Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

JAHRESBERICHT 12/13

VORWORT

Sehr geehrte Leserin, sehr geehrter Leser,

das Jahr 2012 stand für uns im Zeichen einer anregenden Diskussion von Aspekten der Sicherheit im virtuellen und öffentlichen Raum: Was ist unsere Verantwortung für die Gewährleistung von Sicherheit und wie können wir dieser Verantwortung gerecht werden? Diese Fragen und mögliche Antworten darauf motivierten die Fraunhofer-Sicherheitskonferenz »Future Security«, die im Herbst 2012 von uns ausgerichtet erstmals in Bonn stattfand.

Weil sich Technologien entwickeln und unsere Gesellschaft im stetigen Wandel ist, müssen »Sicherheit« und »Gefahr« immer wieder neu definiert werden. Mit der Future Security haben wir Entscheidungsträgern aus Ministerien und Behörden, Wissenschaft und Industrie ein Forum für die Diskussion von neuen Technologien und vielfältigen Aspekten des Themas Sicherheit gegeben. Die erfreuliche Zahl von 360 Besuchern aus aller Welt bestätigt die Bedeutung des Themas Sicherheit für Forschung, Politik, Wirtschaft und Gesellschaft – für uns alle.

In diesem Jahresbericht möchten wir Ihnen ausgewählte neue und bestehende Projekte und Kooperationen vorstellen. 2012 starteten das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Schadsoftware-Analysten des FKIE das Projekt »Systematische Analyse von Botnetzen«, das die zehn gefährlichsten Botnetze untersuchen und Gegenmaßnahmen entwickeln soll. Weitere Themen sind erfolgversprechende Technologien zur akustischen Detektion von Schallquellen und ein neuer Ansatz für die Umsetzung robuster Kommunikationsnetze. Hier soll erstmals Peer-to-Peer-Technologie in den NATO-Standard für Netzwerke integriert werden.

In der Forschung für Verteidigung, Sicherheit und Krisenreaktion war und ist das Fraunhofer FKIE ein starker und verlässlicher Partner für die Bundeswehr, für die Polizei, für zivile Sicherheitseinrichtungen und für Betreiber kritischer Infrastrukturen. Dem Bundesministerium der Verteidigung sowie dessen nachgeordneten Behörden standen wir unverändert als unabhängiger und kompetenter Berater und Dienstleister zur Verfügung. Darüber hinaus steigerte sich im vergangenen Jahr erneut das Auftragsvolumen in der zivilen Vertragsforschung gegenüber dem Vorjahr und übertraf unsere Erwartungen deutlich.

Wir möchten an dieser Stelle wieder unseren Mitarbeiterinnen und Mitarbeitern danken: Ihr Engagement und ihre Leistungen sind die Basis für den erfolgreichen Verlauf unserer Projekte und Grundlage für die Anerkennung, die wir in der Wissenschaft, bei Auftraggebern und Partnern genießen.

Prof. Dr. Peter Martini
Institutsleiter

Prof. Dr. Christopher Schlick
Stellv. Institutsleiter

INHALTSVERZEICHNIS

INHALT

6 Rückblick 2012/2013: Auf Wachstumskurs
8 Abteilungen und Forschungsgruppen
12 Ansprechpartner im Fraunhofer FKIE

14 SENSORDATEN- UND INFORMATIONSFUSION / SDF

14 Kombinierte Sensorik
18 Der Fall mit dem Knall
20 Geruchsexplosion
24 Testflüge in der Gänsebucht

28 KOMMUNIKATIONSSYSTEME / KOM

28 Die Masse macht´s
30 Mut zur Lücke
32 Geräusche intelligent erkennen
36 Kommunizieren im Konvoi

38 INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME / ITF

38 Baum der Erkenntnis
40 Feldtest im Testbett

42 ERGONOMIE UND MENSCH-MASCHINE-SYSTEME / EMS

42 Forscher auf großer Fahrt
48 Mit Smartphone auf Patrouille

54 UNBEMANNTE SYSTEME / US

54 Wärme weist den Weg
56 Routenplanung für Roboter

60 CYBER DEFENSE / CD

60 Routingpolizei im Rechner
62 Quarantäne für digitale Quälgeister

66 FUTURE SECURITY / KURATORIUM / GESELLSCHAFT

66 Future Security 2012: Zukunft - Sicherheit - Bonn
70 Das Kuratorium
72 Standorte der Fraunhofer-Gesellschaft

74 ANHANG / STATISTIK

74 Wissenschaftliche Berichte
76 Ausgewählte Veröffentlichungen
82 Ausgewählte Tätigkeiten in Gremien
86 Impressum

AUF WACHSTUMSKURS

2012 war für das Fraunhofer FKIE ein sehr erfolgreiches Jahr – sowohl die wissenschaftlichen Arbeiten als auch die wirtschaftliche Entwicklung waren exzellent. Zudem wurden wichtige Weichen gestellt, um das Institut als Arbeitgeber noch attraktiver zu machen.

Es war ein Sprung ins kalte Wasser – verbunden mit einem großen Versprechen: 2009, als die Integration der drei FGAN-Institute in die Fraunhofer-Gesellschaft beschlossen wurde, erstellte das Fraunhofer FKIE einen Finanzplan bis 2014. Er sah vor, die Umsätze aus der Vertragsforschung auf knapp 2,7 Millionen Euro zu steigern. Langfristig sollten die Erträge aus zivilen Projekten etwa 30 Prozent und damit eine Marke erreichen, die auch andere Institute der Fraunhofer-Gesellschaft erzielen. Noch einmal zur Erinnerung: 2010, mit dem Start des Fraunhofer FKIE als Fraunhofer-Institut, lag dieser Umsatz bei einem Bruchteil.

