bei der Entwicklung der Benutzer-Registrierung zu wenig auf den Sicherheitsaspekt geachtet. Oder aber die Passwörter werden zwar sicher in der Passwort-Datenbank hinterlegt, sind jedoch aus Unachtsamkeit in den sogenannten Logs im Klartext vorhanden. Logs sind die Protokolle, die das Softwaresystem darüber erstellt, was in ihm geschieht. Wenn sich also ein Nutzer anmeldet, wird dies in diesen Log-Files protokolliert. Eine weitere Möglichkeit ist, dass zwar ein Mechanismus für die sichere Speicherung gebaut wurde, aber nicht regelmäßig aktualisiert wird. Da immer neue Angriffe gegen Hash-Algorithmen möglich werden, müssen diese regelmäßig angepasst werden. Wie also kann diese Sicherheitslücke, die durch menschliches Fehlverhalten verursacht wird, geschlossen werden?

Genau dieser Frage ist das Team um Matthew Smith, Abteilungsleiter »Usable Security and Privacy« am Fraunhofer FKIE und Professor an der Uni Bonn, in einer Studie nachgegangen. Für diese Studie haben die Promovenden Eva Gerlitz (Fraunhofer FKIE), Alena Naiakshina (Uni Bonn) und Anastasia Danilova (Uni Bonn) ein Konzept erarbeitet und Probanden rekrutiert.

Explizite Aufgabenstellung für Sicherheit notwendig

Gesucht wurden Entwickler, die die Aufgabe erhielten, eine Benutzerregistrierungssoftware zu erstellen. Natürlich ohne zu wissen, dass es sich »nur« um eine Studie handelt, damit das Ergebnis nicht verfälscht wird. Und hier kommt Sportsnapshare.com ins Spiel. Denn diese Seite war sozusagen der Köder: der Auftraggeber und die real existierende Seite, für die die Login-Schnittstelle programmiert werden sollte.

Die Gruppe aus 42 Probanden wurde dazu in zwei Gruppen eingeteilt. Die erste Gruppe erhielt einfach nur die Aufgabe, die Registrierung zu entwickeln, während die zweite explizit die Zusatzaufgabe erhielt, dabei die Passwörter der Nutzer sicher zu speichern. Dafür wurden jeweils einer Hälfte beider Gruppen 100 Euro Entlohnung geboten und der jeweils anderen Hälfte mit 200 Euro das Doppelte versprochen. Programmiert wurde in Java.

Nur vier der 21 Probanden aus Gruppe eins legten die Passwörter so ab, dass sie einigermaßen sicher waren. In Gruppe zwei waren es mit 13 von 21 Probanden schon deutlich mehr, wenn auch noch erstaunlich wenige. Die Höhe der Bezahlung wirkte sich in diesem Durchlauf statistisch nicht signifikant aus. Das Fazit: Als Auftraggeber muss man sehr genau spezifizieren, welches Sicherheitsniveau man haben möchte, nur dann wird es auch berücksichtigt.

Mehr Wissenstransfer durch universitäre Lehre und Fachschulungen

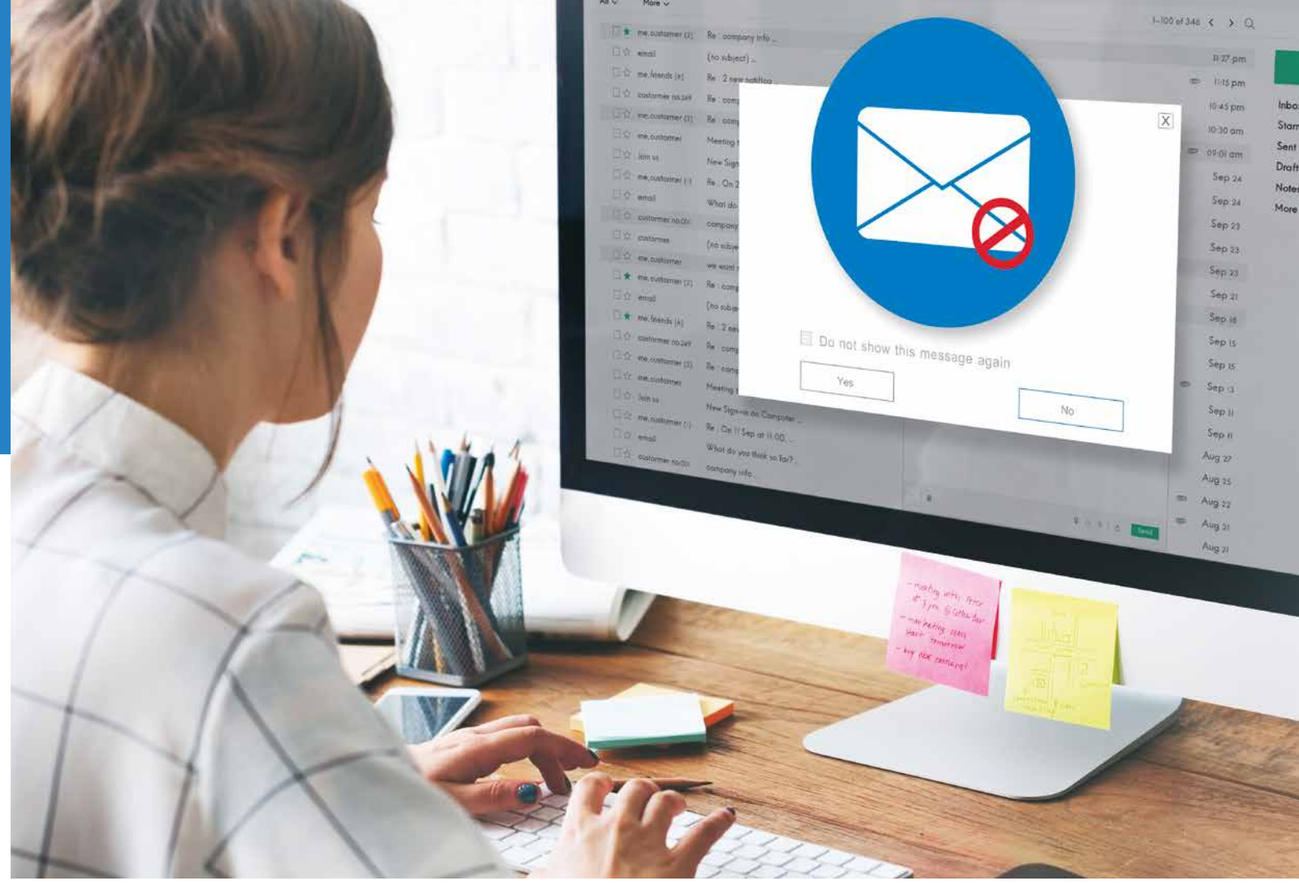
Auch bestätigt das Ergebnis, was sich in einer Vorstudie mit Studierenden der Uni Bonn bereits angedeutet hatte: Programmierer bedienen sich ausgiebig im Web und »programmieren« mittels »copy and paste«. Dabei waren sowohl die Lösungen in der Vor- wie auch der Hauptstudie von sehr unterschiedlichem Sicherheitsniveau. Diese Erkenntnisse können darauf hindeuten, dass an dieser Stelle eine Wissenslücke besteht. Dieser kann etwa durch spezifische Studiengänge, wie dem gerade gestarteten Studiengang Cyber Security an der Uni Bonn, oder aber durch Schulungsmaßnahmen, wie sie durch das Lernlabor Cybersicherheit für kleine und große Unternehmen angeboten werden, beigekommen werden.

Übrigens: Zum Abschluss der Studie wurde natürlich alles aufgeklärt. Und es erhielten am Ende auch alle Entwickler, denen nur 100 Euro geboten wurden, 200 Euro. Im nächsten Schritt soll diese Studie nun noch einmal mit festangestellten Entwicklern durchgeführt werden, um eine breitere Datenbasis zu erhalten und die Ergebnisse der ersten Studie zu verifizieren.

KONTAKT
Prof. Dr. Matthew Smith
Telefon +49 228 7354-218
matthew.smith@fkie.fraunhofer.de

CYBER- UND INFORMATIONSRAUM

DER FAKTOR MENSCH IN DER CYBERSICHERHEIT



»Irgendeiner klickt immer!«

IT-Systeme können noch so gut geschützt sein, es gibt immer einen Unsicherheitsfaktor: den Menschen als Bediener und Nutzer dieser Systeme. Und das Perfide an den Angriffen ist zudem: Sie tarnen sich hervorragend – entweder geben sie sich den Anschein einer vertrauenswürdigen Quelle oder aber sie nutzen das Gewohnte, etwa einen bei dem jeweiligen Arbeitgeber üblichen Inhalt.

Diesen Faktor Mensch hat nun ein Forscher-Team von Uni Bonn und Fraunhofer FKIE untersucht. Dank neuer Messmethoden konnten sie Erstaunliches beobachten: Zwar zeigen sich durch Schulungen positive Effekte auf den Aspekt der Prävention, doch die Detektionsrate kann nach der Schulung sinken. Es können also mehr Angriffe durch die höhere Awareness der Nutzer abgewehrt werden, diese Angriffe werden jedoch deutlich seltener gemeldet.

Kosteneffiziente und genaue Messung von IT-Sicherheitsbewusstsein

Die Messung wurde in zwei Phasen durchgeführt. Dazwischen wurde eine Awareness-Schulung angeboten. Die Probanden wurden dabei in verschiedene Gruppen eingeteilt: solche, die an der Schulung teilnahmen, und solche, die nicht teilnahmen. Im Regelbetrieb der Verwaltung des Universitätsklinikums Schleswig-Holstein, das einer der Projektpartner ist, wurden nun in den Messphasen sogenannte »Artefakte« eingebracht und die Reaktion der Probanden aufgezeichnet. Artefakte stellen in diesem Zusammenhang etwa Phishing-Mails oder andere Arten von Cyberangriffen dar.

Ein Beispiel: Ein Mitarbeiter der Verwaltung, vielleicht aus der Personalabteilung, sitzt an seinem PC-Arbeitsplatz und erledigt Aufgaben, die er mehr oder weniger täglich und routinemäßig durchführt. Nun trifft über sein Mailingsystem eine neue E-Mail mit dem Betreff »Meine Bewerbung« ein. Eigentlich nichts Ungewöhnliches. Der entsprechende Absender aber mutet eher kryptisch an. Es handelt sich um eines der eingespielten Artefakte, das eine Phishing-Mail simuliert.

Interessant ist nun, wie er sich verhält: Ignoriert er die Mail? Öffnet er sie und vielleicht sogar den Anhang? Oder aber identifiziert er die Mail als möglichen Phishing-Versuch und meldet ihn an die entsprechende Stelle? »Genau daran, wie diese Reaktion ausfällt, können wir nun mit wenig Aufwand messen, wie es um das IT-Sicherheitsbewusstsein des Einzelnen bestellt ist«, erzählt Arnold Sykosch, wissenschaftlicher Mitarbeiter im Cyber-Security-Team um Prof. Dr. Michael Meier.

Das Studiendesign für diese Messung wurde im Rahmen eines Konsortialprojekts durch die Uni Bonn erarbeitet und auch die Messung selbst führte das Team um Professor Meier durch. Beteiligt waren zudem das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), das Fachgebiet »Allgemeine Psychologie: Kognition« der Universität Duisburg-Essen, das Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster sowie die Enno Rey Netzwerke GmbH.

Nur Prävention und Detektion gemeinsam bringen Sicherheit

Führt man sich vor Augen, wie allgegenwärtig die Gefahren sind, wird klar, wie fatal es ist, wenn ein Angriff nicht gemeldet wird. FKIE-Wissenschaftler Arnold Sykosch erläutert: »Schon allein ein Webbrowser ist ein so unglaublich kritisches Element, das fast jeder ohne Vorbehalte nutzt. Hier werden zum Teil hochsensible Daten genauso selbstverständlich ausgetauscht, wie auch unbekannte und damit potenziell gefährliche Websites angesurft werden.«

Und, dies zeige die Erfahrung ebenso wie die durchgeführte Studie: Irgendein Nutzer klickt – allen Awareness-Veranstaltungen zum Trotz – doch immer auf die Dateien oder Links, die dann Viren in das System schleusen. Die Meldung eines Angriffs an die Stelle, wo weitere Maßnahmen eingeleitet werden könnten, sei daher von hoher Bedeutung. Hinsichtlich der Gründe für diese Effekte kann Cyber-Security-Spezialist Sykosch bislang nur mutmaßen, da eine Verlängerung des Projektes, in der er genau dies untersuchen möchte, noch aussteht: »Eine denkbare Erklärung für dieses Verhalten könnte sein, dass die geschulten Personen nun das Gefühl hätten, selbst mit dem Angriff fertig werden zu müssen. Ein weiterer Grund kann in dem neuen Bewusstsein liegen, dass ja nur eine Person den Angriff melden muss – und wenn jeder auf den Kollegen setzt, meldet letztendlich keiner den Angriff.«

KONTAKT
Prof. Dr. Michael Meier
Telefon +49 228 7354-249
michael.meier@fkie.fraunhofer.de

ERKENNUNG VON CYBERANGRIFFEN

Schutz vor Datenklau im Unternehmensnetzwerk

Angriffe auf Unternehmensnetzwerke sind längst keine Einzelfälle mehr. Fast täglich berichten Medien über Hackerangriffe, Datenklau, Viren oder Trojaner, die in Unternehmen, Behörden oder Organisationen zum Teil großen, finanziellen Schaden anrichten. Unternehmensnetzwerke sind weltweit in den Fokus gezielter Cyberangriffe gerückt, bei denen wertvolle Daten gestohlen, manipuliert oder gelöscht werden. Oftmals sind es vertrauliche interne Informationen bis hin zu persönlichen Kundendaten, die so in die falschen Hände gelangen. Weiteres Problem: In den meisten Fällen dauert es mehrere Wochen bis Monate, bis ein solcher Cyberangriff überhaupt erst entdeckt wird.

Hier setzt das Team rund um Rafael Uetz aus der Abteilung »Cyber Analysis and Defense« (CA&D) am Fraunhofer FKIE an und erforscht technische Lösungen und neue Methoden zur intelligenten Erkennung und Analyse derartiger Cyberangriffe. Dabei liegt der Fokus auf der zentralen Sammlung und Analyse von Ereignismeldungen aus dem Netzwerk.

Mehrere tausend Meldungen pro Sekunde

Wertvolle Hinweise auf externe Übergriffe finden sich oftmals in den Logdaten der betroffenen Organisationen, wie sie beispielsweise von Betriebs- und Sicherheitssystemen bzw. der Netzwerkhardware erzeugt werden. Eine manuelle Auswertung dieser Daten ist allein aufgrund der Masse – in großen Unternehmen sind das mehrere tausend Ereignismeldungen pro Sekunde – kaum möglich. Übliche Quellen dieser Meldungen sind Logdaten von Betriebssystemen, Firewalls und weiterer Netzwerk- bzw. Sicherheitshardware. Diese enthalten ganz unterschiedliche Informationen und sind aus IT-Security-Sicht gegebenenfalls irrelevant oder enthalten Fehlalarme. Meist lassen sich daher Angriffe auf das Netzwerk nur aus einer Kombination mehrerer Indikatoren erkennen. Hierfür müssen die Daten allerdings in ein gemeinsames Format gebracht werden, damit eine sinnvolle automatische Analyse erfolgen kann. Dies erfordert – je nach Größe des Unternehmens – aber einen erheblichen personellen, technischen wie auch finanziellen Aufwand.

Simulationsumgebung für Cyberattacken

Um den Unternehmen bei der Erkennung von Cyberangriffen auf ihr Netzwerk ein adäquates Werkzeug an die Hand zu geben, hat die Abteilung CA&D die Simulationsumgebung »BREACH« entwickelt. BREACH ist ein Framework zur realitätsnahen Simulation eines kleinen Unternehmensnetzwerks, gegen das gezielte Angriffe automatisiert oder auch manuell durchgeführt werden können. »Das Ziel war, eine kontrollierbare, reproduzierbare und leicht erweiterbare Umgebung für Forschung, Entwicklung und Schulung zu schaffen, um damit die effektive und effiziente Erkennung von Cyberangriffen in den realen Netzwerken zu verbessern«, erläutert Uetz.

Erforderlich ist hierfür auch ein simuliertes Nutzerverhalten, sodass die simulierten Anwender zum Beispiel Websites aufrufen und auf diesen navigieren, interne und externe E-Mails empfangen und versenden sowie Dokumente erstellen, bearbeiten oder löschen. Darüber hinaus werden sie zu Opfern parallel stattfindender, simulierter Cyberangriffe, indem sie zum Beispiel E-Mails mit infizierten Anhängen öffnen. Das BREACH-Framework umfasst mehrere Angriffsmodule, die sich zu typischen mehrstufigen Cyberangriffen zusammensetzen lassen. Dabei liegt der Fokus auf »Advanced Persistent Threats«, also Angriffen von fachkundigen Akteuren mit überdurchschnittlichen Ressourcen. Hiermit werden nicht nur realistischer Netzwerkverkehr, sondern auch realistische Ereignismeldungen generiert.