Ziele übertroffen

Die Pläne von damals hat das Institut ohne Beeinträchtigung seiner Aufgaben gegenüber dem Verteidigungsministerium bei weitem übererfüllt. 2012 hat sich der Anteil der Vertragsforschung über Erwarten erhöht. Der positive Trend dürfte sich 2013 fortsetzen. Mehr Arbeit kann das Institut nur bewältigen, wenn auch die Zahl der Mitarbeiterinnen und Mitarbeiter zunimmt. Hier haben wir in den letzten Jahren ein Wachstum mit Augenmaß verfolgt. 360 Männer und Frauen arbeiteten 2012 am Fraunhofer FKIE.

Mehr Frauen zu Fraunhofer

Noch nicht zufrieden sind wir mit dem Geschlechterverhältnis. In allen wissenschaftlichen Abteilungen sind mehr Männer als Frauen beschäftigt. Zwar ist der Frauenanteil für ein Institut mit naturwissenschaftlich-technischen Themen relativ hoch, dennoch möchte das Institut den Frauenanteil steigern. Dazu engagiert sich das FKIE in Programmen, die jungen Frauen MINT-Studienfächer nahe bringen. Ein Beispiel ist der Girls'Day am 26. April 2012, zu dem das Institut bereits zum neunten Mal seine Pforten für Schülerinnen öffnete. Oder die Wissenschaftsnacht: Gemeinsam mit den Kollegen von Fraunhofer-IAIS, -SCAI und -INT haben wir uns auf dem Münsterplatz in Bonn präsentiert. Das Fraunhofer FKIE zeigte Exponate, wie man Angriffe aus dem Internet abwehrt und wie man Personen an ihrer Sprache erkennt.

Eine enorme Aufmerksamkeit auch in der breiten Öffentlichkeit erzielte die Konferenz »Future Security« Anfang September in Bonn, über die viele Medien berichteten. Das Institut konnte sich hier als führende Forschungseinrichtung für Sicherheitsthemen, insbesondere für Cyber-Security, präsentieren (siehe Seite 66).

Work-Life-Balance wird wichtiger

Wir wissen, dass hochqualifizierte Personen heute großen Wert auf die Work-Life-Balance legen, wenn sie sich für einen Arbeitgeber entscheiden. Die Fraunhofer-Gesellschaft liegt in Rankings der beliebtesten Arbeitgeber für Ingenieure regelmäßig in den Top-Ten. Auf diesen Lorbeeren dürfen wir uns nicht ausruhen. Deshalb begrüßt das FKIE neben der Vermittlung von Kinderbetreuungsplätzen das Programm »Eldercare« der Fraunhofer-Gesellschaft, das Mitarbeiterinnen und Mitarbeitern mit pflegebedürftigen Angehörigen Unterstützung bei der Organisation von Betreuungsmöglichkeiten bietet.

Zwei Berufungen, vier Promotionen

Im Jahresbericht 2011 hatten wir es schon verkündet: Dr. Michael Meier hat einen Ruf als Professor für IT-Sicherheit am Institut für Informatik der Universität Bonn erhalten. Prof. Meier hat den Ruf angenommen und wurde vom Rektor der Universität am 27. April 2012 offiziell zum »Universitätsprofessor der Universität Bonn am FKIE« ernannt. Seine Antrittsvorlesung hielt Meier am 5. Dezember 2012 zum Thema »Architektur, Technologien und Herausforderungen des IT-Frühwarnsystems AMSEL«. Mit Michael Meier stärkt das FKIE seine gute Zusammenarbeit mit der Universität und baut seine Aktivitäten in der Analyse und Bekämpfung von Cyber-Kriminalität weiter aus.

Ebenfalls zum Professor berufen wurde Nils Aschenbruck, der seit dem 1. März 2012 mit seinem Arbeitsgebiet »Verteilte Systeme« die Informatik der Universität Oldenburg verstärkt. Auch Aschenbruck ist ein ausgewiesener Experte in Sachen IT-Sicherheit und Cyber-Defense.

Die wachsende Bedeutung des Themas IT-Sicherheit spiegelt sich auch in den Promotionen des vergangenen Jahres wider. Zwei erfolgreiche Promotionen – von Elmar Gerhards-Padilla und von Felix Leder – beschäftigen sich mit der Erkennung von Routingangriffen beziehungsweise der Klassifikation von Schadsoftware. Auch die anderen Abteilungen vermeldeten erfolgreiche Promotionen: von Martina Brötje und Felix Govaers. Herzlichen Glückwunsch!

Das Fraunhofer FKIE im Profil

Das Fraunhofer FKIE forscht für die Bundeswehr, zivile Sicherheitsbehörden und die Industrie. Informationen gewinnen, übertragen, verarbeiten, darstellen und schützen – dies sind die Kernaufgaben des Instituts. Führungsinformationssysteme, die ein exaktes Lagebild erstellen, Assistenzsysteme, die komplexe Informationen und Kontextwissen verknüpfen und sichtbar machen, oder Verfahren der Augmented Reality sind nur einige Beispiele, wie das Institut die schnelle und sichere Kommunikation zwischen Mensch und Technik fördert. Im Mittelpunkt der Arbeiten stehen immer die Anforderungen des Kunden, Ziel jedes Projekts ist die praktische Umsetzung.

Wichtigster Denk- und Lösungspartner des Fraunhofer FKIE ist das Bundesministerium für Verteidigung, das auch für die Grundfinanzierung des Instituts sorgt. Das Institut kooperiert mit zahlreichen nationalen und internationalen Forschungseinrichtungen, Universitäten und industriellen Partnern und ist eingebunden in die Forschungsorganisationen der NATO und der Europäischen Union. An den beiden Standorten des Fraunhofer FKIE in Wachtberg und Bonn arbeiten 360 Mitarbeiterinnen und Mitarbeiter. Der Etat im Jahr 2012 betrug cirka 26 Millionen Euro.

ABTEILUNGEN UND FORSCHUNGSGRUPPEN

SENSORDATEN- UND INFORMATIONSFUSION / SDF

Herr der Lage mit mehr Wissen

Der Mensch verarbeitet Sinneseindrücke und leitet daraus Handlungen ab. Doch unsere Sinne reichen nicht immer aus, etwa wenn es darum geht, Sicherheitsrisiken zu erkennen. Hier helfen Sensoren und Aufklärungssysteme: Sie beschaffen Daten und Informationen und verdichten diese automatisch zu einem Lagebild. Sie erleichtern so Entscheidungen in komplexen Situationen. Die Abteilung entwickelt für militärische und zivile Auftraggeber Methoden der Informationsfusion, von theoretischen Konzepten über Simulationen bis zum Entwurf von Prototypen.

KOMMUNIKATIONSSYSTEME / KOM

Robuster Informationsaustausch

Eine reibungslose Kommunikation kann in Krisensituationen Menschenleben retten. Deshalb müssen Kommunikationssysteme auch dann noch arbeiten, wenn Teile einer Kommunikationsinfrastruktur zusammengebrochen sind, wenn die Teilnehmer mobil sind oder wenn sie Geräte mit unterschiedlichen Standards nutzen. Die Abteilung arbeitet für militärische Auftraggeber an Konzepten für einen robusten Datenaustausch – von den physikalischen Eigenschaften der Funkwellenausbreitung bis zum Netzmanagement. Immer im Blick: Die Praxistauglichkeit nach den Wünschen des Kunden.

INFORMATIONSTECHNIK FÜR FÜHRUNGSSYSTEME / ITF

Immer im Bilde

Wer gemeinsam handeln will, braucht einheitliche Informationen. Der Austausch von Daten und Lagebildern über die Grenzen von Technik, Sprache und Raum hinweg ist deshalb essentiell für effektives Handeln in sicherheitskritischen Situationen. Die Abteilung unterstützt die Bundeswehr und ihre internationalen Partner bei der Konzeption und der Erprobung von Führungsinformationssystemen aus einem Guss, die Missverständnisse vermeiden und die sich flexibel an neue Situationen anpassen lassen.

ERGONOMIE UND MENSCH-MASCHINE-SYSTEME / EMS

Der Mensch im Mittelpunkt

Technischer Fortschritt ist kein Selbstzweck – er muss immer dem Menschen nutzen. Hier setzt die Abteilung an: Sie entwickelt intuitive Mensch-Maschine-Schnittstellen für Kommunikations- und Führungssysteme, die sich auch in Gefahren- und Stresssituationen – etwa bei militärischen Einsätzen – noch intuitiv bedienen lassen. So werden komplexe Lagebilder und Führungsprozesse für den Menschen transparent. Die Experten nutzen dazu virtuelle Simulation und Augmented Reality, also die Anreicherung der Realität um Zusatzinformationen, sowie innovative Verfahren zur Telekooperation. Die Betrachtung von Mensch und Technik als Einheit und die Zusammenführung in einem flexiblen Mensch-Maschine-System gewährleistet die effektive Interaktion der Akteure.

UNBEMANNTE SYSTEME / US

Der verlängerte Arm des Menschen

Sie inspizieren havarierte Kernkraftwerke oder spüren Verschüttete nach einem Erdbeben auf: Immer häufiger gehen Roboter dorthin, wo es für Menschen zu gefährlich ist. Heute werden solche Roboter noch ferngesteuert, doch künftig sollen sie teilweise autonom agieren. Dazu entwickelt die Forschungsgruppe Assistenzsoftware, die Sensordaten auswertet und Bewegungen steuert – für einzelne Roboter, aber auch für Szenarien, wo mehrere Roboter gemeinsam eine Aufgabe bewältigen müssen. Ziel ist dabei immer die Entlastung des Operateurs, der dadurch Freiraum für komplexe Entscheidungen bekommt.

CYBER DEFENSE / CD

Schutz vor Attacken aus dem Cyber Space

Sie sind die Seuche des 21. Jahrhunderts: Viren, Trojaner und Botnetze, mit denen Kriminelle fremde Rechner kapern und ausspionieren und sogar ganze Industrieanlagen lahmlegen. Die Forschungsgruppe Cyber Defense arbeitet an Verteidigungsstrategien. Sie hat dazu ein Labor eingerichtet, in dem sie digitale Schädlinge anlockt, untersucht und unschädlich macht. Außerdem beraten die Experten Behörden, Bundeswehr und Unternehmen, wie sie sich gegen Cyberattacken schützen.

ANSPRECHPARTNER IM FRAUNHOFER FKIE

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

Sensordaten- und Informationsfusion

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

- Datenfusion für Array-Sensoren
- Ortung und Navigation
- Weitbereichsüberwachung

Kommunikationssysteme

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

- Aufklärung und Störung
- Software Defined Radio
- Robuste heterogene Netze

Cyber Defense

Forschungsgruppenleiter
Dr. Jens Tölle
Telefon 0228 9435-513
jens.toelle@fkie.fraunhofer.de

Forschungsgruppenleiter
Prof. Dr. Michael Meier
Telefon 0228 7354-249
michael.meier@fkie.fraunhofer.de

Stellv. Institutsleiter
Prof. Dr. Christopher Schlick
Telefon 0228 9435-287
christopher.schlick@fkie.fraunhofer.de

Informationstechnik für Führungssysteme

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

Interoperabilität verteilter Systeme

Architekturen für Führungssysteme

Informationsanalyse

Ergonomie und Mensch-Maschine-Systeme

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

Systemtechnik

Human Factors

Unbemannte Systeme

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

Schematische Darstellung eines Aufklärungsfluges mit AMOS-T. Die Fusion von LIDAR und IR Daten führt zu einem verbesserten Lagebewusstsein.