Auf diese gesammelten Ereignismeldungen werden dann Methoden angewandt, die eine nachfolgende automatische Analyse erleichtern bzw. überhaupt erst möglich machen. Ereignisse werden normalisiert und um Zusatzinformationen ergänzt, sodass sich unterschiedliche Ereignistypen miteinander vergleichen lassen.

Das vom Fraunhofer FKIE entwickelte Framework kann für ganz unterschiedliche Zwecke verwendet werden: Zum einen können damit existierende Sicherheitsprodukte getestet werden. Zum anderen besteht die Möglichkeit, neue Methoden zur Angriffserkennung zu evaluieren. Aber nicht nur das: So kann das Framework auch für Schulungen verwendet werden, beispielsweise für Mitarbeiter aus den Bereichen Incident Response und Computerforensik, die die Simulationsumgebung einsetzen können, um ihre Kenntnisse in diesem Bereich zu verbessern. Und auch als effektive Awareness-Maßnahme kann das System zum Einsatz kommen, indem Mitarbeitern realistische Angriffe wie z. B. Phishing-Mails und deren Folgen für das Unternehmensnetzwerk gezeigt werden. Ein sinnvoller Einsatz, um Angriffe aus dem Cyberraum frühzeitig zu erkennen. Uetz: »Um eine bessere Erkennung von Datendiebstählen zu ermöglichen, stellen wir Partnern des Fraunhofer FKIE das BREACH-Famework kostenlos zur Verfügung.«

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

AVIATION AND SPACE

Militärische und zivile Luftfahrt stehen für Spitzentechnologie und Innovation. Das Fraunhofer FKIE entwickelt einsatznahe Prototypen für Airport-Management-Systeme, Sensornutzlast- und Fusionskonzepte für fliegende Plattformen, Methoden zur Bedrohungserkennung wie z. B. Beschuss und erforscht den Themenkomplex Nutzung und Abwehr von UAS.

DROHNENABWEHR

Bestmöglicher Schutz vor Angriffen aus der Luft

Drei Tage legte eine Drohne den Londoner Flughafen Gatwick lahm. Erst im Juni 2019 gab es zwei ähnliche Vorfälle in Singapur und erneut in Großbritannien. Derartige Ereignisse, bei denen von Hobby-Piloten gesteuerte Drohnen Schäden oder Störungen verursachen, häufen sich. Wenn jedoch bereits ohne böse Absicht derartige Auswirkungen verursacht werden können, welche Möglichkeit bieten Drohnen dann erst demjenigen, der vorsätzlich Schaden herbeiführen möchte?

Das Problem ist kein neues, doch seine Brisanz verschärft sich, je länger es dauert, geeignete Lösungen zu entwickeln. Denn je länger sensible Punkte wie Massenveranstaltungen, Auftritte wichtiger Persönlichkeiten und Kritische Infrastrukturen wie Flughäfen, Kraftwerke oder Werksgelände ohne ausreichenden Schutz sind, desto wahrscheinlicher ein Angriff.

Ein Team des Fraunhofer FKIE beschäftigt sich damit, das bestmögliche Drohnenabwehrsystem zu entwickeln, zuletzt seit zweieinhalb Jahren als Konsortialführer in AMBOS, einem der vier großen vom BMBF geförderten Drohnenprojekte. An dem deutsch-österreichischen Verbundvorhaben waren insgesamt 16 Partner aus Forschung, Industrie und von Anwenderseite beteiligt. Flankiert wird die technische Entwicklungsarbeit durch gesellschaftsrelevante Begleitforschung mit Blick auf rechtliche und ethische Aspekte. Denn nur, wenn der rechtliche Rahmen klar ist, kann die Abwehr von Drohnen auch tatsächlich erfolgen.

Multimodale Sensoren für bestmögliche Detektion

Die erste Herausforderung liegt in der Schwierigkeit, Drohnen überhaupt erst zu detektieren. Der entwickelte und bereits erfolgreich getestete Demonstrator bindet für ein bestmögliches Ergebnis gleich mehrere Sensoren ein: Funk, Akustik, Elektrooptik, Infrarot und Radar. Die akustische Sensorik etwa wurde kooperativ durch Diehl Defence, Fraunhofer IDMT und Fraunhofer FKIE entwickelt. Die FKIE-Wissenschaftler steuerten vor allem die Algorithmen bei, die die Drohnenflugbahn zeitlich tracken können. Ihre besondere Leistungsfähigkeit ebenso wie ihre Robustheit gegenüber Umgebungsgeräuschen haben sie bei Messkampagnen und der Abschlussdemonstration bereits unter Beweis gestellt.

Ergonomisch optimierte Lagedarstellung

Doch erst durch die Fusion der gesammelten Daten zu Informationen entsteht ein umfassendes Bild und kann eine Drohne möglichst zuverlässig detektiert werden. Auch hier kamen wiederum Arbeiten des Fraunhofer FKIE zum Einsatz: Fusionsalgorithmen, die auf das beste Ergebnis hin trainiert wurden. Der Clou dahinter: Um die Stärken jeder Sensorart optimal zu nutzen, werden die Daten in der Fusion gewichtet verarbeitet und Erwartungsparameter eingesetzt, die die Präzision der Schätzung angeben.

Damit die zusammengeführten Informationen nun auch für die Nutzer, in der Regel Einsatzkräte der Polizei, erfassbar sind, werden sie ebenso wie die möglichen Interventionsmethoden in einem Lagedarstellungs- und Entscheidungsunterstützungssystem ergonomisch optimiert aufbereitet. Die Wissenschaftler des

Fraunhofer FKIE führten zahlreiche Workshops mit Polizeikräften durch, um das User-Interface so nutzerorientiert wie möglich zu gestalten. Entsprechend groß war das Lob während der Abschlussdemonstration im Juni 2019 für dieses Kernsystem, das in der Form neuartig ist.

Entscheidungsunterstützung bei Intervention

In der Auswahl der Abwehrmaßnahmen liegt die nächste Hürde. »Man kann nicht für jedes Szenario die gleichen Abwehrmethoden einsetzen«, so Hans Peter Stuch, Verbundkoordinator von AMBOS und Leiter des FKIE-Teams, das sich auf Counter-UAV-Maßnahmen spezialisiert hat. So ist zwar der Einsatz eines High-Power-Electro-Magnetics-Moduls, das die Steuerelektronik der Drohne außer Kraft setzt und sie so zum Absturz bringt, sehr sinnvoll und effektiv, wenn eine Drohne auf freier Fläche gestoppt werden soll. Völlig ungeeignet ist sie jedoch, wenn sich die Drohne gerade über einer Menschenmenge befindet. Auch dieses Problem wird durch das Entscheidungsunterstützungssystem adressiert, indem es dem Nutzer je nach Situation die passende Interventionsmöglichkeit vorschlägt. Im Falle eines Szenarios mit einer großen Menschenmenge kann beispielsweise ein Jammer eingesetzt werden, der die Signale des Steuerlinks, diejenigen zur Satellitennavigation oder beides stören kann. Das Entscheidende: der Jammer wirkt auch auf größere Distanz, also noch bevor die Drohne die Menschenmenge erreicht hat.

Weiterentwicklung:
Mobiles System bringt Flexibilität

Nun kann man nicht bei jedem Einsatz ein ganzes Lagezentrum mitnehmen und vor Ort aufbauen. »Die logische Weiterentwicklung war da ein kompaktes, mobiles System für die Fusion, Lagedarstellung und Entscheidungsunterstützung«, erklärt FKIE-Wissenschaftler Sven Fuchs. An dieses Kernsystem können dann je nach Bedarf beliebige Sensoren und Effektoren angebunden werden. Möglich wird das jeweils durch einen Adapter, welcher in diesem Falle ein Stück Code ist, der die verschiedenen Komponenten mit der zentralen Einheit verbindet. Entstanden ist ein modulares, hochskalierbares Kernsystem zur Drohnenabwehr mit hohem Marktpotenzial.

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

HOSTILE FIRE INDICATION

Hubschrauber unter Beschuss

Der Beschuss durch Handfeuerwaffen stellt in terroristischen und militärischen Einsatzszenarien eine ernste Bedrohung für Hubschrauber und ihre Besatzungen dar. Durch den hohen Eigenlärmpegel wird ein derartiger Angriff oft erst nach der Landung anhand der Einschusslöcher entdeckt. Die Schützen an Bord befinden sich daher im Daueralarmzustand. Permanent scannen sie die Umgebung unter sich nach potenziellen Angreifern. Gemeinsam mit drei Industriepartnern hat das Fraunhofer FKIE eine Sensorlösung entwickelt, die Beschuss detektiert, klassifiziert und meldet.

An Bord eines Hubschraubers ist es laut, die Lage am Boden unübersichtlich. Aus der Vogelperspektive sind sie daher zunächst einmal alle verdächtig: einzeln stehende Personen, Fahrzeuge oder auch Personen, die sich auf Dächern oder Ladeflächen von Pickups und LKW aufhalten. Bei ihnen allen könnte es sich um potenzielle Schützen handeln. Stress für die Besatzung an Bord, die neben verdächtigen Konstellationen wie diesen vor allem auch Ausschau nach Mündungsfeuer und Rauchentwicklung hält. Ein eindeutiger Beweis für direkten Beschuss ist jedoch auch das nicht. Fakt aber ist: Angriffe durch Handfeuerwaffen haben sich im Kontext militärischer Einsätze zunehmend zu einem Bedrohungsszenario für Hubschrauber entwickelt. Wie kann Technologie helfen?

Lösungskonzept: Sensoren, Vernetzung und Fusion

Das bundeswehrbeauftragte Forschungsprojekt »Hostile Fire Indication (HFI) bei Hubschraubern« hat einen Lösungsansatz in Form eines Assistenzsystems entwickelt, das Beschuss durch Handfeuerwaffen detektiert, klassifiziert und der Hubschrauberbesatzung meldet. Voraussetzung hierfür ist die Aufklärung unterschiedlicher Parameter und Größen: Zeitpunkt und Ort der dichtesten Annäherung des Geschosses zum Luftfahrzeug, d. h. Passierabstand und Richtung zum »Closest Point of Approach« (CPA), Projektilgeschwindigkeit und Kaliber des Geschosses sowie Geschossbahnparameter wie Bahnrichtung und Ursprung des Geschosses zur Lokalisierung des Schützen. Ermittelt werden diese Informationen durch das Zusammenspiel vernetzter akustischer, optronischer und radarbasierter Sensoren sowie darauf basierender Verfahren der Sensordaten- und Informationsfusion.

Optimierungstool Sensordatenfusion

Die herangezogenen Sensorklassen Akustik, Optik und Radar detektieren unabhängig voneinander unterschiedliche Merkmale eines abgefeuerten Geschosses: So erfasst der akustische Sensor den Mündungs- und Geschossknall, die Infrarot-Kamera bei einer ausreichend hohen Bildrate den Mündungsblitz einer abgefeuerten Waffe. Die radarbasierte Detektion wiederum, im Projekt durch ein Doppler-Radar umgesetzt, erkennt nur Geschosse in unmittelbarer Umgebung des Hubschraubers. Einen wichtigen Teil der Untersuchungen stellte daher die Fusion aller gesammelten Sensorinformationen dar. Sie sollte zur Steigerung der erzielbaren Aufklärungsleistung und damit zur Verbesserung der Zuverlässigkeit, Robustheit und Genauigkeit des HFI-Konzeptes beitragen.

Evaluierung mittels realer Flug- und Beschusskampagnen

Das Sensorik-Konzept wurde im Rahmen des zweijährigen Projekts so weit umgesetzt, dass es in eine Demonstrator-(Hubschrauber-)Plattform eingerüstet und im Rahmen mehrerer realer Flug- und Schießkampagnen auf dem Gelände der Wehrtechnischen Dienststelle für Waffen und Munition (WTD 91) in Meppen getestet werden konnte. Mittels »gezieltem Vorbeischuss« mit unterschiedlichen Kalibern aus verschiedenen Richtungen und bei unterschiedlichen Fluggeschwindigkeiten des eingesetzten Hubschraubers konnten Sensortechnologien und erarbeitete Fusions-ansätze erfolgreich evaluiert werden.

Konsortium aus Industrie und Forschung

An der Ausarbeitung der F&T-Studie, die durch das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) beauftragt war, waren neben dem Fraunhofer FKIE (Sensordatenfusion) mit Airbus Helicopters Deutschland (Integration, Demonstrator, Generalunternehmer), Rheinmetall Defence Electronics (Akustik- und Infrarot-Sensorik) und Hensoldt (Radar-Sensorik) drei weitere namhafte Industriepartner beteiligt. »Das Projekt ist zunächst offiziell beendet«, erklärt FKIE-Forschungsgruppenleiter Dr. Marc Oispuu den aktuellen Stand, »allerdings sind alle Partner strategisch daran interessiert, ihre Produkte weiterzuentwickeln. Die im Rahmen der Studie erarbeiteten Ergebnisse werden daher entsprechend weiterverwendet und fließen so eventuell zu gegebener Zeit in ein Folgeprojekt ein.«

KONTAKT
Dr. Marc Oispuu
Telefon +49 228 9435-853
marc.oispuu@fkie.fraunhofer.de

HUBSCHRAUBERSIMULATION FÜR AUSBILDUNG UND TRAINING

Mit VR-Brillen den realen Einsatz trainieren

Hubschrauber-Missionen stellen die Besatzungen oftmals vor große Herausforderungen: Gelände erkunden, Verletzte bergen, schwierige Transporte, Unterstützung der Kameraden am Boden aus der Luft. Das bedeutet höchste Anforderungen an die Crew an Bord. Doch auch wenn jeder Einsatz anders ist, lassen sich kritische und gefährliche Situationen durch gezielte Trainings beherrschbar machen. Bislang wird die gesamte Besatzung wenig in Simulationen trainiert. Virtuelle Lernumgebungen könnten für ein individualisiertes Training der vollständigen Besatzung sorgen.

In einem Kooperationsprojekt mit der Wehrtechnischen Dienststelle für Waffen und Munition (WTD 91) in Meppen werden seitens des Fraunhofer FKIE die Möglichkeiten betrachtet, welche Einsatzgebiete für Virtual Reality-Anwendungen in der Bundeswehr existieren. Anhand praxisnaher Studien und Probandenexperimenten wird u. a. der mögliche Einsatz von Virtual Reality (VR) zur Aus- und Weiterbildung für die Mitglieder der Hubschrauber-Crew getestet. Dabei geht es neben der praktischen Umsetzbarkeit auch um Potenziale und Grenzen der VR-Technologie am konkreten Beispiel kompetenzorientierter Ausbildung und individualisierten Lernens.

Sinnvolle Ergänzung zur praktischen Ausbildung

VR wird in der Bundeswehr bislang kaum angewendet, um die Soldaten auf aktuelle und bevorstehende Einsätze im In- und Ausland vorzubereiten. Für die Mitglieder der Hubschrauber-Crew könnte VR jedoch den Vorteil haben, dass der Trainingsflug individualisiert, effektiv und kosteneffizient gestaltet werden kann. »VR bietet ein besonderes Potenzial für die Vermittlung von Ausbildungsinhalten. Allerdings kann sie die traditionelle Ausbildung im Hubschrauber natürlich nicht ersetzen, dafür aber spezielle Trainingseinheiten sinnvoll ergänzen«, erläutert FKIE-Projektleiterin Mara Kaufeld. Bei der Studie stehen ihr nicht nur VR-Brillen, sondern auch eine Bewegungsplattform seitens der WTD 91 zur Verfügung. Diese Kombination sorgt für ein optimales Trainingsumfeld in dem Experimentalsystem, das neben der visuellen Wahrnehmung auch die Bewegungen des Hubschraubers nachempfindet. Die aktivierte Bewegungsplattform kann dabei helfen, die Übertragung von Trainingsinhalten auf die Realsituationen zu erleichtern. Um den Unterschied noch deutlicher herauszuarbeiten und das persönliche Trainingsempfinden der Probanden zu erfassen, haben alle Teilnehmer das Training mit und ohne Bewegung der Plattform durchgeführt.

Verschiedene Schwierigkeitsgrade

Die Szenarien, die bei der kombinierten VR- und Bewegungsplattform-Simulation »durchflogen« werden, sind eher experimenteller Natur und werden in künftigen Schritten zunehmend realistischer. Zunächst geht es darum, das Potenzial der Technik zu analysieren. An den verschiedenen Testläufen haben neben Non-Professionals, also Menschen ohne Flugerfahrung, auch sehr flugerfahrene Soldaten teilgenommen, die sensibel auf veränderte Darstellung, Geräusche und Bewegungen reagieren. Weiterer Schwierigkeitsgrad: Während des Trainings mussten die Probanden mehrere Aufgaben bewältigen, wie zum Beispiel bestimmte Objekte innerhalb der vorbeifliegenden Landschaft erkennen. Im Anschluss befragte Kaufeld zusammen mit Experten der WTD die Teilnehmer mit standardisierten Fragebögen in halbstrukturierten Interviews über die psychische Beanspruchung während des Simulatortrainings. Außerdem gaben sie Auskunft über Symptome der Simulatorkrankheit, die vielfach bei VR-Anwendungen auftritt, sowie über ihre verschiedenen Wahrnehmungen während der Tests. Darunter fällt auch, inwieweit simulierte Szenarien den Aufbau von Vertrauen und Kompetenz sowie eine gewisse Routine im Umgang mit kritischen Situationen fördern. Zudem wurden die Teilnehmer zum »Präsenzempfinden« befragt, also dem Gefühl, sich in der virtuellen Welt zu befinden und darin zu agieren.