KOMBINIERTE SENSORIK

Forscher des Fraunhofer FKIE vereinen Daten aus unterschiedlichsten Sensoren, wie Funkpeiler, Laser-Radar oder Bilder in unterschiedlichen Spektralbereichen. So lässt sich unbekanntes Gelände von unbemannten Flugplattformen genauer aufklären.

Unbemannte Luftfahrzeuge liegen im Trend. Sie liefern bei militärischen Einsätzen Informationen über ein unbekanntes Gebiet, ohne dass sich ein Pilot in Gefahr begeben muss. Allerdings können Miniflugzeuge nicht über einer interessanten Stelle still stehen und länger beobachten – das gelingt nur Drehflüglern wie dem AMOS-T. Der unbemannte Helikopter hat einen Rotordurchmesser von drei Metern und kann 25 Kilogramm Nutzlast tragen. Damit macht er seinem Namen alle Ehre: »Amos« kommt aus dem Hebräischen und bedeutet so viel wie »der Beladene«.

Beladen wird AMOS-T auch, von Experten der Abteilung Sensordaten- und Informationsfusion des Fraunhofer FKIE. Vor zwei Jahren hat das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) die Anschaffung des Helikopters gefördert, damit das Institut im Auftrag der Bundeswehr die Eignung zur Aufklärung unbekannten Geländes testen kann. In den vergangenen zwei Jahren hat das FKIE unbemannte Flugobjekte mit immer mehr Sensoren bestückt, die das Gelände abtasten (siehe Seite 27).

Laserecho verrät Geländeprofil

Zuletzt hat das Team von FKIE-Projektleiter Marek Schikora AMOS-T mit einer besonderen Kombination von Sensoren bestückt. Die Wissenschaftler haben eine Wärmebildkamera mit einem LIDAR (Laser Imaging Detection and Ranging) kombiniert. Der Laserscanner misst aus der Laufzeit des Laserlichts und des Echos die Entfernung zu einem Objekt, liefert also ein Höhenprofil des Bodens und das zentimetergenau. Mit an Bord ist ein GPS-Navigationssystem, das sich nicht allein auf Satellitensignale verlässt, sondern das mit Beschleunigungssensoren und Drehsensoren ausgerüstet ist. Es bestimmt die Position des Helikopters auf wenige Zentimeter genau und erkennt seine Neigung im Raum auf ein Zehntelgrad.

Die einzelnen Sensoren sehen nicht alles. Erst die Kombination ermöglicht eine umfassende Aufklärung. Der Laser erkennt zum Beispiel das Laub der Bäume, aber nur eingeschränkt was darunter ist. Hier kommt ein weiterer Sensor ins Spiel: eine Wärmebildkamera. Sie macht warme Bereiche durch rote Farbe sichtbar, kalte Bereiche sind blau. Eine Person am Boden erscheint also als roter Bereich im Bild, sogar unter dem Blätterdach kann die Kamera Personen aufspüren. Eine verlässlichere Aussage ergibt sich durch die Fusion beider Sensorarten.

Wissenschaftlich interessant und neu ist die Kombination von LIDAR und Wärmebildkamera. Man erhält ein dreidimensionales Geländeprofil mit der Temperatur als Farbe. Eine Person ist dann nicht nur ein roter Fleck, sondern eine rote Ausstülpung. Das liefert einen viel besseren Eindruck der Szene als jedes Bild alleine. Beide Sensoren arbeiten unabhängig vom Tageslicht, sie liefern also nachts die gleichen Bilder wie am Tag. Bei der Vermisstensuche kann dies der entscheidende Vorteil sein. Die Daten der Sensoren laufen in einem Rechner zusammen, der im Rumpf des Helikopters steckt. Von dort werden einige der Bilder per Funk in die Operationszentrale übermittelt.

AMOS-T fliegt bei Testflügen autonom. Das Navigationssystem wird vorher mit Koordinaten gefüttert, die der Helikopter selbstständig abfliegt, nur im Notfall greift der Operateur ein. Der Operateur kann den Helikopter über einer Stelle schweben lassen und diese Stelle näher untersuchen. Das ist zum Beispiel nützlich, wenn Rettungskräfte nach verschütteten Personen suchen oder austretendes Gas in einem Chemiewerk aufspüren wollen.

Mit der Kombination aus LIDAR und Wärmebildkamera ist ein Anfang gemacht. Als nächstes soll die Datenfusion automatisch ablaufen, bisher ist Handarbeit nötig, um die Bilder zur Deckung zu bringen. Außerdem möchte das Team von Marek Schikora die Auflösung des Wärmebilds

Sensordatenfusion mittels UAS ermöglicht zeitkritische Aufklärung im Katastrophenfall ohne Gefährdung der Einsatzkräfte.

erhöhen. Das ist noch ziemlich grobpixelig und liefert weit weniger Informationen als eine klassische Kamera. Dafür sind Wärmebildkameras aber sehr schnell. Das am AMOS-T montierte Modell schafft 60 Aufnahmen pro Sekunde. Das bietet die Möglichkeit, die Auflösung künstlich zu steigern. Dazu überlagert man mehrere leicht versetzte Aufnahmen zu einem Bild mit dann deutlich höherer Auflösung. Außerdem plant das Team, die bereits vorhandene Klassifikation von Objekten in den Aufnahmen weiter zu verbessern und vollständig zu automatisieren und vor allem verschiedene nicht-bildgebende Sensoren zum Einsatz kommen. Bisher muss der Operateur entscheiden, bei welchen Bildteilen es sich um eine Straße, ein Auto, ein Haus, Bäume oder um eine Person handelt.

Weitere Messkampagnen geplant

Für 2013 sind zwei Messkampagnen geplant, bei denen die Fortschritte überprüft werden sollen. Auch diese Flüge werden wie schon die Messkampagne 2012 auf einem Truppenübungsplatz stattfinden. Denn wegen seines Gewichts von 100 Kilogramm bräuchte der AMOS-T sonst eine Sonderaufstiegsgenehmigung.

Marek Schikora
Telefon +49 228 9435-816
marek.schikora@fkie.fraunhofer.de

DER FALL MIT DEM KNALL

In ihrer aktuellen Arbeit beschäftigt sich Miriam Häge mit der Peilung von Schallquellen – zum Beispiel von Scharfschützen.

Bundeswehr Heereslehrübung ILUE 2012 auf dem Truppenübungsplatz Bergen und Münster.

Ein Hinterhalt, Schüsse fallen. Blitzschnell muss die Truppe entscheiden, woher die Schüsse kommen, um in Deckung zu gehen. Für unsere Ohren ist das fast unmöglich, weil es bei einem Schuss zweimal knallt – an der Gewehrmündung und durch den Überschallknall am Geschoss. Technisch kann man sich das zunutze machen und aus dem Zeitversatz dieser beiden Knallereignisse die Richtung des Schusses bestimmen. Dass das funktioniert, hat Miriam Häge vergangenes Jahr auf dem Truppenübungsplatz in Hammelburg nachgewiesen.

Schwieriger wird es, wenn ein Hubschrauber beschossen wird, denn dessen Rotorblätter erzeugen selbst enorme Störgeräusche. In diesem Lärm ist es eine Kunst, Schüsse zu erkennen oder gar ihre Richtung herauszufinden. Auch dafür soll es künftig Software geben, Versuche mit dem AMOS-Helikopter des Fraunhofer FKIE sind geplant.

Um den Schlaf gebracht

Die Detektion akustischer Signale ist Thema gleich mehrerer Projekte am FKIE. Eines ist eine Machbarkeitsstudie zur Frage, ob sich Flugzeuge anhand ihrer akustischen Signale bereits in größerer Entfernung detektieren lassen. Das Problem: Auf den Türmen von Windrädern sind rote Blinklichter installiert, die Flugzeuge und Helikopter warnen und Kollisionen vermeiden sollen. Allerdings gibt es immer wieder Beschwerden von Anwohnern, die sich durch das Blinklicht gestört fühlen. Ein Ausweg wäre, dass man die Lampen nur einschaltet, wenn tatsächlich ein Flugzeug auf Kollisionskurs ist, fliegt es weit vorbei, soll die Lampe ausgeschaltet bleiben.

2012 hat Miriam Häge mit ihren Kollegen an einem Windrad in Wiemersdorf getestet, ob dieses Konzept erfolgversprechend ist. Auf der Gondel eines Windrades hat das Team Mikrofone installiert, ein Helikopter der Bundespolizei flog vorher abgesprochene Routen ab. Resultat: Das Konzept funktioniert. Die FKIE-Forscher können an den Geräuschen erkennen, ob sich ein Luftfahrzeug dem Windrad nähert, und das bis zu einer Reichweite von drei Kilometern – noch zu wenig, um die Blinkleuchten abzuschalten. Bis das akustische Detektionssystem zum Einsatz kommen kann, sind deshalb weitere Arbeiten nötig.

Miriam Häge
Telefon +49 228 9435-816
miriam.häge@fkie.fraunhofer.de

GERUCHSEXPLOSION

Eine neue elektronische Nase spürt Sprengstoffe auf. Josef Heinskill vom Fraunhofer FKIE hat die Datenanalyse und ein Trainingsprogramm dafür entwickelt.

Das kleine Glasfläschchen sieht eigentlich ganz harmlos aus. Ein paar Milliliter einer klaren und geruchlosen Flüssigkeit schwappen darin. »Das ist TATP, ein hochexplosiver Sprengstoff«, klärt Josef Heinskill auf und hantiert mit dem Fläschchen, als wäre es ein harmloser Parfümflakon. Die Informatikerin am FKIE kennt die Reaktionen ihrer Besucher schon. »Keine Angst«, beschwichtigt sie, »in flüssigem Zustand ist es völlig harmlos.« In trockener Form allerdings nicht: TATP (Triaceton-Triperoxid) ist einer jener tückischen Sprengstoffe, die Terroristen ohne großen Zeitaufwand herstellen können. Die explosive Chemikalie wurde vermutlich beim Attentat in der Londoner U-Bahn eingesetzt, wo sie 56 Menschen in den Tod riss.