Routine für gefährliche Einsätze

Das Feedback der Teilnehmer auf diese Form der technischen Unterstützung innerhalb der Ausbildung war gut. Insbesondere die realistische Darstellung durch VR und Bewegungsplattform wurde seitens der Probanden als sinnvolle Trainingsergänzung hervorgehoben, um mehr Routine für die anspruchsvollen Hubschrauber-Einsätze zu gewinnen.

Ein nächster Schritt auf dem Weg zum VR-Einsatz bei der Aus- und Weiterbildung wäre ein Test mit einem vernetzten Training für zwei oder mehrere Besatzungsmitglieder. Hier könnten dann neben der Lösung gemeinsamer Aufgaben auch noch die Teamfähigkeit sowie verschiedene Kommunikationsprozesse zwischen den einzelnen Akteuren an Bord des Hubschraubers im Fokus der neuen Studie stehen.

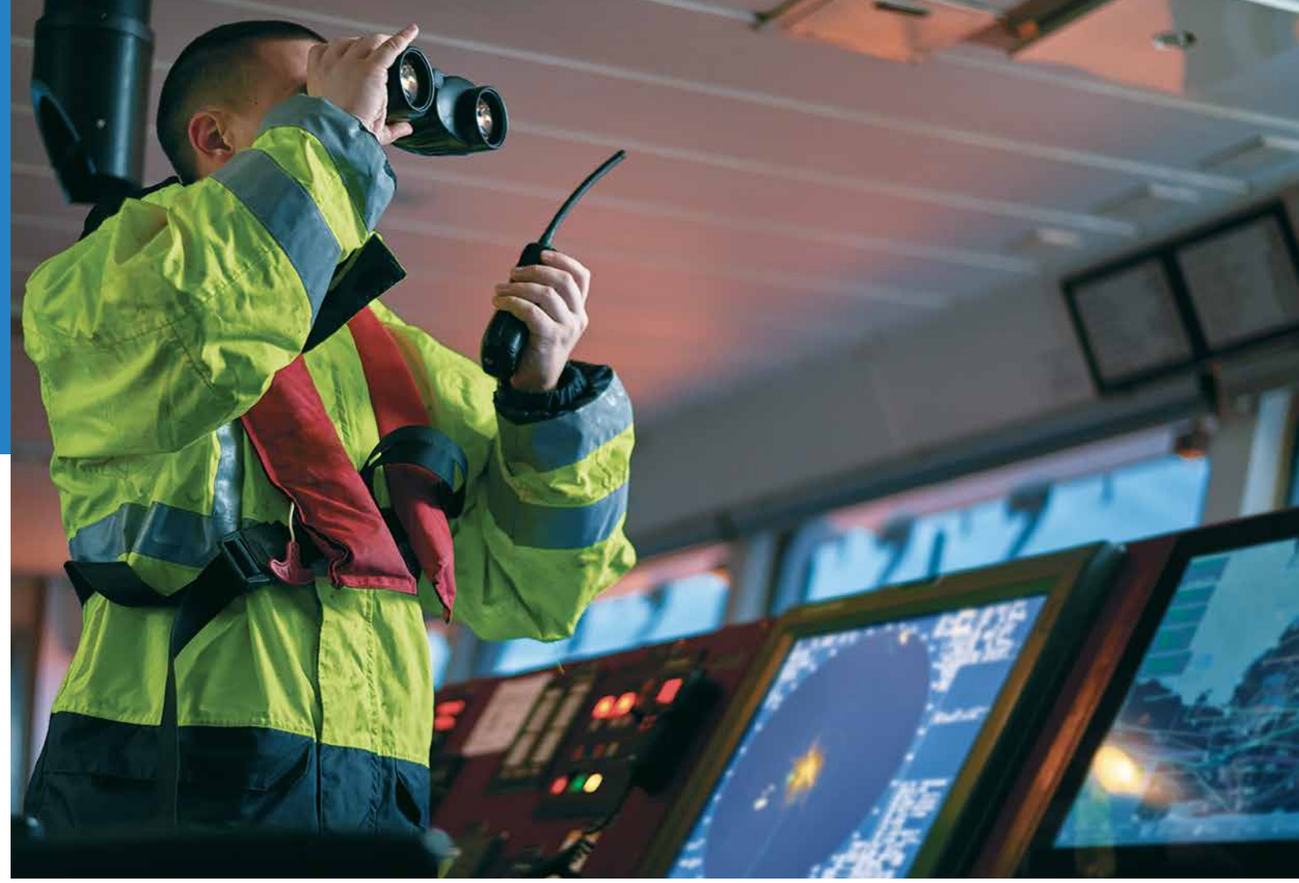
KONTAKT
Mara Kaufeld
Telefon +49 228 50212-419
mara.kaufeld@fkie.fraunhofer.de

MARITIME SYSTEMS

Fragestellungen zum Schutz und Einsatz maritimer Systeme und Infrastrukturen für militärische wie auch zivile Anwendungen zählen zu den Kernforschungsfeldern des Fraunhofer FKIE. Die Arbeiten sind dabei vorrangig auf sicherheitsrelevante Aspekte fokussiert, wie beispielsweise die Cybersicherheit maritimer IT-Systeme, die Hafenüberwachung durch Passivradar und sichere Unterwasserkommunikation.

MARITIME SYSTEMS

CYBERSICHERHEIT FÜR MARITIME IT-SYSTEME



Schutz der Brücke vor Cyberangriffen

Blockierte Seewege, havarierte oder gar kollidierte Kreuzfahrt- und Containerschiffe: Eingriffe in IT-Systeme an Bord können katastrophale Folgen für Mensch und Umwelt wie auch immense wirtschaftliche Schäden mit sich bringen. Denn mit der Digitalisierung, der vermehrten Nutzung von IT-Systemen sowie der zunehmenden Vernetzung der IT wächst auch an Bord von Schiffen das Risiko für Angriffe aus dem Cyberraum. An dieser Stelle wird das Fraunhofer FKIE aktiv und trägt mit seiner Analyse maritimer IT-Systeme und notwendigen Schutzmaßnahmen zu mehr Sicherheit in der Seeschifffahrt bei.

Längst sind Schiffe mit modernster Informations- und Kommunikationstechnik ausgestattet. Diverse intelligente Teilsysteme sorgen für einen reibungslosen Schiffsbetrieb. Aber: Elektronik wie Navigations-, Tracking- und Kollisionswarnsysteme dienen zwar der Sicherheit auf See, stellen aber gleichzeitig eine Angriffsfläche für Cyberkriminalität dar und müssen daher ausreichend geschützt sein. Zudem steigern die IT-Systeme nicht nur die Vernetzung an Bord, sondern liefern gleichzeitig eine wesentliche Verbindung nach extern. Insbesondere diese Kommunikationswege zwischen Land und Schiff bieten eine besondere Angriffsfläche für Manipulationen. Denn anders als zum Beispiel bei Firmennetzen steht nicht das Abgreifen sensibler Daten im Vordergrund. Vielmehr liegt der Schwerpunkt bei der funktionalen Sicherheit an Bord, wenn zum Beispiel Hacker eine Schadsoftware in der Leittechnik von Schiffen platzieren, Koordinaten ändern oder sich Zugriff auf sicherheitsrelevante Teilsysteme verschaffen.

Angriffsvektoren wurden identifiziert

Folgerichtig ist die langfristige Absicherung maritimer IT-Systeme auch ein Thema für die Abteilung »Cyber Analysis and Defense« (CA&D) am Fraunhofer FKIE. Eindeutiger Fokus der Wissenschaftler rund um Christian Hemminghaus liegt darin, die Schifffahrtsbranche dabei zu unterstützen, das Cyberrisiko beherrschbar zu machen, indem Brückensysteme gegen Angriffe von außen abgesichert werden.

In einer Studie des Bundesamtes für Verkehr und digitale Infrastruktur (BMVI) wurde zunächst eine Cyberrisikoanalyse integrierter Brückensysteme durchgeführt, um Gefährdungen und Angriffsvektoren zu identifizieren. Mit den Ergebnissen wurden dann aktuelle Standards und Best Practices seitens der maritimen Branche verglichen. Auf Grundlage der Risikoanalyse entwickelten die FKIE-Wissenschaftler in Zusammenarbeit mit Herstellern, Betreibern und Behörden im Rahmen des Projektes ACTRESS (»Architecture and Technology Development Platform for Realtime Safe and Secure Systems«) ein Modell für ein integriertes Brückensystem mit Umgebungssimulation. Denn allein schon wegen der bestehenden Gesetzeslage kann an dieser Stelle nur »an Land« getestet werden: »Die experimentelle Durchführung von Cyberangriffen auf fahrenden Schiffen ist aus Sicherheitsgründen nicht erlaubt«, erläutert Hemminghaus. »Deshalb ist unser Ziel, mithilfe realistischer Angriffs- und Schadenssimulationen ein systematisches Risikomanagement für die maritime Branche in die Wege zu leiten.« Darunter ist die Detektion von Cyberangriffen ebenso zu verstehen wie Maßnahmen gegen Schadsoftware, ein Update von Systemen sowie die Entwicklung langfristiger Sicherheitsmaßnahmen und -technologien.

Heterogene IT-Landschaft an Bord

Als problematisch erweist sich laut Hemminghaus die heterogene IT-Landschaft auf Schiffen: Ein Nachrüsten an Bord befindlicher Systeme gestaltet sich oftmals als sehr schwierig. Denn das Alter der Bord-IT sorgt in vielen Fällen dafür, dass wirksamer Schutz kaum etabliert werden kann. Außerdem steht der lange Lebenszyklus von Schiffen im Gegensatz zu modernen, wirkungsvoll geschützten IT-Anlagen. »Größte Herausforderung für die Schifffahrt wird daher sein, Apparaturen an Bord auf einen Stand der Technik zu bringen, wie man ihn an Land hat«, meint Hemminghaus. Das würde für viele Reedereien ein kostenintensives Umrüsten auf die neueste Technik bedeuten, dafür aber eine langfristige Reduzierung von Angriffszielen auf maritime IT-Systeme.

Bislang haben sich die Forschungsarbeiten am Fraunhofer FKIE auf den Schutz der Schiffsbrücken und der Navigation beschränkt. »Um allerdings eine ganzheitliche Cybersicherheit an Bord zu gewährleisten, darf die gesamte, angrenzende Schiffselektronik nicht außer Acht gelassen werden«, warnt Hemminghaus. Aus diesem Grund werden sich künftige Forschungen auch auf die externe Kommunikation der Schiffe, die Automation, den Schiffsantrieb sowie die Energieversorgung des Schiffes fokussieren, um weitere Angriffsszenarien wie auch Angreifermodelle konsequent im Blick zu haben.

KONTAKT
Christian Hemminghaus
Telefon +49 228 50212-605
christian.hemminghaus@fkie.fraunhofer.de

MARITIME SYSTEMS

HAFENÜBERWACHUNG DURCH PASSIVRADAR

Bedrohungsdetektion für Schiffe im Hafenbereich

Das amerikanische Kriegsschiff »USS Cole« erlangte traurige Bekanntheit, als zwei radikalislamische Selbstmordattentäter ein mit Sprengstoff beladenes Schlauchboot gegen den Zerstörer steuerten. 17 US-Soldaten starben bei dem Angriff im Hafen von Aden/Jemen. Der Vorfall spiegelt ein neues Bedrohungsszenario für Häfen und Marinestützpunkte wider. Im Auftrag der Bundeswehr entwickelt das Fraunhofer FKIE eine Passivradar-Lösung, die kleine, agile, eventuell angreifende Boote im Hafengebiet erkennt, trackt und meldet.

Die Bedrohungslage für Schiffe, Häfen und Marinestützpunkte hat sich geändert. Längst spielen darin nicht mehr andere Kriegsschiffe die einzige Rolle, sondern auch terroristische Szenarien mit schnellen, wendigen Schlauch- oder Aluminiumbooten. Zur ihrer Erkennung und Bewertung der Bedrohung hat das Fraunhofer FKIE im Auftrag der WTD 71, der Wehrtechnischen Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung, ein System entwickelt, das auf passivem, multistatischem Radar mit GSM-Basisstationen als Beleuchtern basiert. »Die Lösung sollte dabei auch Anwendungsszenarien umfassen, in denen deutsche Schiffe in fremden Häfen liegen und das andere Land bzw. der jeweilige Hafenbetreiber somit Hausrecht hat«, erläutert FKIE-Projektleiter Benjamin Knödler die Herausforderung des Forschungsvorhabens. »Aktivradar ist dort keine Option, da hierfür individuelle Genehmigungen erforderlich sind. Aus diesem Grund haben wir Passivradar als Methode eingesetzt, um die Überwachungslücke zu schließen.«

Mobilfunk-Basisstationen als Beleuchter

Ausschlaggebend für diesen Lösungsansatz ist die Tatsache, dass sich in der Umgebung von Hafenanlagen in der Regel zahlreiche Mobilfunk-Sendemasten befinden, die küstennah eine optimale Versorgung sicherstellen. Diese Masten senden permanent ein Signal, das auch für einen passiven Radarbetrieb genutzt werden kann. Passive Coherent Location (PCL) nennt sich die passive Sensortechnologie, die hierbei zum Einsatz kommt und die bestehende Signale, wie beispielsweise von Mobilfunk-Basisstationen oder von analoger/digitaler Rundfunktechnologie, zur Beleuchtung von bewegten Zielen verwendet. Mobilfunksignale für Passivradar zu nutzen, stellt eine Herausforderung dar, da ihre Signalform nicht für den Radarbetrieb optimiert und ihre Sendeleistung relativ gering ist. Von Vorteil ist allerdings die große Anzahl verfügbarer Basisstationen und der durch sie permanent vorhandenen Broadcast-Signale.

Durch die Reflexion dieser Signale an einem Ziel (Boot) kann mittels passiver Empfangssensorik auf den Zielzustand (Position, Geschwindigkeit des Bootes) geschlossen werden. Über mehrere Messzeitpunkte hinweg kann somit eine Spur des Ziels (Track) erstellt werden. Multistatik, also die Beleuchtung aus unterschiedlichen Perspektiven, spielt hierbei immer eine wichtige Rolle. In besonderem Maße allerdings bei kleinen, agilen Booten, die nur eine geringe, sich zudem schnell fortbewegende Reflexionsfläche bieten. »Die Broadcast-Signale der Basisstationen sollen die Mobilfunkversorgung sicherstellen, und dies logischerweise vor allem in Bodennähe. Sie eignen sich somit gut für die Überwachung niedrigerer Hafenbereiche«, berichtet Knödler. »Weiterer Vorteil der Methode ist, dass die Marine sie überall einsetzen kann – selbst an ausländischen Stützpunkten.« Das gesamte hierfür erforderliche Equipment, das auf einen Anhänger oder in einen Container passt, kann auf dem Schiff mitgeführt werden. »Das gesamte System ist in 1,5 Stunden funktionsbereit.«

Erfolgreiche Messkampagnen in Eckernförde

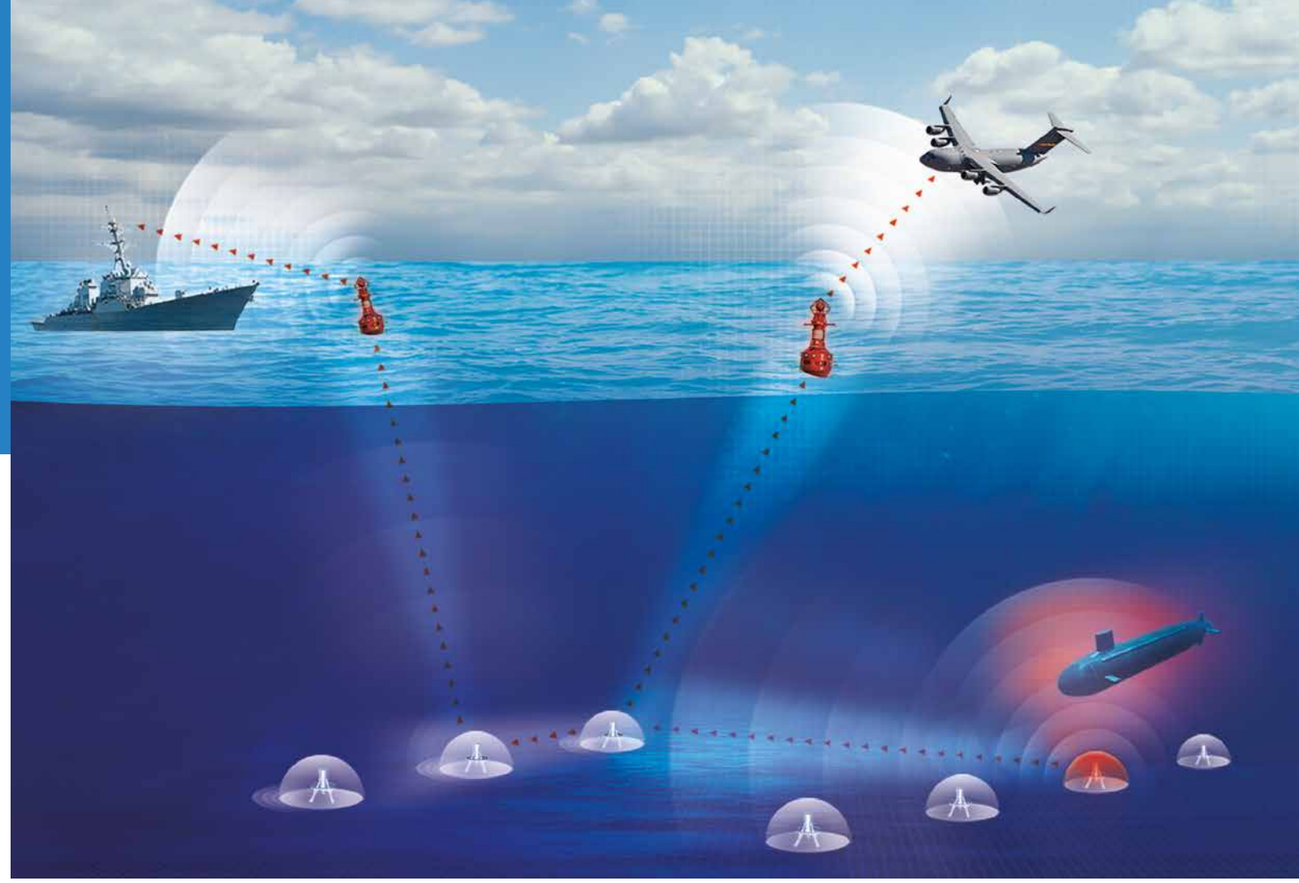
Zur Überprüfung der Leistungsfähigkeit des Systems wurden seit Beginn des Projekts im Jahr 2015 insgesamt vier Messkampagnen in der Bucht von Eckernförde durchgeführt. Die Szenarien wurden dabei aufwendig nachgestellt – mit großen Schiffen, kleinen Booten und teils sogar Jetskis, die im Einsatz waren. Die Detektions- und Trackingergebnisse verbesserten sich von Jahr zu Jahr. »Wir haben das System unter allen Witterungsbedingungen getestet, auch bei schlechtem Wetter mit starkem Seegang und hohen Wellen«, erzählt Knödler. »Die Abschlussdemonstration im September 2018 war ein voller Erfolg. Wir konnten Hard-, Software und Datenfusion so weit optimieren, dass das System jetzt Schritt haltend, lediglich mit einem Initial-Zeitversatz von fünf bis sechs Sekunden arbeitet. Zu Beginn des Projekts war die Auswertung noch reine Laborsache. Das Passivradar lebt von der Sensordatenfusion. Erst sie ermöglicht die erfolgreiche Lokalisierung und das Tracking von Zielen.«

Einbindung unterschiedlicher Mobilfunktechnologien geplant

Das Projekt wird aktuell im Rahmen einer Folgezuwendung fortgeführt. Die Weiterentwicklung besonders innovativer und hochleistungsfähiger Ansätze, zum Beispiel Track-before-Detect, stehen hierbei im Zentrum der Untersuchungen, ebenso wie die Verwendung von Signalen unterschiedlicher Mobilfunkstandards wie beispielsweise LTE. Ihre Hinzunahme als Beleuchter erlaubt eine größere Abdeckung und Genauigkeit sowie die Detektion und das Tracking von Zielen, die bei der Verwendung nur einer Technologie eventuell nicht erfasst werden. Weitere Vorteile sind außerdem die noch größere Anzahl verfügbarer Basisstationen und somit die optimale Ausleuchtung der überwachten Hafengebiete.

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

SICHERE UNTERWASSERKOMMUNIKATION



Internet of Things unter Wasser

Vernetzte Geräte sind allgegenwärtig. Jeder ist in das Internet of Things, in die miteinander kommunizierenden Technologien, eingebunden. Was an Land völlig normal ist, ist unter Wasser jedoch alles andere als selbstverständlich. Aber getreu dem Fraunhofer-Motto »Geht doch!« hat sich ein Forscherteam des Fraunhofer FKIE genau dies zum Ziel gesetzt: Unterwassersensoren, U-Boote, autonome Tauchfahrzeuge, Bojen und Schiffe untereinander zu vernetzen.

Anwendungsszenarien sind etwa der Klimaschutz, Frühwarnsysteme, aber auch die militärische Kommunikation und Aufklärung. Hierzu hat das FKIE-Team um Michael Goetz gemeinsam mit der Wehrtechnischen Dienststelle für Schiffe und Marinewaffen, Maritime Technologie und Forschung (WTD 71) bereits vor vier Jahren das Netzwerkprotokoll GUWMANET® entwickelt.

Höhere Datenraten für bessere Kommunikation und mehr Freiheitsgrade

Nun ist 2018 das Folgeprojekte SALSA (Smart Adaptive Long and Short Range Underwater Acoustic Networks) auf EU-Ebene gestartet. Ging es zunächst darum, Ad-hoc-Netzwerke über Bodenknoten überhaupt erst zu ermöglichen, geht es in SALSA darum, durch den Einsatz von zwei Frequenzbändern höhere Datenraten zu erzielen. Denn die in GUWMANET® eingesetzten Schallwellen boten zwar durch tiefe Frequenzen die im Vorgängerprojekt geforderten hohen Reichweiten, konnten aus diesem Grund aber auch nur geringe Datenraten übertragen. Durch die Ergänzung um ein weiteres Frequenzband, welches besonders hochfrequent ist, soll eine Steigerung der Datenrate erzielt werden. So sollen nun etwa Tauchfahrzeuge in die Lage versetzt werden, deutlich besser zu kommunizieren und zu interagieren.

Bojen überbrücken die Grenze zwischen Unter- und Überwasserwelt

Doch nicht nur auf EU-Ebene wird weitergearbeitet, auch auf nationaler Ebene wird mit Beteiligung von Fraunhofer FKIE an diesem Thema weitergeforscht. So werden beispielsweise zwei Prototypen von Bojen – auch hier wieder in Zusammenarbeit mit der WTD 71 – entwickelt, die als Bindeglied zwischen Unter- und Überwasserkommunikation fungieren sollen. Hierzu haben Michael Goetz und seine Kollegen die Prototypen einerseits mit einem Unterwasser-Modem ausgestattet und sie andererseits zu schwimmenden LTE-Zellen gemacht.

Insbesondere der Einsatz des Mobilfunkstandards der vierte Generation, also LTE, ist im maritimen Bereich noch völlig neu. Erst durch diese Idee kann das Unterwassernetz an die sich in Betrieb befindlichen Schiffe angebunden werden. »Wir schließen hier eine Lücke und erzielen deutlich mehr Freiheitsgrade,« so der Wissenschaftler, »Man muss bedenken, dass es zuvor notwendig war, die Schiffe zu ankern, damit sie überhaupt erst etwas empfangen konnten. Auch mussten so viele Maschinen auf dem Schiff wie möglich abgestellt werden, damit die schwachen Signale des Ad-hoc-Netzwerks nicht gestört wurden. Dies alles ist nun nicht mehr notwendig.«

Entscheidend: der Sicherheitsfaktor

Eine zweite Neuerung, die diese Art der Kommunikation erst für den militärischen Einsatz brauchbar macht, ist die Berücksichtigung des Sicherheitsaspekts. Goetz und seine Kollegen haben die Unterwasserkommunikation durch Verschlüsselungsmöglichkeiten ergänzt und damit vor Cyberangriffen geschützt. Goetz hat aber auch schon die nächsten Baustellen und Weiterentwicklungspotenziale im Blick: »Wenn die Bojen im Einsatz sind, wird auch denkbar, dass diese zum Stören oder Aufklären der gegnerischen Kommunikation genutzt werden können. Auch können Sensoren angebunden und Akustikaufzeichnungen angefertigt werden. Den Anwendungsmöglichkeiten sind also kaum Grenzen gesetzt!«

KONTAKT
Michael Goetz
Telefon +49 228 50212-477
michael.goetz@fkie.fraunhofer.de

LAND SYSTEMS

Der Bedarf an teilautonomen Assistenzfunktionen zur Leistungssteigerung landgebundener Systeme für militärische und zivile Zwecke wächst. Sie vereinfachen deren Steuerung und Navigation oder unterstützen die Umgebungswahrnehmung und Tele-Manipulation. Das Fraunhofer FKIE erforscht und entwickelt Funktionsdemonstratoren für den Test im realen Einsatz.

AUFBAU DES DEUTSCHEN RETTUNGSROBOTIK-ZENTRUMS

Intelligente Roboter unterstützen Einsatzkräfte

1,3 Millionen Feuerwehrleute leisten in Deutschland jährlich rund 3,9 Millionen Einsätze. Hierbei müssen sie sich immer wieder großer Gefahr aussetzen. Künftig sollen die Einsatzkräfte daher von intelligenten Robotern unterstützt werden. Zu diesem Zweck haben 13 Projektpartner aus Brandschutz, Industrie und Forschung, darunter das Fraunhofer FKIE, Ende 2018 das Projekt »Aufbau des Deutschen Rettungs-robotik-Zentrums« (A-DRZ) gestartet. Das Kompetenzzentrum entsteht auf dem ehemaligen Dortmunder Industriegelände Phoenix-West und soll bis Ende 2022 fertiggestellt sein.

»Schicke ich meine Mannschaft da rein oder nicht?« Tag für Tag stehen Einsatzleiter der Feuerwehren vor dieser Frage und befinden sich damit in einem Entscheidungs-dilemma. Sie sind vertraut mit ihren Kolleginnen und Kollegen, kennen deren Familien, tragen Verantwortung für sie. Genauso bewusst sind sie sich ihres beruflichen Auftrags. Und der heißt: Menschen aus Gefahren retten und Schaden begrenzen. Oft sind Lage und Gefahr-potenzial eines Einsatzszenarios allerdings nicht klar. Eine schwierige Entscheidung also für die Einsatzleiter. Und immer mit dem Risiko verknüpft, die falsche zu treffen. Denn trotz guter Ausbildung, taktischen Konzepten und Schutzausrüstung werden weltweit jedes Jahr Tausende von Feuerwehrleuten im Einsatz verletzt oder getötet.

Rettungsrobotik-Zentrum mit Living Lab gestartet

Um dieses Risiko einzudämmen, sollen Roboter künftig unterstützen. Sie sollen Aufgaben übernehmen, die die Einsatzabwicklung effizienter und vor allem sicherer für die Einsatzkräfte machen. Auf dem ehemaligen Dortmunder Industriegelände Phoenix-West entsteht zu diesem Zweck ein Kompetenzzentrum, in dem mobile Robotersysteme für die zivile Gefahrenabwehr in einem sogenannten Living Lab erforscht und entwickelt werden. Eine Besonderheit des Labors sind die daran angeschlos-senen, innen und außen liegenden Versuchsflächen, auf denen die Systeme gemeinsam mit den Anwendern in realen Einsatzszenarien auf ihre Tauglichkeit erprobt werden. Basis bilden die vier Leitszenarien »Feuer«, »Ein-sturz & Verschüttung«, »Detektion von Gefahrstoffen« und »Hochwasser«. Die Anforderungen an die unter-stützenden Robotersysteme sind dabei komplex und viel-fältig. Zudem drängt die Zeit, denn die Einsatzkräfte sind Tag für Tag den Gefahren ausgesetzt. Und in zunehmen-dem Maße stehen sie vor Einsatzszenarien, die sie vor riesige Flächen und großen zeitlichen Druck stellen, Stichwort: Waldbrände und Hochwasser.

Mit der Implementierung des A-DRZ arbeiten in Deutsch-land erstmalig Einsatzkräfte, Forscher und Industrie gemeinsam an der Entwicklung von Rettungsrobotern zur Unterstützung in der zivilen Gefahrenabwehr. Auch der Aufbau einer national und international agierenden Robotik-Einsatzgruppe für den Krisenfall ist geplant. Zudem sollen Test- und Prüfkriterien für eine spätere Standardisierung und Zertifizierung unterschiedlicher Robotersysteme erarbeitet werden.

Flexible, modulare Roboter erforderlich

Schwerpunkt des Projektanteils des Fraunhofer FKIE ist die Zusammenführung von Hard-, Software und Schnitt-stellen der Technik. »Einige Feuerwehren haben bereits Roboter für spezielle Aufgaben im Einsatz, der Großteil jedoch nicht«, erläutert FKIE-Projektleiter Thomas Barz und weist damit auf eine der großen Herausforderungen seiner Arbeit hin. »Ziel muss sein, die robotischen Syste-me so einheitlich, modular und flexibel wie möglich zu gestalten. Je besser das gelingt, desto wahrscheinlicher sind die Chancen für ihre möglichst zeitnahe und breit-flächige Einführung zur Unterstützung der Einsatzkräfte.« Bereits beim ersten Verbundtreffen sechs Monate nach Projektstart konnte sein Team einen weit fortgeschrittenen Stand der Aufgaben vorweisen. Barz: »Wir haben sehr schnell das Initialkonzept für eine plattformübergreifende Modularisierung erstellt, damit alle anderen Partner dar-auf aufbauen können.«

BASF als größte Werkfeuerwehr assoziiert

Fraunhofer FKIE konnte zudem BASF als assoziierten Projektpartner für den Aufbau des Rettungsrobotik-Zentrums werben. Die Werkfeuerwehr des Konzerns stellt den Brandschutz auf dem weltweit größten zusam-menhängenden Chemie-Areal und kooperiert mit dem Institut bereits bei der Entwicklung von Roboterplatt-formen zur Unterstützung ihrer Einsatzkräfte. Ein wichti-ger beratender Partner somit.

Finanzielle Anschubförderung

Das Bundesministerium für Bildung und Forschung (BMBF) unterstützt das auf vier Jahre angelegte Projekt im Rahmen der Förderbekanntmachung »Zivile Sicher-heit – Innovationslabore/Kompetenzzentren für Roboter-systeme in menschenfeindlichen Umgebungen« mit 11,9 Millionen Euro. »Angesichts eines jährlichen BMBF-Gesamtbudgets für die Sicherheitsforschung von 60 Millionen ist das ein großer Batzen Geld«, machte BMBF-Ministerialrätin Sabine ten Hagen-Knauer bei der Auftaktveranstaltung zum Start des Projekts deutlich und damit auch die hohen Erwartungen, die von Geld-geberseite mit dem Vorhaben verknüpft sind. Langfris-tiges Ziel ist es, das Kompetenzzentrum auch über die Initiierungs- bzw. Förderphase hinaus zu etablieren, um kontinuierlich immer leistungsfähigere Robotik für Rettungskräfte am Markt verfügbar zu machen.

KONTAKT
Thomas Barz
Telefon +49 228 9435-623
thomas.barz@fkie.fraunhofer.de

AUTOMATISIERTES FAHREN

Kooperatives, statt autonomes Fahren für die Bundeswehr

Autonom fahrende Autos nehmen eine Schlüsselrolle in der Mobilität der Zukunft ein. Die Automobilindustrie arbeitet in unterschiedlichen Kooperationen auf Hochtouren daran, autonome oder zumindest automatisierte Fahrzeuge weiter zu entwickeln und auf den breiten Markt zu bringen. Im Bereich von Nutzfahrzeugen und Fahrdiensten sicherlich flächendeckender als bei privaten Serien-Pkws. Aber lässt sich diese Technologie auch für die Bundeswehr nutzbar machen? Und für welche militärischen Fahrzeugtypen? Diesen Fragen geht das Wissenschaftler-Team der Abteilung »Systemergonomie« (SE) des Fraunhofer FKIE nach.

Die Rahmenbedingungen, unter denen automatisiertes Fahren zum Beispiel bei Panzern eingesetzt werden kann, sind um einiges komplexer als im Fall der zivilen Nutzung, auch wenn selbst diese alles andere als trivial ist. Entsprechend können die Technologien, die im zivilen Bereich automatisiertes Fahren bereits ermöglichen und einen Einsatz auf speziellen Strecken und in bestimmten Verkehrssituationen zulassen, nicht ohne Einschränkungen in den militärischen Einsatz übernommen werden. Ein militärisches Fahrzeug muss beispielsweise sowohl für den Straßenverkehr als auch für Gefechtssituationen ausgelegt sein, was schon allein aufgrund der unterschiedlichen Bodenbeschaffenheit eine große Robustheit, etwa der Sensoren, erfordert.