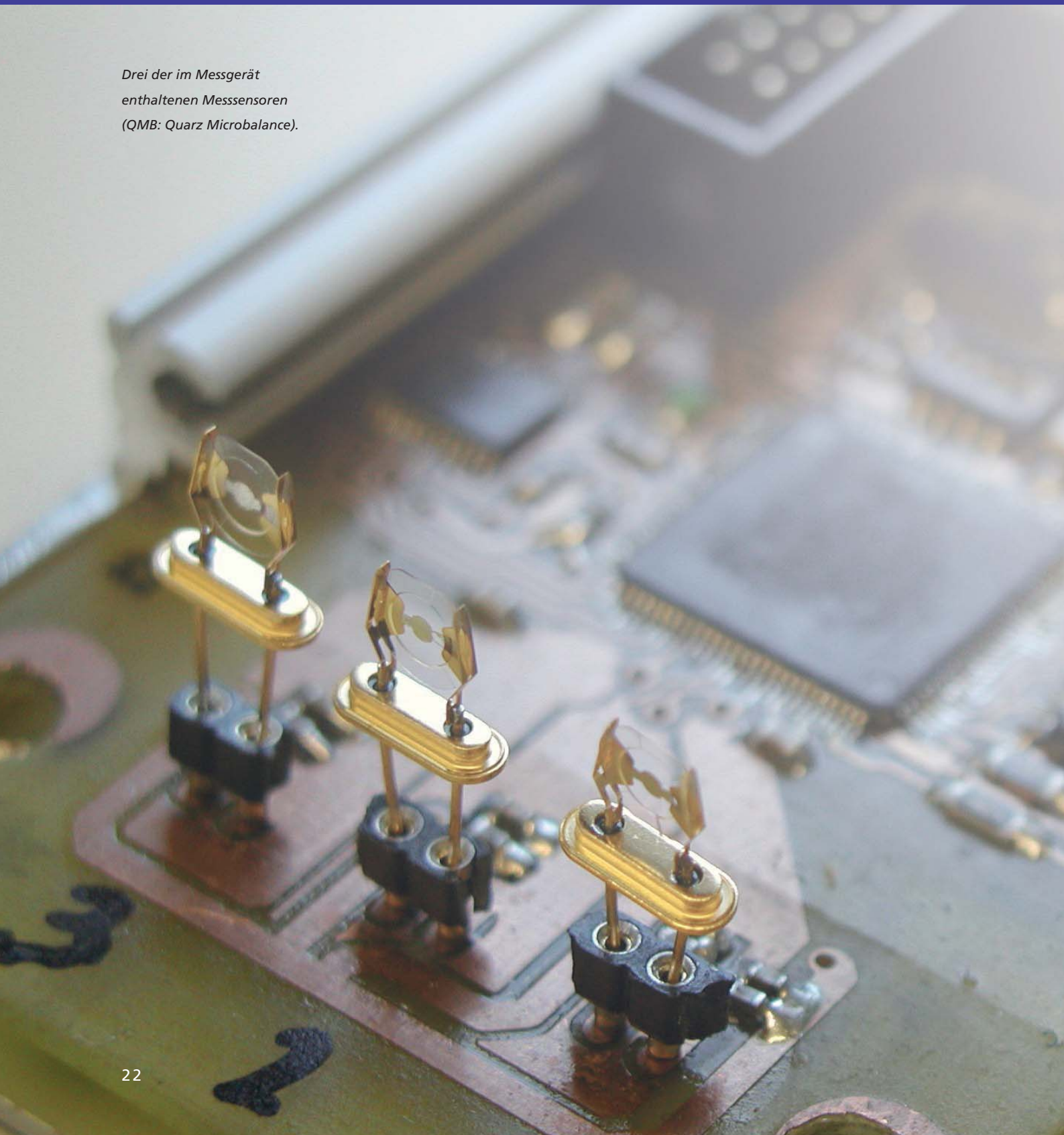
In Josef Heinskills Büro kann so etwas nicht passieren. Chemiker der Johannes-Gutenberg Universität in Mainz haben ein Lösungsmittel für TATP entwickelt, das den Sprengstoff im übertragenen Sinne in Watte packt. Gemeinsam mit den Kollegen in Mainz und Informatikern der Universität Bonn hat Heinskill einen Sensor entwickelt, der gefährliche Stoffe erschnüffeln kann – bald vielleicht sogar zuverlässiger als eine Hundenase. Gefördert wurde das Projekt »ENQUETE«, das Ende 2012 abgeschlossen wurde, vom Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen.

Untrüglicher Geruchssinn

Josef Heinskill hält das Fläschchen mit dem explosiven Stoff an ein Metallrohr, an dem vorne kleine Löcher zu sehen sind. Auf einem Bildschirm fangen rote Balken an zu tanzen und Sekunden später bleibt ein einzelner roter Balken übrig. Darunter steht: TATP 99%. Die Schnüffelnase hat den Sprengstoff also mit 99-prozentiger Sicherheit erkannt. Genau das ist es, worauf Polizei, Drogenfahnder und Katastrophenschutz seit langem warten: ein Messgerät, das gefährliche oder illegale Substanzen blitzschnell und mit hoher Zuverlässigkeit erkennt. TATP steht ganz oben auf der Wunschliste, denn für diese Substanz gibt es bisher keine zuverlässige Nachweismethode. Es sieht aus wie Zucker und fällt beim Röntgen oder in Massenspektrometern nicht auf, lässt sich also zum Beispiel an Flughäfen kaum aufspüren.

Der Sensor entdeckt nicht nur TATP – er erkennt auch andere Stoffe. Heinskill öffnet ein zweites Fläschchen, ohne auf das Etikett zu schauen. Nach wenigen Sekunden blinkt der Balken »Aceton« auf. Das Spiel lässt sich beliebig wiederholen, zum Beispiel mit Benzin, Ethanol oder Toluol.

Das Konzept für den Sensor QMB-Sensor (Quarz Microbalance) stammt von der Universität Mainz. Dort hatte man die Idee, Schwingquarze als »Riechrezeptoren« zu verwenden. Die Chemiker bringen eine Chemikalie auf den Schwingquarz auf, die eine bestimmte Substanz einfängt, zum Beispiel TATP. Strömt Luft vorbei, die TATP-Moleküle enthält, docken diese Moleküle an der Chemikalie auf dem Schwingquarz an. Durch das minimal höhere Gewicht schwingt der Quarz etwas langsamer und das lässt sich mit einer Elektronik messen.



Drei der im Messgerät enthaltenen Messsensoren (QMB: Quarz Microbalance).