Die Lösung aus der Forschung:
Kooperatives Fahren

Eine Lösung verspricht hier die Forschung der FKIE-Wissenschaftler, denn der Schwerpunkt der Abteilung Systemergonomie (SE) liegt gerade in der Erforschung der kooperativen Fahrzeugführung. Gemeint ist hiermit die adaptierbare, zwischen Fahrzeug und Fahrzeugführer geteilte Kontrolle, was im Begriff der »adaptiven Automation« zusammengefasst wird. Dabei kann je nach den Erfordernissen der Situation die Kontrolle in unterschiedlichen Stufen der Assistenz und Automation an das technische System abgegeben und wieder übernommen werden. »Hierbei handelt es sich um kooperativ geführte, assistierte, teil- und hochautomatisierte Systeme, also ein ausgefeiltes, balanciertes Mensch-Maschine-System«, betont SE-Abteilungsleiter Professor Dr.-Ing. Frank Flemisch.

Nutzergerechte Gestaltung
aus dem Kreativlabor der Forscher

Wie genau dies eingesetzt werden kann, wird u. a. im sogenannten »Exploroscope« erforscht. Dort entstehen mithilfe von Methoden des partizipativen Gestaltens Mock-ups, Papierprototypen sowie Systemkonzepte und -entwürfe bis hin zu Soft- und Hardware-Prototypen. An einem derartigen Hardware-Prototyp kann die optimale Lösung für die Anwender bis ins Detail ausgearbeitet werden. Vorteil dieser Vorgehensweise ist, mit klar definiertem Aufwand, Lösungsmöglichkeiten bereits früh erleb- und überprüfbar zu gestalten, sodass Risiken teurer Fehlentwicklungen deutlich vermindert werden. So kann beispielsweise getestet werden, wie stark haptische Signale des Systems angelegt sein müssen, etwa der Widerstand eines Gaspedals bei der Anpassung von Geschwindigkeit oder Abstand beim Abstandsregeltempomat oder auch eine Vibration des Lenkrads, wenn

der Fahrzeugführer in heiklen Situationen darauf hingewiesen werden soll, dass er umgehend wieder die Kontrolle übernehmen muss.

Der Mensch als Entscheidungsträger im Loop

Vielfältige Aspekte gibt es vorausschauend zu bedenken. Ziel bei der Konzeptionierung von (teil-)automatisiertem Fahren für das Militär ist eine »meaningful human control«, der Mensch bleibt also, wie immer bei Fraunhofer FKIE, im Loop und letztendlich auch in der Verantwortung. Voraussetzung dafür sind Handlungsfähigkeit auf der einen und ein ausreichendes Situationsverständnis auf der anderen Seite. Wichtig ist dies insbesondere dann, wenn das automatisierte Fahrzeug etwa ein Schützen- oder Kampfpanzer, also mit Waffen ausgestattet ist.

Auch sind inzwischen Multiplattform-Konzepte denkbar, also eine Vernetzung und gemeinsame Steuerung von Fahrzeugen, darunter auch z. B. Unmanned Ground Vehicles (UGVs). Dies erfordert eine Datenanbindung der einzelnen Fahrzeuge, damit diese unter Umständen auch aus der Ferne gesteuert werden können. Hier sind einerseits sichere Kommunikationsverbindungen notwendig und andererseits entsprechende Schnittstellen zu berücksichtigen, die Interoperabilität gewährleisten. Dies erhöht die Komplexität des Systems um einen weiteren Faktor, da neben Automation und Fahrer auch ein möglicher Operateur, der das Fahrzeug aus der Ferne steuert, ins System integriert werden muss.

An dieser Stelle kommt der Aspekt der »Cybersicherheit« ins Spiel. Auch dahingehend müssen derartige automatisierte Systeme selbstverständlich besonders robust ausgelegt sein. Dies gilt gleichermaßen für den zivilen Bereich des automatisierten Fahrens: Denn auch dort muss sichergestellt sein, dass die immer stärker vernetzten bis hin zu automatisiert fahrenden Autos vor Cyber-Angriffen gefeit sind.

KONTAKT
Marcel Baltzer
Telefon +49 228 9435-594
marcel.baltzer@fkie.fraunhofer.de

INTERNATIONALE STANDARDISIERUNGSARBEIT

Interoperabilitätsstandard für militärische Fahrzeuge

Das Szenario: Der Ernstfall ist eingetreten. Die Streitkräfte der NATO-Staaten – etwa die 2015 für diesen Ernstfall aufgestellte Very High Readiness Joint Task Force (VJTF) – müssen einem Bündnispartner beistehen. Soldaten verschiedener Nationen sind Seite an Seite im Einsatz, sie tauschen Informationen aus und auch die Fahrzeuge und die darin verbauten Komponenten sind in den Informationsverbund integriert. Voraussetzung hierfür ist etwas, das man auf den ersten Blick allerdings nicht sehen kann: ein Standard, der sicherstellt, dass all diese Einzelteile interoperabel sind, also »miteinander sprechen« können. Ein derartiger Standard mit dem Fokus auf Landfahrzeuge wird am Fraunhofer FKIE in der Abteilung »Informationstechnik für Führungssysteme« erarbeitet. Projektleiter Dr. Daniel Ota hat einen Einblick gegeben, was genau dahinter steckt.

Seit 2011 entwickelt Fraunhofer FKIE mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) und der Wehrtechnischen Dienststelle für landgebundene Fahrzeugsysteme, Pionier- und Truppentechnik (WTD 41) den Standard für die NATO Generic Vehicle Architecture, kurz NGVA. Ein solcher Standard ist notwendig, um zu gewährleisten, dass alle militärischen Landfahrzeuge und die einzelnen darin verbauten Komponenten wie beispielsweise Laserentfernungsmesser, Videokameras oder Führungsinformationssysteme interoperabel sind. Dies ist deswegen wichtig, weil die Fahrzeuge und Geräte in aller Regel nicht von ein und demselben Produzenten stammen, sondern vielmehr von unterschiedlichen Zulieferern.

Internationale Zusammenarbeit

»Standardisierung beinhaltet viel Gremienarbeit, im Falle von NATO-Standards natürlich auf internationaler Ebene«, bringt Ota seinen Alltag bei der Erarbeitung von NGVA auf den Punkt. Er selbst leitet hierfür u. a. zwei NGVA-Arbeitsgruppen. »Wir arbeiten dabei eng mit Frankreich, den Niederlanden und Großbritannien zusammen, aber auch mit Australien und Kanada. Nächste Woche treffen wir uns zum Beispiel in den Niederlanden, danach richten wir selbst ein Meeting aus, wahrscheinlich in Bonn«, beschreibt Ota die agile Zusammenarbeit. Aktuell wird die zweite Version des Standards erarbeitet. Sie ist ein Update der ersten Version, die im Februar 2018 ratifiziert wurde. Die neue Version wird um zusätzliche Funktionalitäten erweitert, insbesondere um den Aspekt der Cybersicherheit. Geplant ist, die Arbeiten hierzu Anfang 2020 abzuschließen und ebenfalls bei der NATO zur Ratifizierung einzureichen.

Der Standard besteht aus Anforderungen an die Stromversorgung einerseits und an den elektronischen Datenaustausch andererseits. Teil dessen ist ein Datenmodell, das in Form von UML-Diagrammen (**U**nified **M**odelling **L**anguage) spezifiziert wird. Ein weiterer Aspekt ist die Betriebssicherheit (Safety) von Fahrzeugen. Schließlich legt der Standard auch ein Verifikationsverfahren fest.

Simulation zum Testen von Komponenten

Das Fraunhofer FKIE betreibt ein Testlabor, in dem der Standard implementiert ist. Hier können ein Fahrzeug und die gewünschten Komponenten simuliert, aber auch echte Hardware eingebunden werden, etwa eine Videokamera. Simuliert und getestet werden dann der Nachrichtenaustausch und das Verhalten der Komponenten. Das Datenmodell, das den nach NGVA standardisierten Informationsaustausch beschreibt, muss bei der Prüfung korrekt implementiert sein, soll die jeweilige Komponente den Test bestehen. Die Hersteller von Subsystemen können im FKIE-Testlabor testen lassen, ob ihre Systeme auch tatsächlich interoperabel sind. Eine zweite Version dieses Testlabors ist bei der WTD 41 aufgebaut worden, sodass die dortige Prüfstelle diese Tests auch selbst durchführen kann.

»Spannend wird es, wenn das erste Fahrzeug in Betrieb genommen wird, das ab der ersten Designphase auf den NGVA-Standard aufbaut«, konstatiert Ota. Dies wird schon bald der Fall sein: Aktuell befindet sich ein entsprechendes Fahrzeug in der Beschaffung durch OCCAR, die europäische Beschaffungsorganisation. Funktioniert alles perfekt, wird der Mehrwert für den Beschaffungsprozess und bei der zukünftigen Kampfwertsteigerung hoch sein.

KONTAKT
Dr. Daniel Ota
Telefon +49 228 9435-732
daniel.ota@fkie.fraunhofer.de

MEILENSTEINE

KARRIEREWEGE

Förderung mit Blick auf den Einzelnen

Die Entwicklungsmöglichkeiten am Fraunhofer FKIE, das seinen Mitarbeitenden ein so hohes Maß an Gestaltungsspielraum bietet, sind vielfältig. Nicht nur, was Themen wie Führung und Management angeht, sondern dank einer eigenen Personalentwicklung auch im Hinblick auf hochspezifische, wissenschaftlich-fachliche Weiterentwicklung. Das umfangreiche Förderangebot beinhaltet neben Einzelschulungen wie »Machine Learning, Tensor Flow« auch ein breites Spektrum an Formaten wie Seminarreihen und Förderprogramme, die Kollaboration und Vernetzung systematisch unterstützen.

»Willkommen« für neue Mitarbeitende

Doch bevor die Mitarbeitenden an ihre Weiterentwicklung denken können, müssen sie erst einmal »richtig« am Institut ankommen. So veranstaltete das Fraunhofer FKIE Anfang 2019 erstmalig für alle neuen Mitarbeitenden einen Welcome Day, um sie »an Bord zu holen« und ihnen Orientierung zu geben – mit kleinen Hilfen für den Joballtag an einem Forschungsinstitut, aber auch mit einem Rundumblick auf das große Ganze. Und mit vielen Möglichkeiten, die neuen Kolleginnen und Kollegen kennenzulernen.

Aus diesem Anlass präsentierte Institutsleiter Professor Peter Martini zunächst die Strukturen der Fraunhofer-Gesellschaft, um dann »unser FKIE« vorzustellen. »Denn wir sind ein ganz besonderes, ein richtig starkes Institut«, so der Institutsleiter. Mit Blick auf das Mission Statement »Wir arbeiten jeden Tag daran, die Welt sicherer zu machen.« betonte Martini: »Wir tragen alle zu unserer Mission bei, die Kollegen aus der Wissenschaft, aus der Technik und aus der Verwaltung.«

Organisiert wurde das abwechslungsreiche Programm durch die FKIE-eigene Personalentwicklung, durch die die Durchführung institutsspezifischer Formate und bedarfsorientierte Weiterbildung ermöglicht werden. So gab es während der Welcome-Veranstaltung nicht nur Infostände, an denen es Gelegenheit gab, sich über verschiedene Ansprechpartner, relevante Abläufe und das breite wissenschaftliche Spektrum zu informieren. Auch erhielten die Teilnehmer bei einem Rundgang durch das Institut spannende Einblicke in aktuelle Forschungsprojekte. Stationen waren zum Beispiel die Robotikhalle, die Operationszentrale der Zukunft, der Fahrsimulator, das Usability-Labor und die Postergalerie der Sensordatenfusion. Und weil ein Tag allein nicht ausreicht, um das »Mitmachinstitut« mit all seinen Facetten kennenzulernen, schloss sich eine dreiteilige Workshop-Reihe an den Welcome Day zu den Themen »Administration und Organisation«, »Wissenschaftliche Praxis« und »Projektmanagement und -durchführung« an.

Ausrichtung auf mehr Agilität und Individualität

Die Welcome-Reihe ist Teil eines breiten Angebotes, das von institutsspezifischen Qualifizierungen über interne Seminarreihen bis hin zu hochkarätigen Programmen der Fraunhofer-Gesellschaft und vielen weiteren Formaten wie Mentoring oder Coaching reicht. Voraussetzung dafür sind u. a. eine individuelle Entwicklungsplanung und eine kontinuierliche Begleitung. Der strategische Ausbau individualisierter Qualifizierung und Förderung ist eingebettet in die Institutsstrategie 2024. Nachhaltige Personalentwicklung berücksichtigt Rahmenbedingungen der modernen Arbeitswelt ebenso wie die des sich rasch ändernden Wissenschaftsumfeldes und setzt daher zunehmend auf selbstorganisiertes, kollaboratives und arbeitsplatznahes Lernen. Die Zusammenarbeit in Projekten ist vielfach von Agilität geprägt, und so setzt auch Fraunhofer FKIE zunehmend auf temporäre Verantwortung, persönliche Initiative und flexible Strukturen. Daher gibt es am Institut keine starr definierten Karrierepfade. Vielmehr werden persönliche Entwicklungswege gefördert und u. a. durch die passende Kombination von Qualifizierungen nach »Baukastenprinzip« sowie durch die Teilnahme an Seminarreihen oder Förderprogrammen unterstützt.

Dazu gehören etwa »TALENTA«, die »Advanced Management Class« oder das Prädikatsprogramm »Fraunhofer Forschungsmanager«. Diese sind als besonderer Benefit für einzelne Mitarbeiterinnen und Mitarbeiter vorgesehen. Die Nominierung erfolgt auf Vorschlag der Institutsleitung bei der Fraunhofer-Gesellschaft.

TALENTA

»Fraunhofer TALENTA« ist ein gezieltes und ganzheitliches Förderprogramm für Wissenschaftlerinnen, das in drei Programmlinien TALENTA *start*, TALENTA *speed up* und TALENTA *excellence* auf den unterschiedlichen Ebenen der Karriereentwicklung ansetzt. Jede der Programmlinien hat eine Laufzeit von zwei Jahren und beinhaltet die Unterstützung bei der Schärfung des eigenen Karriereziels, Budget für Weiterbildung sowie ein Zeitkontingent für die eigene Entwicklung.

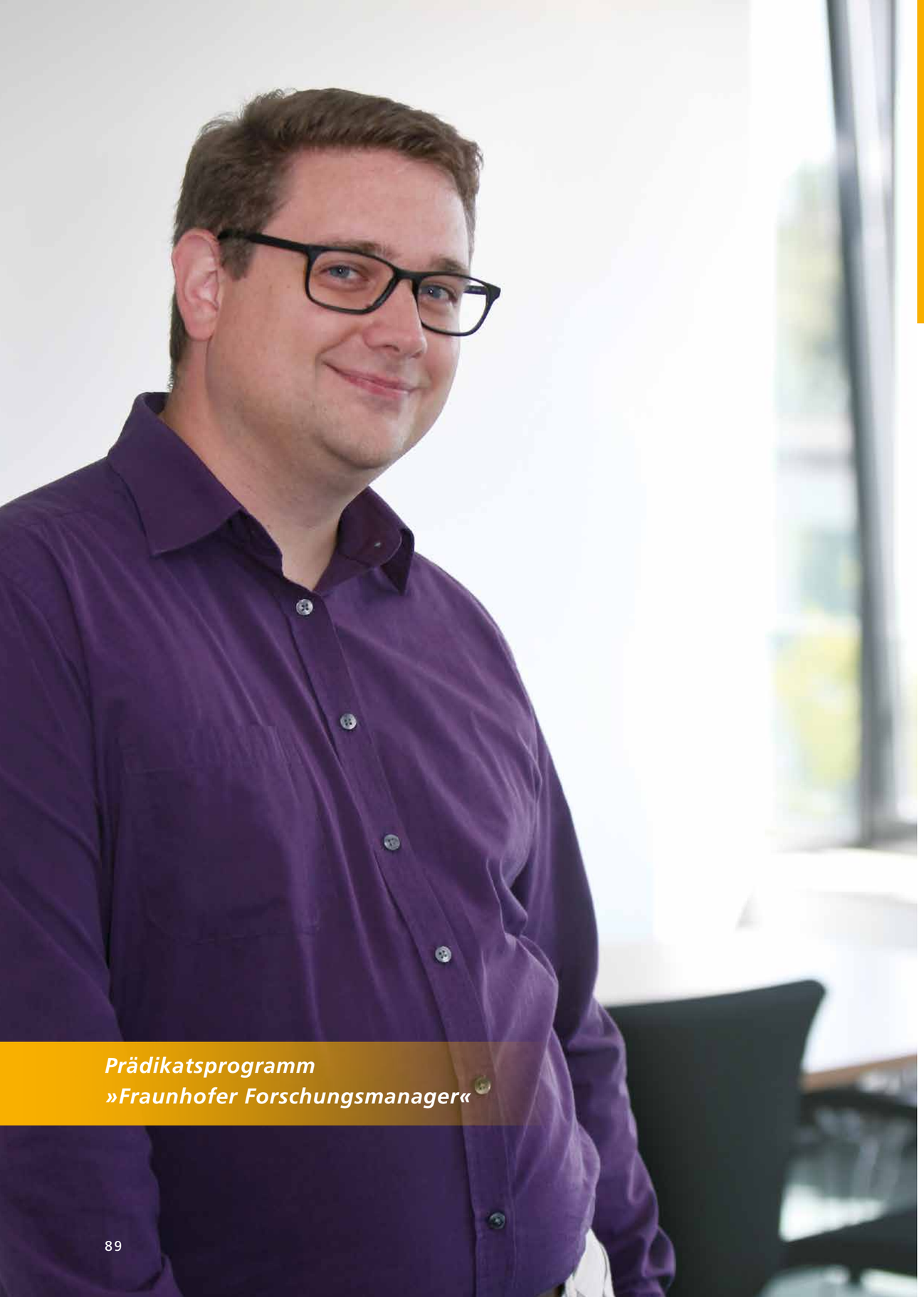
Advanced Management Class

Die zwei Jahre dauernde »Advanced Management Class« richtet sich inhaltlich auf die Bereiche Management, Leadership und Selbststeuerung aus und legt einen besonderen Fokus auf Vernetzung. Im Zentrum des Programms steht die individuelle Entwicklung von erfahrenen Führungskräften sowie Leistungsträgerinnen und -trägern. Die Programmelemente, beispielsweise Seminare, Projektarbeit, Peergroup-Sessions und Coaching, bilden dabei den thematischen Rahmen, der Raum für die Ausgestaltung und Bearbeitung von spezifischen und individuellen Fragestellungen bietet.

Prädikatsprogramm Fraunhofer-Forschungsmanager/in

Das Prädikatsprogramm ist ein institutsübergreifendes Qualifizierungsangebot, das sich an Leistungsträger und -trägerinnen mit erster Führungserfahrung oder mit strategischer Verantwortung beispielsweise im Bereich Business Development richtet. Es setzt an den konkreten Herausforderungen der Institute an und ermöglicht den Teilnehmenden durch seine hohe Praxisrelevanz eine besondere Handlungsfähigkeit an der Schnittstelle zwischen Wissenschaft und Wirtschaft.

KONTAKT
Dr. Eva Kneise
Telefon +49 228 9435-113
eva.kneise@fkie.fraunhofer.de



Prädikatsprogramm »Fraunhofer Forschungsmanager«

Peter Weidenbach

»Karriere ist wie eine Autofahrt«

Als Peter Weidenbach im März 2019 offiziell zum Forschungsgruppenleiter in der Abteilung »Cyber Analysis & Defense« (CA&D) ernannt wurde, bedankte sich der 35-Jährige bei Abteilungsleiter Dr. Elmar Padilla und Kollegen mit einer kurzen, fröhlichen Rede. Seine Karriere verglich er darin mit einer Autofahrt: »Manchmal ist man auf dem richtigen Weg, manchmal verfährt man sich. Manchmal gibt es Baustellen, manchmal auch Straßensperren.« Der 35-jährige Diplom-Informatiker hat in seiner Zeit am FKIE alles erlebt und lobt: »Wurde es schwierig, war ich nie allein.«

Netzwerke, Kryptographie und IT-Security waren die Themen, die Peter Weidenbach schon während seines Informatikstudiums an der Uni Bonn am meisten interessierten. Diesem Schwerpunkt ist er bis heute treu geblieben – mit Erfolg: »Applied System Analysis« ist der Name der neu ernannten Forschungsgruppe, in der aktuell sechs Wissenschaftler und fünf studentische Hilfskräfte unter seiner Anleitung mitarbeiten. Im Kern ihrer Forschungsarbeit steht die automatisierte Schwachstellensuche in Software, mit besonderem Fokus auf Firmware.

Immer auf der Suche nach Sicherheitslücken

So konnten Weidenbach und sein Team eine gefährliche Schwachstelle in Netzwerkdruckern aufdecken, die angesichts ihres großen Risikopotenzials auf breites öffentliches Interesse stieß. Im Dezember 2017 stellte der Netzwerkspezialist sie erstmalig im Rahmen der Cyber Defence Conference in Bonn vor. Die Darlegung seiner so spannenden wie erschreckenden Erkenntnisse schaffte es daraufhin direkt zu umfassender Berichterstattung bei heise online. »Da war ich schon stolz«, gibt der gebürtige Bonner zu.

Angelockt vom guten Arbeitsklima

Am Fraunhofer FKIE schätzt Weidenbach vor allem die großen Freiheitsgrade bei der Arbeit, aber auch die gute Stimmung im Team, die sehr freundschaftlich, fast familiär sei. Das habe er schon während seiner Diplomarbeit gespürt, bei der er vom Institut betreut wurde. Nach dem Uniabschluss war für ihn klar, dass er bleiben möchte.

Jetzt ist Weidenbach selbst Forschungsgruppenleiter und gibt seinem eigenen Team mit auf den Weg: »Wir Führungskräfte sind euer Navigationssystem. Doch wie beim Auto funktioniert das Navi nur, wenn ihr ihm auch kommuniziert, wohin ihr wollt – welche Pläne, Ziele, Wünsche ihr habt. Nur so können wir euch auf eurem Weg unterstützen.« Das FKIE ist dankbar für den talentierten Wissenschaftler und schlug ihn für das Prädikatsprogramm »Fraunhofer Forschungsmanager« vor. An diesem nimmt Weidenbach seit April 2019 teil.

»Advanced Management Class«

Dr. Michael Gerz

»Man gewinnt einen Blick auf das große Ganze«

Es ist schon eine besondere Ehre für die »Advanced Management Class« der Fraunhofer-Gesellschaft ausgewählt zu werden. Auf den Vorschlag der eigenen Institutsleitung folgt ein komplexes Bewerbungs- und Auswahlverfahren für das begehrte Karriereprogramm. Dr. Michael Gerz vom Fraunhofer FKIE gehört zu den 19 Teilnehmern – und ist damit Teil einer gemeinsamen Mission.

»Die Entwicklung und Qualifizierung von Führungskräften in strategischen Schlüsselfunktionen« hat sich die Advanced Management Class (AMC) zum Ziel gesetzt. Mit dem neu gegründeten Förderprogramm will die Fraunhofer-Gesellschaft Leistungsträger mit Führungsverantwortung, die in ihren Bereichen auch strategische Ziele verfolgen, auf ihrem Karriereweg unterstützen. Zwei Jahre dauert das Programm, das sich über vier Qualifizierungsmodule erstreckt und Themen wie »Strategisches Management«, »Leadership« und »Organisationsdesign« umfasst. Zum Thema »Change Management« haben die AMC-Teilnehmer z. B. die Einführung einer neuen Software in einem Unternehmen durchgespielt. Gerz: »Dabei muss man nicht nur mit der Geschäftsleitung an einem Strang ziehen, sondern auch soziale Netze jenseits der Führungshierarchien nutzen, um alle Mitarbeiter rasch für eine neue Idee zu gewinnen.«

Vernetzung mit Führungskräften

Den Abschluss bildet das Modul »Selbstmanagement«, in dem neben Resilienz und Stressmanagement auch das 360-Grad-Feedback eine wichtige Rolle spielt. Hier steht dann jeder Teilnehmer mit seiner Persönlichkeit im Mittelpunkt und erhält passgenaue Unterstützungsvorschläge für die individuelle und berufliche Entwicklung.

Aber es ist nicht nur die persönliche Weiterbildung, die für Dr. Gerz den besonderen Reiz dieses Führungsprogramms ausmacht. Auch die Vernetzung mit anderen Führungskräften ebenso wie mit Stakeholdern der Fraunhofer-Gesellschaft gehört dazu. »Man gewinnt einen neuen Blick auf das große Ganze.« Auch wenn man Teil der Fraunhofer-Gesellschaft sei, blicke man durch den intensiven Austausch untereinander doch gewissermaßen von außen auf bestehende Strukturen und Strategien. Aufgefrischt und geschult werde auch der Blick auf das eigene Institut. »Insbesondere im Modul »Strategisches Management« wurden Problemstellungen an konkreten Beispielen durchdekliniert und analysiert. Hier sieht man, wie in anderen Instituten gedacht wird, worauf der Fokus liegt und welche Optionen den Mitarbeitern zur Verfügung stehen. Gleichzeitig erkennt man auch, welche Chancen und Freiheiten das Fraunhofer FKIE bietet.«

Denn das eigene Institut kennt Dr. Michael Gerz bereits aus der Zeit, bevor sich das FKIE 2009 der Fraunhofer-Gesellschaft angeschlossen hat. Seit 2004 ist der Informatiker als Mitarbeiter in der Abteilung »Informationstechnik für Führungssysteme« tätig. Er leitet die Forschungsgruppe »Interoperability & Testing« und vertritt das Fraunhofer FKIE in verschiedenen NATO-Arbeitsgruppen.

»Fraunhofer TALENTA«

Dr. Jessica Schwarz

Den Kurs auf Führungs-verantwortung gesetzt

Das Team von Dr. Jessica Schwarz besteht aktuell aus sechs Mitarbeitern. Erst kürzlich ist es durch die Zusammenführung der Abteilungen MMS und HF um drei wissenschaftliche Mitarbeiter und eine studentische Hilfskraft gewachsen. »Das muss sich jetzt erst einmal einspielen,« stellt Schwarz fest. Eine Aufgabe, die bewältigt werden muss. Dabei hilft ihr die TALENTA-Förderung, die sie einerseits für ihre Entwicklung hin zur Führungskraft nutzen möchte und andererseits für den Ausbau ihres Forschungsthemas. Ihre Promotion konnte sie dank der Förderung schon erfolgreich abschließen.

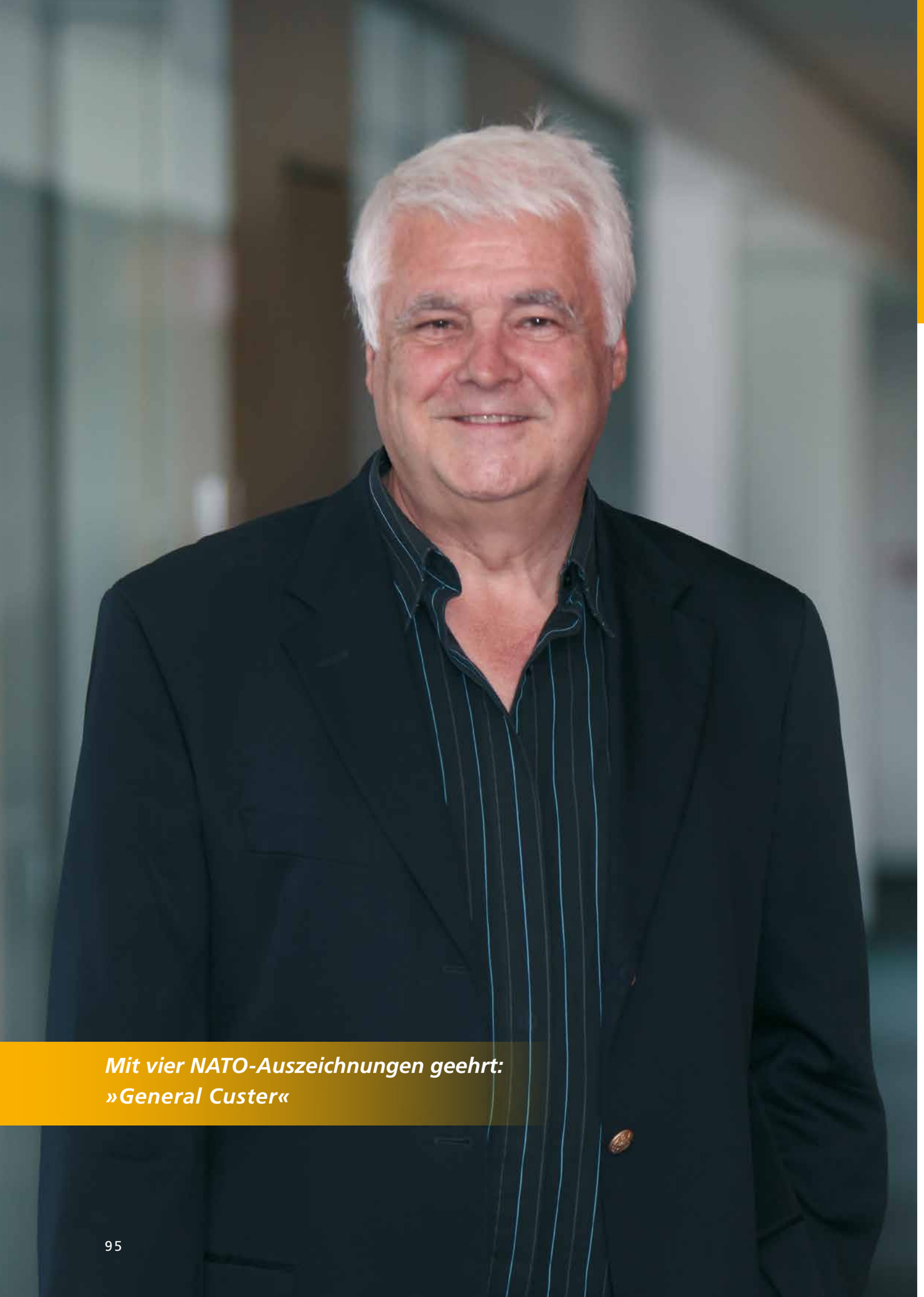
Im Bereich Mensch-Maschine-Systeme würde sie arbeiten, soviel stand für Jessica Schwarz schon während ihres Studiums der Psychologie an der Universität Koblenz-Landau fest, das sie 2008 beendete. Schnell nach ihrem Einstieg bei einem Industrieunternehmen wurde ihr klar: »Das Thema war das richtige, aber ich wollte lieber forschen.« So nahm sie im April 2009 eine Stelle am FKIE an, das damals noch Teil der FGAN war und sich kurze Zeit später der Fraunhofer-Gesellschaft anschließen sollte.

Einstieg in die Forschung

Richtig los ging dann alles mit dem Projekt KOBE, in dem ein Konzept zur Multitouch-Bedienung für die Lagebeurteilung und Luftzielerfassung entwickelt wurde. Schwarz eigener Schwerpunkt lag dabei auf der Evaluation und Bewertung des Konzepts. Ab 2013 folgten die Vorhaben AMISTAD, AMIGOS und ARAMIS, die sie zusammen mit ihrem Kollegen Sven Fuchs bearbeitete. Eine glückliche Fügung, wie Schwarz im Rückblick findet: Ergänzen sich doch die jeweiligen Forschungsschwerpunkte gut und ließen sich zudem im Rahmen einer jeweiligen Promotion vertiefen. Schwarz hat hierfür erforscht, wie sich die Zustände der Nutzer, die an einem System arbeiten, erfassen lassen, also ob der Nutzer z. B. ermüdet, gestresst oder abgelenkt ist. Währenddessen beschäftigt Fuchs sich damit, welche Adaptierungsstrategien seitens des technischen Systems zur Verfügung stehen, um den Nutzer bestmöglich zu unterstützen.

Ausbau des eigenen Thema

Im Rahmen von TALENTA möchte Schwarz ihr Thema »Empirische Systembewertung und Nutzerzustandserfassung« weiter ausbauen und daher weitere Projekte akquirieren. Potenzial hat das Thema allemal, kann es doch domänenübergreifend für die Gestaltung adaptiver Systeme aber auch bei Usability-Untersuchungen eingesetzt werden. Schwarz bringt es auf den Punkt: »Insbesondere bei sicherheitskritischen Aufgaben ist es wichtig, technische Systeme so zu gestalten, dass der menschliche Operateur optimal in seiner Tätigkeit unterstützt wird. Die Erfassung des Nutzerzustands kann hier einen entscheidenden Mehrwert bieten, zum Beispiel um zu bestimmen, wann und welche Art von Unterstützung der Mensch benötigt, um seine Aufgaben sicher und effizient zu bewältigen.«



Mit vier NATO-Auszeichnungen geehrt: »General Custer«

Jürgen Kaster

40 Jahre Forschung für Frieden und Sicherheit

Dass er als Zivilist in einigen NATO-Kreisen respektvoll »General Custer« genannt wird, beweist: FKIE-Wissenschaftler Jürgen Kaster hat sich mit seiner langjährigen, herausragenden Forschung für die militärische Lagebearbeitung und Lagedarstellung großen Respekt erarbeitet – und das sowohl auf nationaler wie auch auf internationaler Ebene. Für seine Verdienste erhielt er im Jahr 2018 mehrere hochkarätige NATO-Auszeichnungen. Eine große Ehre für Kaster, der seit diesem Jahr eigentlich den wohlverdienten Ruhestand antreten könnte, sich jedoch aus Leidenschaft für seine Arbeit dazu entschlossen hat, noch länger am Fraunhofer FKIE zu bleiben.