Detektion von TATP mit Hilfe des entwickelten Messgeräts.

Olfaktorischer Fingerabdruck

Derzeit enthält das Messgerät, das als Prototyp wie ein kleiner Handstaubsauger aussieht, sechs Schwingquarze. Jeder Quarz ist für ein bestimmtes Gasmolekül zuständig, das typischerweise in dem aufzuspürenden Stoff vorkommt. Es gibt also keinen Quarz allein für TATP, alle sechs Quarze zusammen bestimmen vielmehr eine Art olfaktorischen Fingerabdruck, der typisch für die Substanz ist.

Hier kommt die Expertise der Abteilung Sensordatenfusion des FKIE ins Spiel. Die Fraunhofer-Experten verstehen es, aus scheinbar unzusammenhängenden Signalen Schlüsse zu ziehen. Häufig sind ihre »Rohstoffe« Funksignale, manchmal aber auch Signale, wie sie der neuartige Geruchssensor mit seinen sechs Quarzen liefert. Wenn die roten Balken am Bildschirm tanzen, übersetzt die Software von Josef Heinskill – der sogenannte Klassifikator – die Signale der Quarze in ein Profil, das für TATP, Aceton oder Benzin jeweils immer gleich ist. Ist das Profil eindeutig, schnellt der Balken, der für den aufgespürten Gefahrstoff steht, bis auf 100 Prozent. Allerdings gibt es unglaublich viele chemische Substanzen. Um sie alle zu entdecken, ist noch ein weiter Weg zurückzulegen.

Eine Frage des Trainings

Im Labor mit einem Fläschchen konzentriertem TATP klappt der Nachweis natürlich fast immer mit hundertprozentiger Sicherheit. Aber wie sieht es aus, wenn etwa Zollfahnder im Hafen den Inhalt eines Containers überprüfen wollen, um festzustellen, ob der Inhalt korrekt deklariert wurde oder ob zum Beispiel Drogen an Bord sind? Der Sensor müsse nahe an der Probe sein, sagt Heinskill, durch Containerwände werde es schwierig. Unmöglich ist es aber nicht und deshalb steht nun im FKIE ein Training an, das den Sensor auch mit stark verdünnten und mit anderen Substanzen maskierten Stoffgemischen testet. Die Schnüffelnase muss dann zeigen, ob sie auch unter realen Einsatzbedingungen besser ist als eine Hundenase.

Die Bedienung ist jedenfalls sehr einfach. Das Team von FKIE-Institutsleiter Professor Peter Martini an der Universität Bonn hat eine Software fürs Smartphone entwickelt, die das Ergebnis des Schnüffeltests in Sekundenschnelle auf dem Display eines iPhone zeigt. Es gibt bekanntlich für alles eine App – demnächst also auch eine App für Sprengstoff- und Drogenfahnder.

Noch einen weiteren Vorteil hat die elektronische Nase. Sie wäre in der Serienproduktion deutlich preiswerter als bisherige Gassensoren, und Batterien sind auf Dauer auch billiger als Hundefutter. Dazu fehlt allerdings noch ein Industriepartner, der den Entwicklungsaufwand bis zur Serienreife mitträgt. Professor Siegfried Waldvogel von der Universität Mainz ist derzeit auf der Suche nach einem geeigneten Partner. Ist der gefunden, könnten weitere Ideen umgesetzt werden, etwa die Bestimmung der Menge eines Gefahrstoffs.

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

TESTFLÜGE IN DER GÄNSEBUCHT

Forscher des Fraunhofer FKIE haben in Kanada getestet, wie sich mehrere unbemannte Flugzeuge vernetzen lassen.

Wer nach Neufundland reist, sucht Ruhe in einsamer Natur. Er muss allerdings abgehärtet sein, denn im Nordosten Kanadas steigt die Nachttemperatur nur wenige Wochen im Sommer über den Gefrierpunkt. Luftwaffenpiloten der NATO lassen sich davon nicht abschrecken. Der Flughafen im Städtchen Happy Valley-Goose Bay ist seit Jahrzehnten beliebtes Reiseziel. Mit seinen beiden drei Kilometer langen Landebahnen inmitten unbewohnter Landschaft ist der Ort ideal, um Tiefflüge zu üben oder neue Fluggeräte zu testen.

Im Sommer 2012 waren auch Wissenschaftler des Fraunhofer FKIE in Goose Bay. Sie arbeiten zusammen mit Kollegen von Cassidian sowie mit Partnern aus Finnland und der Schweiz in einem Projekt, in dem ein Systemdemonstrator »Agile UAV (Unmanned Aerial Vehicle – unbemannte Flugzeuge) in vernetzter Umgebung« entwickelt und getestet wird. Das Projekt soll zeigen, dass unbemannte Flugzeuge Ziele erkennen und auch in der Luft verfolgen können. Diese Idee ist nicht neu, neu hingegen ist, mehrere unbemannte Flugzeuge so zu vernetzen, dass sie gemeinsam eine solche Mission möglichst autonom bewältigen können, allerdings so dass der Mensch immer die letzte Kontrolle hat. Es wurde dazu ein anspruchsvolles, da äußerst komplexes Szenario einer weiten Raumüberwachung kombiniert mit einer Nahaufklärung durch zwei kooperative Plattformen, die auf vorprogrammiertem Kurs ihren Missionen nachkommen, kreiert.

Technologieträger Barracuda und Learjet bei der Landung in Goose Bay.