Direkt nach der Uni ging es damals los: »Nur einen Tag nach der Beendigung meines Studiums der Elektrotechnik an der RWTH Aachen habe ich in Wachtberg meine Stelle am damaligen Forschungsinstitut für Anthropotechnik angetreten«, erinnert sich Kaster zurück. Aus einer Vertretungsstelle für einen Mitarbeiter, der für drei Jahre an die NATO »ausgeliehen« wurde, sind 40 Jahre geworden. Vieles hat sich in dieser Zeit immer wieder geändert: Institutsnamen und -zuordnungen, Institutsleiter, Kolleginnen und Kollegen, die kamen und gingen. »Eins ist jedoch stets geblieben«, verrät der Wissenschaftler, »ich bin jeden Tag, und ich meine damit wirklich jeden Tag, gerne zum Institut gekommen.«

Die Gründe dafür waren vielschichtig. Kaster: »Für mich persönlich war und ist der individuelle Freiraum am wichtigsten, der die Forschungsarbeit an unserem Institut charakterisiert. Die Möglichkeit zur Selbstverwirklichung – wenn auch natürlich in einem gesetzten Rahmen – ist für mich eine unbezahlbare Qualität, die ich in meiner Laufbahn immer wieder sehr intensiv und motivierend erlebt habe. Genauso wie die vielfältigen – auch internationalen – Kontakte, die man im Rahmen der Arbeit knüpft.«

Spannender Forschungsmix

Begonnen hat für ihn alles mit Grundlagenforschung in der Ergonomie. »Meine berufliche Laufbahn gliedert sich exakt in zwei Hälften, die sich synergetisch ergänzt haben: Auf 20 Jahre Grundlagenforschung in der Ergonomie folgte die Ausrichtung verstärkt hin zu anwendungsorientierter Forschung, die dann im Jahr 2009 mit der Eingliederung des FKIE in die Fraunhofer-Gesellschaft offizieller Schwerpunkt wurde.« Für Kaster eine positive Entwicklung. Nach den vielen Jahren des klassisch wissenschaftlichen Alltags geprägt von Experimenten, Veröffentlichungen, Vorträgen und Konferenzen, also letztlich mit Aktivitäten vorwiegend innerhalb der Scientific Community, stand nun die direkte Rückkopplung mit Anwendern und die hautnahe Erfahrung des praktischen Einsatzes der entwickelten Konzepte und Demonstratoren im Mittelpunkt.

Fokus auf militärische Lagebearbeitung

Dabei blieb Kaster einem Themenbereich von Beginn seiner Laufbahn an treu: der militärischen Lagebearbeitung und -darstellung. Im Laufe von vier Jahrzehnten verschaffte er sich ein umfassendes und einzigartiges Experten-

wissen, das ihm große Achtung bei Bundeswehr- und NATO-Partnern einbrachte. So arbeitete er bereits 1993 an der Ausstattung des Bundeswehr-Lagezentrums in der Somalia-Krise mit sowie in den Folgejahren an der Lagebearbeitung der NATO-Schutztruppen SFOR und KFOR. Die 20 Jahre in der Ergonomie-Forschung betrachtete Kaster dabei immer als Schlüssel zu den späteren Erfolgen: »Denn hier haben wir grundlegend gelernt, auch hochkomplexe Anwendungen intuitiv bedienbar zu machen.«

Persönlichkeitsprägende Reisen

Die beste Lösung für eine Aufgabe zu finden, ist nur möglich, wenn die realen Rahmenbedingungen, unter denen sie später eingesetzt wird, bekannt sind: »Nur wer den wirklichen Bedarf der Zielgruppe genau kennt, kann adäquate Lösungskonzepte anbieten. Waren es über viele Jahre spannende Reisen zu wissenschaftlichen Konferenzen, so waren es später meine für einen Wissenschaftler eher untypischen Dienstreisen in Krisenregionen wie den Balkan und Afghanistan, die ich nicht missen möchte.«

Warum? Dazu fällt Kaster zuerst ein (Nicht-IT)-Beispiel ein: »In Kabul haben wir uns gewundert, warum Wasserflaschen oftmals nicht im Schatten, sondern in Fensternischen und damit in der prallen Sonne gestapelt wurden. Irgendwann haben wir gefragt. Die Antwort: Weil gefüllte Wasserflaschen ein guter Splitterschutz sind. Nach nur 14 Tagen in Kabul bist du ein anderer Mensch.« Will sagen: In einem Einsatzland gelten völlig andere Rahmenbedingungen als zu Hause auf der grünen Wiese. Das Beispiel ist direkt auf Führungsinformationssysteme übertragbar: Nur wer den wirklichen Bedarf genau kennt, ist in der Lage, aufgabenangepasste, kompetenzförderliche Lösungen zu erarbeiten. »Mit diesem Grundverständnis haben wir viele Projekte erfolgreich bearbeiten können«, so Kaster.

Gefragt nach einem Moment, der ihm in besonderer Erinnerung geblieben ist, muss Kaster nicht lange überlegen: »Das war ebenfalls in Kabul. Die Bundeswehr hatte seinerzeit die Leitung der Kabul Multinational Brigade (KMNB) übernommen und wir haben die Aufklärungszentrale vor Ort mit ausgeplant. Unser Beitrag war ein Auswertesystem, das wir im Camp Warehouse in einer 14-tägigen Gewaltaktion bei bis zu 52 Grad Mittagshitze und zirka drei Stunden Schlaf pro Nacht einrichteten. Als sich einige Zeit darauf ein schreckliches Attentat ereignete, war laut Erfahrungsbericht der deutsche Kommandeur der am besten informierte Entscheidungsträger in Kabul. Dank unserer Wissensdatenbank!«

Was wünscht er sich für die Zukunft!? »Erfolgreiche Software-Entwicklung ist hochdynamisch und agil. Die größte Herausforderung ist es, Anwendungslösungen zeitnah und sachgerecht an die Truppe heranzutragen. Im Sinne der Soldaten im Einsatz sind effizientere Beschaffungsverfahren dringend notwendig.«

VITA

1975	Studium der Elektrotechnik / RWTH Aachen
1980	Start als wissenschaftlicher Mitarbeiter am Forschungsinstitut für Anthropotechnik (FAT)
1992	Kommissarische Leitung der Abteilung »Anzeige« am FAT
2002	Stellvertretende Leitung der Abteilung »Informationstechnik für Führungssysteme« (ITF) und Leitung der Forschungsgruppe »Wissens- und Workflow-Management«
seit 2009	Leitung der ITF-Forschungsgruppe »Kollaborationsprozesse« am Fraunhofer FKIE

Franziska Schmidt

Vom Girls'Day zur Wissenschaftlerin

Franziska Schmidt weiß, was sie will. Und das schon von frühester Kindheit an. Beim Girl'sDay 2005 nahm die damals 14-Jährige mit fünf Mädchen an dem Workshop »Wir erstellen eine Webseite« am Fraunhofer FKIE teil. Weichenstellung nennt man solche Ereignisse in der Rückschau: Neben Schule und Studium blieb sie dem FKIE treu. Heute arbeitet die Informatikerin in der Abteilung »Informationstechnik für Führungssysteme« (ITF).

Aber nicht nur der Girls'Day brachte die gebürtige Bonnerin zum FKIE. »Richtig guter Informatik-Unterricht an der Schule« hat sie dazu motiviert, sich intensiv mit Computern zu beschäftigen, sich früh einen eigenen Laptop zu wünschen. Dafür ist sie ihrem ehemaligen Lehrer bis heute dankbar. Die Frage nach dem Schülerpraktikum kurz vor der Oberstufe stellte sich ihr gar nicht: Ihr war klar, dass sie zum FKIE wollte. Bei Annette Kaster, heute Leiterin der Abteilung »Mensch-Maschine-Systeme«, erlebte sie erstmals den Arbeitsalltag am Institut, nahm an Besprechungen mit externen Partnern teil und fühlte sich von Beginn an als Teil des Teams.

Den entscheidenden Tipp fürs Studienfach erhielt sie ebenfalls während ihres Praktikums: Medieninformatik sollte es werden. Zum Glück in Köln, keine weite Entfernung zum Fraunhofer FKIE also. Ihre Bewerbung für ein weiteres Praktikum kam so gut an, dass ihr direkt eine Stelle als studentische Hilfskraft angeboten wurde und auch die Bachelorarbeit betreute ein FKIE-Wissenschaftler. Nach dem Studium folgte dann 2018 für Franziska Schmidt die Festanstellung in der ITF-Forschungsgruppe »Interoperability & Testing». Allerdings soll auch der Master in ihrem Lebenslauf nicht fehlen. Den macht sie zurzeit, indem sie berufsbegleitend den internationalen Studiengang »Webscience« an der TH Köln studiert. Zwei Mal pro Woche betritt sie nach ihrer Forschungsarbeit den virtuellen Hörsaal und belegt die Online-Vorlesungen von 19 bis 22 Uhr. Die Begeisterung für ihr Fach und ihren Job sind Franziska Schmidt anzumerken und das bei jeder Karrierestufe. Echter Fraunhofer FKIE-Spirit!

Franziska Schmidt arbeitet seit 2018 für die Abteilung ITF.

PROMOTIONEN

Zeichen der engen Zusammenarbeit mit verschiedenen Universitäten und Fachhochschulen sind vierzehn erfolgreich abgeschlossene Promotionen am Fraunhofer FKIE. In dem so umfangreichen und komplexen Projektgeschäft wie dem des Fraunhofer FKIE sind sie keine Selbstverständlichkeit und verlangen einen hohen persönlichen Einsatz aller Beteiligten, Betreuern, Doktorvätern und -müttern und natürlich den Promovenden selbst. Umso mehr freut sich das ganze Institut mit, wenn es wieder heißt: **»Habemus doctorem!«**

PROMOTIONEN

THOMAS BARABOSCH
»Formalization and Detection of Host-Based Code Injection Attacks in the Context of Malware«
Rheinische Friedrich-Wilhelms-Universität Bonn

CHRISTIAN STEFFES
»Exploiting Structural Signal Information in Passive Emitter Localization«
Rheinische Friedrich-Wilhelms-Universität Bonn

HENNING PERL
»Big Data and Security - Three Case Studies«
Rheinische Friedrich-Wilhelms-Universität Bonn

KHALED YAKDAN
»A Human-Centric Approach for Binary Code Decompilation«
Rheinische Friedrich-Wilhelms-Universität Bonn

ULRICH ENGEL
»Development and Analysis of an Anti-Jam Preprocessor for Satellite Navigation Receivers«
Universität Siegen

DANIEL BENDER
»Airborne Navigation by Fusing Inertial and Camera Data«
Rheinische Friedrich-Wilhelms-Universität Bonn

MICHAEL FELDMANN
»Tracking von Objektgruppen und ausgedehnten Zielobjekten«
Karlsruher Institut für Technologie KIT

JULIAN HÖRST
»Performance Analysis of Bearings-only Tracking Problems for Maneuvering Target and Heterogeneous Sensor Applications«
Rheinische Friedrich-Wilhelms-Universität Bonn

ALTAMASH KHAN
»Nonlinear Filtering based on Log-homotopy Particle Flow – Methodological Clarification and Numerical Evaluation«
Rheinische Friedrich-Wilhelms-Universität Bonn

DANIEL OTA
»Early De-Risking of Land Vehicles Open System Architecture Implementations«
University of Brighton

JESSICA CONRADI
»Ergonomische Gestaltung adaptierbarer Mensch-Computer-Interfaces für die Interaktion beim Gehen«
Rheinisch-Westfälische Technische Hochschule Aachen

JESSICA SCHWARZ
»Multifaktorielle Echtzeitdiagnose des Nutzerzustands in adaptiver Mensch-Maschine-Interaktion«
Technische Universität Dortmund

PREISE UND AUSZEICHNUNGEN

Für ihre herausragenden Forschungsergebnisse und ihr außerordentliches Engagement wurden wieder zahlreiche FKIE-Mitarbeiterinnen und -Mitarbeiter national wie auch international ausgezeichnet. Neben verschiedenen Förderpreisen, die an ganz junge Wissenschaftler verliehen wurden, standen aber auch besondere Lebensleistungen im Fokus der Ehrungen. Sowohl die wissenschaftliche Community als auch Industrie, NATO und Bundeswehr würdigten die Forschungsleistungen des Fraunhofer FKIE vielfach. **#Wirsindstolz!**

BEST PAPER AWARD DFRWS 2017
für das Team Daniel Plohmann, Martin Lambertz und Jan-Niclas Hilgert

SILVIA CORADESCHI ROBOCUP AWARD 2018
für Padmaja Kulkarni

BEST PAPER AWARD DER ICMCIS 2018
für das Team Anne Diefenbach,
Roberto Rigolin Ferreira Lopes und anderen

YOUNG SCIENTIST BEST PAPER AWARD DER ICMCIS 2018
für Souradip Saha

TECHNOLOGY OF THE YEAR AWARD 2018
für Dr. Marc Adrat

AFCEA-STUDIENPREIS 2018
Platz 1 für Kevin Wilkinghoff
Platz 2 für Hans Schily

HENSOLDT-FÖRDERPREIS 2018
für Hans Schily und Katharina Klein

NATO SCIENTIFIC ACHIEVEMENT AWARDS 2018
für Christoph Barz, Norman Jansen und Albert Pritzkau

AOC AWARD 2018
für Hans Peter Stuch

Stand 09/2017 - 09/2019

GOOGLE SECURITY AND PRIVACY RESEARCH AWARD 2018
für Prof. Dr. Matthew Smith

VDI-FÖRDERPREIS 2018
für Kevin Wilkinghoff

BEST CREATIVE SOLUTION ELROB 2018
für das FKIE-Robotik-Team

NATO-AUSZEICHNUNGEN 2018
für Jürgen Kaster
- »15 Jahre NATO Allied Command Transformation«
- CWIX Coin
- ****-Medaille »Deputy Supreme Allied Command Transformation Nielson«
- Commander's Coin of Excellence

HACKATHON-SIEG DER SAFETY DAYS 2019
für Manas Pradhan

BEST PAPER AWARD DFRWS 2018
für Martin Lambertz und Jan-Niclas Hilgert

ENRICH 2019 KATEGORIE »SEARCH & RESCUE«
Platz 1 für das FKIE-Robotik-Team

AFCEA-STUDIENPREIS 2019
Platz 1 für Christopher Krah
Platz 2 für Padmaja Kulkarni

NATO SET PANEL EXCELLENCE AWARD 2019
für Dr. Alexander Charlish

DFRWS FORENSIC RODEO (DFRWS USA) 2019
Platz 1 für Jan-Niclas Hilgert und Martin Lambertz

SONDERWERTUNG FORENSIK DER NATO-ÜBUNG LOCKED SHIELDS 2019
Platz 1 für Daniel Plohmann und das Bundeswehr-Team

VERANSTALTUNGEN

Externe Messen, strategische Treffen, Besuche, Teilnahme an Konferenzen wie auch Präsentationstermine bei Kunden – sind für die Arbeit des Fraunhofer FKIE besonders wichtig.

Sie dienen dem fachlichen Austausch mit Partnern und Anwendern sowie der Vernetzung in der wissenschaftlichen Community. Einige der FKIE-Veranstaltungshighlights der Jahre 2018 und 2019 sind auf den innenliegenden Seiten zusammengestellt.

2018

Zukunftsarbeit für die Marine

Wie kann die Unterstützung für die Marine seitens des Fraunhofer FKIE aussehen? Und was hat das Institut hierfür eventuell längst in seinem Portfolio? Diese Fragen standen im Mai 2018 im Mittelpunkt eines dreitägigen Expertenaustauschs zwischen dem Marineunterstützungskommando II und der FKIE-Forschungsgruppe »Leitzentralen und Entscheidungsunterstützung« von Oliver Witt. Schon ab der ersten Minute herrschten rege Diskussionen und direkt ging es in die Detailarbeit: Studienergebnisse wurden diskutiert, Schwachstellen analysiert und Unterstützungsfunktionalitäten dokumentiert. Die Ergebnisse fasste Fregattenkapitän Ralf Henning zusammen: »Ein Zeichen dafür, wie wichtig ein solcher Austausch ist und wie viel wir voneinander lernen und profitieren werden.«

15. Mai 2018
Marineunterstützungskommando zu Besuch am Fraunhofer FKIE

01
24. Januar 2018
Besuch Kommando Sanitätsdienste der Bundeswehr

02
28. Februar 2018
Tag der Industrie

03
09. März 2018
Präsentation der NATO-Aktivitäten

04
11. / 12. April 2018
AFCEA-Fachaustellung

05

06
09. Juni 2018
Tag der Bundeswehr

26. / 27. Juni 2018
DWT-Forum »Digitalisierung der Landstreitkräfte«

07

08
29. August 2018
FKIE-Technologieforum 2018

09
09. - 11. Oktober 2018
12. SDF Symposium

10
14. November 2018
AFCEA Zukunfts- und Technologieforum

26. November 2018
Unterzeichnung des Kooperationsvertrags mit dem Kommando CIR

11
09. November 2018
Gründung des Cyber Security Clusters Bonn

Festakt im Alten Rathaus Bonn

Durch die zahlreichen und dicht angesiedelten Player ist Bonn längst das Kompetenzzentrum Europas für Cyber Security: BSI, KdoCIR, Bundespolizei, Deutsche Telekom – und eben auch das Fraunhofer FKIE. Dieses Pfund soll künftig noch stärker ausgespielt und Kompetenzen, Netzwerke und High-End-Technologien aus Wirtschaft, Politik und Forschung zusammengeführt werden. So wurde am 9. November 2018 im Alten Rathaus das Cyber Security Cluster Bonn (CSCB) gegründet. Fraunhofer FKIE ist Gründungsmitglied und stellt mit Institutsleiter Prof. Dr. Peter Martini den zweiten Vorsitzenden. Bonn hat ein besonderes Alleinstellungsmerkmal und steht im Bereich Cyber Security für Höchstsicherheit, betonte auch Fraunhofer-Präsident Professor Reimund Neugebauer, der der persönlichen Einladung von Professor Martini nach Bonn gefolgt war.

12
11. / 12. Dezember 2018
SGW-Konferenz Informationstechnik

2019

Innovative Technologien für Aufklärung und Führung

»Smarte Führungsunterstützung im 21. Jahrhundert« lautete das Thema der 33. AFCEA-Fachausstellung, die vom 10. bis 11. April 2019 im Bonner Hotel Maritim stattfand. Daran angeschlossen war ein Symposium mit Fachvorträgen, darunter auch die Vorstellung des neu gegründeten Cyber Security Clusters Bonn durch FKIE-Institutsleiter und stellvertretenden Cluster-Vorsitzenden Prof. Dr. Peter Martini. Passend zum Ausstellungsthema zeigte das Fraunhofer FKIE innovative Technologien, beispielsweise den Prototyp eines skalierbaren, resilienten, interoperablen und adaptierbaren Führungsinformationssystems. Weiterhin wurden ein mobiles System zur Schussdetektion sowie ein bereits mehrfach prämiertes Verfahren zur Sprechererkennung in Audiodaten vorgestellt.

10. / 11. April 2019
AFCEA-Fachausstellung

01
08. Januar 2019
Besuch der Bonner Polizeipräsidentin Ursula Brohl-Sowa

02

03
13. / 14. März 2019
Cyber Security Tech Summit Europe

04
10. April 2019
Verbundtreffen A-DRZ

23. / 24. April 2019
Counter-UAS Symposium

05

06

07
01. - 05. Juli 2019
EnRicH The European Robotics Hackathon

Roboter übten für den nuklearen Ernstfall

Atomarer Störfall im österreichischen Atomkraftwerk Zwentendorf – zum Glück nur ein Szenario beim »2nd European Robotics Hackathon (EnRicH) 2019«, bei dem zehn internationale Teams eine Woche lang den Ernstfall probten. »EnRicH ist der einzige Wettbewerb in Europa, bei dem mit echter Strahlung geübt wird. Hier zeigt sich, was die europäische Robotik im Fall der Fälle leisten kann«, machte General Michael Janisch, Leiter des Amtes für Rüstung und Wehrtechnik (ARWT) des österreichischen Heeres, bei der Eröffnung deutlich. Gemeinsam mit dem Fraunhofer FKIE organisierte sein Amt den Wettbewerb zum zweiten Mal. So war es möglich, dass die den Teilnehmern gestellten Szenarien durch echte radioaktive Strahlungsquellen und den einzigartigen Veranstaltungsort maximal realitätsnah waren.

08
27. / 28. August 2019
DWT-Forum »Bundeswehrlogistik«

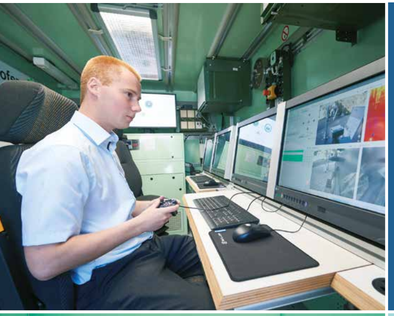
09

10
10. Oktober 2019
Karrieretag Bonn

11
21. / 22. November 2019
Futuras in Res

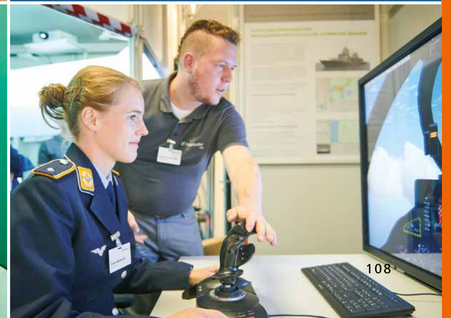
13. / 14. November 2019
Strategie-Audit

12
10. / 11. Dezember 2019
Cyber Defence Conference



Besucherrekord beim FKIE-Technologieforum 2018

Mit 300 Besuchern konnte das FKIE-Technologieforum einen neuen Rekord vermelden. Die geladenen Gäste erhielten exklusive Einblicke in die aktuellsten und spannendsten Forschungsergebnisse am Fraunhofer FKIE: Anhand von 30 Exponaten inklusive Live-Vorführungen und Fachvorträgen präsentierten die FKIE-Mitarbeiter u. a. Virtual Reality für Unbemannte Systeme, ein Lagezentrum der zivil-militärischen Zusammenarbeit , ein automatisiertes Tool zur Social-Media-Beobachtung oder auch KI-Methoden für die Funkaufklärung.



FKIE VERNETZT

KOMMANDO CYBER- UND INFORMATIONSRAUM
KURATORIUM UND KOOPERATIONEN

KOMMANDO CYBER- UND INFORMATIONSRAUM

Ein neues Bündnis für mehr IT-Sicherheit

Die enge Zusammenarbeit zwischen dem Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr und dem Fraunhofer FKIE steht auf einem neuen Fundament: Generalmajor Jürgen Setzer, Stellvertretender Inspekteur Kommando Cyber- und Informationsraum, und Institutsleiter Professor Peter Martini unterzeichneten im November 2018 einen Vertrag, um im Bereich Cybersicherheit künftig noch enger zu kooperieren.

Bei der stetig wachsenden Bedrohung durch Hacker-Angriffe in allen Bereichen wird deutlich, dass künftig nur eine gemeinsame und gesamtstaatliche Strategie eine Cybersicherheit in Deutschland auf hohem Niveau gewährleisten kann. Vor diesem Hintergrund findet vor allem durch einen intensiven, regelmäßigen Erfahrungsaustausch und gegenseitige Hospitationen ein Wissenstransfer statt, von dem die Mitarbeiterinnen und Mitarbeiter des KdoCIR wie auch die des Fraunhofer FKIE profitieren.

»Die Bundeswehr und das FKIE verbindet eine langjährige, vertrauensvolle Zusammenarbeit. Unser Institut leistet mit seinen anwendungsorientierten Forschungsarbeiten einen wichtigen Beitrag zur Sicherung der Systeme und Netze der Bundeswehr. Der Kooperationsvertrag schafft zusätzliche Möglichkeiten, speziell im Bereich Cybersicherheit auch andere, neue Wege zu gehen«, betonte Professor Martini. So werden beispielsweise im Bereich der IT-Forensik Übungen mit gemischten Teams durchgeführt mit dem Ziel, aktuelle Gefahrenlagen, Bedrohungsszenarien, Angriffswerkzeuge und Tätergruppen zu identifizieren und zu analysieren.

Auch aus Sicht von Generalmajor Setzer wird mit der Kooperation ein bedeutender Mehrwert erzielt. »Cybersicherheit kommt eine zentrale Bedeutung in unserer zunehmend digitalisierten Welt zu. Angriffe auf das weitreichende, vernetzte IT-System der Bundeswehr erfolgen täglich und erfordern eine kontinuierliche Härtung unseres Netzes einschließlich der Netzwerkzugänge. Das Fraunhofer FKIE ist auf diesen Feldern einer der Taktgeber in punkto Erforschung sicherer, virtueller Datenwelten und -wege. Mit unserer Zusammenarbeitsvereinbarung gehen wir einen wegweisenden Schritt, Sicherheitsrisiken einzudämmen und künftigen Bedrohungen zu begegnen.«

Das Kommando Cyber- und Informationsraum

Ihm sind direkt das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr und das Zentrum für Geoinformationswesen der Bundeswehr unterstellt. Rund 13.500 Dienstposten gehören zum Cyber- und Informationsraum, dem jüngsten Organisationsbereich der Bundeswehr. Ähnlich wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft und See zuständig sind, sind diese für die Dimension Cyber- und Informationsraum verantwortlich und stellen den Betrieb und Schutz der IT-Systeme der Bundeswehr, sowohl im Inland als auch im Einsatz, sicher. Weiterhin stärken sie Fähigkeiten zur Aufklärung und Wirkung im CIR und entwickeln diese weiter.

Generalmajor Jürgen Setzer und Prof. Dr. Peter Martini bei der feierlichen Unterzeichnung des Kooperationsvertrages am 26. November 2018.

KURATORIUM UND KOOPERATIONEN

KURATORIUM

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

Victoria Appelbe
Amt für Wirtschaftsförderung, Bonn

Ralf Brümmer
Securitas GmbH, Berlin

GenMaj Dr. Michael Färber
BMVg – Bundesministerium der Verteidigung, Bonn

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

Andreas Könen
BMI – Bundesministerium des Innern, für Bau und Heimat, Berlin

BrigGen Jens-Olaf Koltermann
BMVg – Bundesministerium der Verteidigung, Berlin

Dr. Mathias Pauli
ROHDE & SCHWARZ GmbH & Co. KG, München

Prof. Dr. Delphine Reinhardt
Georg-August-Universität Göttingen

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

Thomas Tschersich
T-Systems International GmbH, Bonn

Joost Verton
Airbus Defence and Space GmbH, Taufkirchen

MR Norbert Michael Weber
BMVg – Bundesministerium der Verteidigung, Bonn

Prof. Dr. Klaus Wehrle
Rheinisch-Westfälische Technische Hochschule Aachen

Dr. Thomas Weise
Rheinmetall AG, Düsseldorf

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

KOOPERATIONEN

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

FRAUNHOFER-ALLIANZEN
Big Data
Space
Embedded Systems

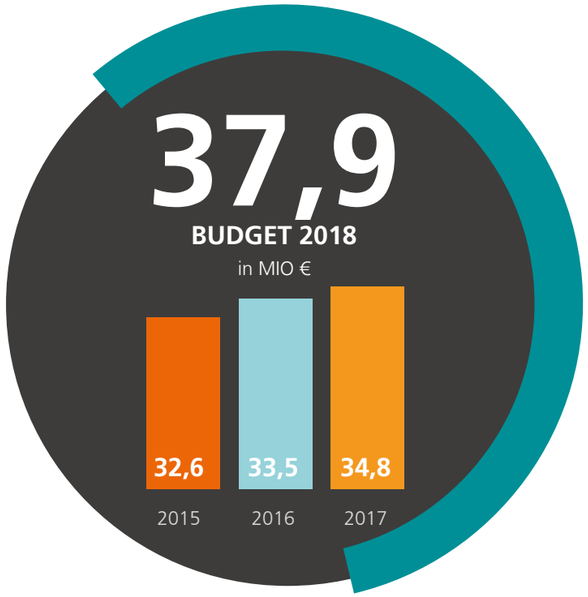
UNIVERSITÄTSKOOPERATIONEN
Rheinische Friedrich-Wilhelms-Universität Bonn
Rheinisch-Westfälische Technische Hochschule Aachen
Hochschule Bonn-Rhein-Sieg

PARTNER
Allianz für Cybersicherheit
Cyber Security Cluster Bonn
Kommando CIR (KdoCIR)

Stand 10/2019

SERVICE

ZAHLEN UND FAKTEN

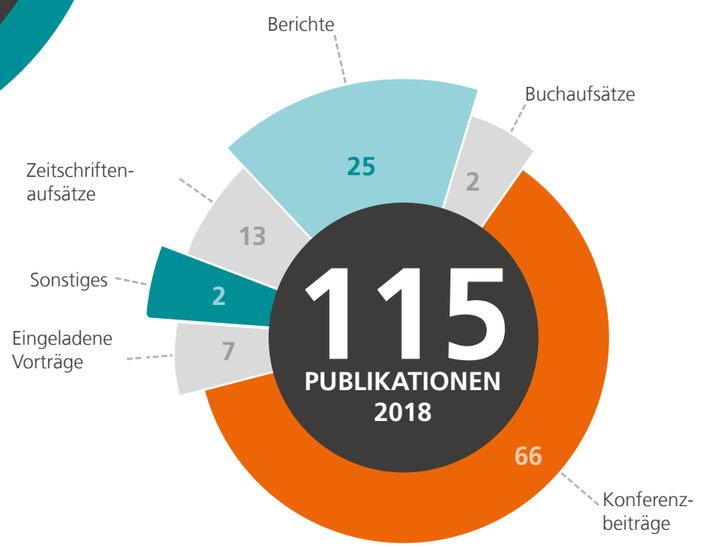


88 BETREUTE ABSCHLUSSARBEITEN 2018

48 Bachelor
33 Master
7 Promotion

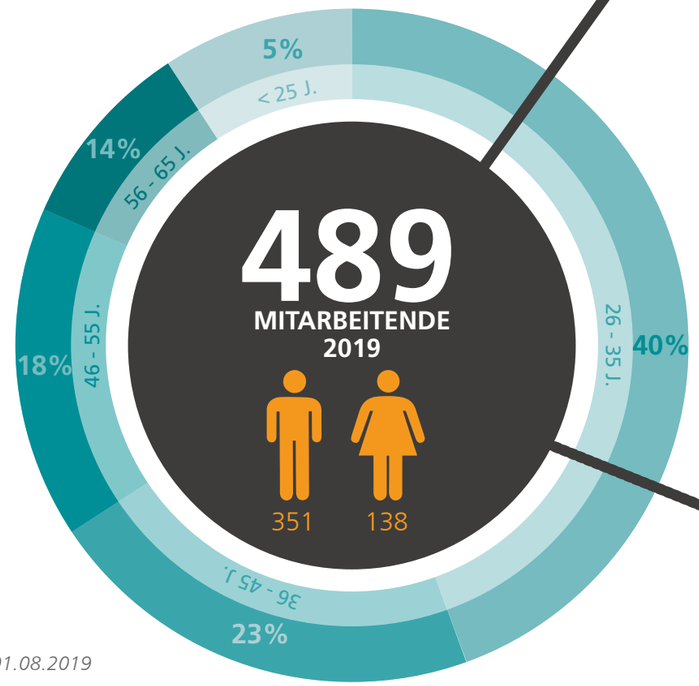
STUDIENRICHTUNGEN (HÄUFIGSTE)

- Informatik
- Elektro- und Informationstechnik
- Ingenieurwesen
- Mathematik
- Psychologie
- Physik und Astronomie



87 LEHR-VERANSTALTUNGEN

47 SoSe 2018
40 WiSe 2018/19



25 NATIONALITÄTEN

SOCIAL MEDIA
Stand 31.10.2019

LINKEDIN 1053
TWITTER 1718

Stand 01.08.2019

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 72 Institute und Forschungseinrichtungen. Mehr als 26 600 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 2,6 Milliarden Euro. Davon fallen 2,2 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Rund 70 Prozent dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Rund 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 Januar 2019
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, Christina Haberland, Silke Wiesemann

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

LAYOUT I SATZ I FOTOMONTAGE
Petra Kaiser, Daphne Siegel

BILDQUELLEN
Bilder © Fraunhofer FKIE

Wachtberg-Werthhoven, November 2019

AUSNAHMEN
Cover NicoElNino / iStock®
Seite 9 iloveotto + somartin / 123RF® Montage
Seite 11 Uwe Bellhäuser / das bilderwerk
Seite 13 Hans-Jürgen Vollrath / Ahr-Foto
Seite 26 BBK
Seite 27 gyn9037 / 123RF®
Seite 30 Jan-Otto, sorapop / iStock®, 123RF® Montage
Seite 31 mcjantree / 123RF®
Seite 34 ipopba / 123RF®
Seite 35 D-Keine / iStock®
Seite 38 Fabian Vogl
Seite 39 freedomnaruk / 123RF®
Seite 42 Yuri_Arcurs / iStock® Montage
Seite 45 Uwe Bellhäuser / das bilderwerk
Seite 48 oticki / 123RF®
Seite 50 stockbrocker / 123RF® Montage
Seite 52 hxdbzxy / 123RF®
Seite 53 Uwe Bellhäuser / das bilderwerk
Seite 56 przemekklos / 123RF®
Seite 58 rawpixel / 123RF®
Seite 60 pwstudio / 123RF®
Seite 61 Uwe Bellhäuser / das bilderwerk
Seite 66 WTD 91
Seite 69 mf-guddyx / iStock®
Seite 72 Denys Yelmanov / iStock®
Seite 74 Tryaging, s-cphoto / iStock® Montage
Seite 76 iStock® / Montage - Volker Kurzidim
Seite 80 fouroaks / 123RF® Montage
Seite 84 akiyoko / 123RF®
Seite 99-102 dervish37 / 123RF®
Seite 103/108 Volker Lannert
Seite 104 scusi / 123RF®
Seite 112 fotosamui / 123RF®
Seite 113 Tawng / 123RF®