Fliegender Barracuda

Genau dieses Szenario haben die Projektpartner in Kanada durchgespielt. Als unbemanntes Luftfahrzeug kam der Technologieträger Barracuda von Cassidian zum Einsatz. Das drei Tonnen schwere unbemannte Flugzeug flog schon 2009 und 2010 ähnliche Tests in Goose Bay. Die Rolle einer zweiten Plattform übernahm ein bemannter Learjet, der mithilfe einer Autopilot-Anlage und einer extra eingerüsteten, ständigen Datenfunkverbindung ein unbemanntes Flugzeug simulierte. Ziele bei den fünf Testflügen waren mehrere Fahrzeuge, die durchs Gelände fuhren, sowie ein niedrig fliegender Helikopter.

Die FKIE-Forscher haben für den Demonstrator eine Software entwickelt, die Zielobjekte verfolgt und die Datenstränge beider fliegender Systeme vereint. Die waren mit völlig unterschiedlichen Sensoren bestückt, um möglichst viele unterschiedliche Daten zu erhalten. Der Learjet war mit einem Radar ausgerüstet, das ein großes Gebiet überwachte, der Barracuda mit optischen und Wärmebildkameras, die Ziele aus der Nähe erfassten.

Das Erfassen und Verfolgen der Objekte – das so genannte Tracking – erfolgt in mehreren Schritten: Das Radar an Bord des Learjets sendet seine Daten an die Bodenstation, die daraus Objekte sowie ihre Bewegungsrichtung – die Tracks – erkennt. Diese Trackingspuren potenzieller Objekte werden an den Barracuda übermittelt, der mit seinen Kameras das Objekt näher unter die Lupe nimmt. Auch diese Aufnahmen gelangen ins Kontrollzentrum, wo sie mit den Aufnahmen des Radars fusioniert werden. Diese Tracks werden wieder zum Barracuda zurückgespielt, der die weitere Beobachtung übernimmt. Der Operateur im Kontrollzentrum kann die Szene verfolgen und sich die Tracks in einem Video anzeigen lassen, das die Kamera an Bord des Barracuda laufend aufnimmt.

Beim Bestimmen der Tracks kommt den FKIE-Experten langjähriges Know-how der Abteilung Sensordaten- und Informationsfusion zugute. Um aus der Bewegung des Zielobjekts die Bewegung in den nächsten Sekunden vorherzusagen, arbeitet das Team mit einem Schätzverfahren, bei dem mehrere hypothetische Bewegungen in die Berechnung einfließen. Das ist notwendig, weil die Daten der Kameras relativ grob sind. Die Software gleicht die prognostizierten Wege laufend darauf ab, ob sie noch mit den aktuellen Daten der Kameras übereinstimmen. Liegen die Tracks, die die Barracuda-Sensoren liefern und die Tracks aus dem Radar an Bord des Learjets sowie der fusionierte Track nahe genug beisammen, geht die Software davon aus, dass es sich um ein und dasselbe Objekt handelt. Die Software gibt dann den Ort und die voraussichtliche Bewegungsrichtung des Objekts aus sowie den zu erwartenden Fehler.

Helikopter ersetzt Learjet

Mit der Kampagne in Kanada ist dieses Projekt erst einmal abgeschlossen. Das ist allerdings nicht das Ende der Forschung am Fraunhofer FKIE. Denn in einem nächsten Schritt sollen die Sensordaten des Barracuda mit Beobachtungsdaten eines unbemannten Helikopters fusioniert werden, der bis 25 kg Nutzlast tragen kann und auch in anderen Projekten der Abteilung Sensordaten- und Informationsfusion Verwendung findet. Damit ändert sich auch das Einsatzszenario. Während die beiden Flugzeuge 2012 bei den Flügen in Kanada ein großes Gebiet überwachen mussten, soll es künftig um kleinere Areale gehen. Dann wird insbesondere die Lokalisierung von Emittern Thema sein, also das Aufklären von Quellen, die während des Betriebs elektromagnetische Strahlung aussenden.

Julian Hörst
Telefon +49 228 9435-761
julian.hoerst@fkie.fraunhofer.de

MIT FLEISS ZUM PREIS

Miriam Häge (28) entwickelt am Fraunhofer FKIE Methoden zur Peilung von Funk- und Schallquellen. Für ihre Arbeiten wurde sie mehrfach ausgezeichnet.

Sie haben kürzlich für Ihre Master-Arbeit den Preis der Deutschen Gesellschaft für Ortung und Navigation (DGON) gewonnen. Herzlichen Glückwunsch!

Vielen Dank. Das ist eine große Ehre für mich, denn die DGON ist eine sehr renommierte Organisation.

Die Jury lobt den hervorragenden Aufbau Ihrer Arbeit und das hohe Innovationspotenzial. Worum geht es genau?

Es geht um die Peilung von Funkquellen aus der Luft von einer autonomen Flugplattform. Dazu nutzt man ein Antennenarray, also eine Anordnung von mehreren Antennen. Dieses Array sollte möglichst klein und leicht sein, da die Zuladungskapazität des Fluggerätes begrenzt ist. Bedingt durch die geringe Größe des Arrays ist aber auch die Peilauflösung eingeschränkt. Um die Peilung zu verbessern, kann man als zusätzliche Information die Polarisation der Funkwellen, also die Orientierung des elektrischen Feldes, auswerten. In meiner Masterarbeit habe ich ein Modell entwickelt, das die Polarisation berücksichtigt. Das Konzept funktioniert, das zeigen Messungen im Labor, Tests im echten Einsatz stehen aber noch aus.

Die Master-Arbeit haben sie im Studiengang Angewandte Physik an der Hochschule Koblenz absolviert. Das war aber gar nicht ihr ursprüngliches Studienfach?

Das stimmt. Ich habe zuerst Medizinische und Sportmedizinische Technik ebenfalls an der Hochschule Koblenz studiert. In Verbindung damit habe ich mich im Jahr 2008 für die Bachelor-Arbeit am FKIE beworben und in der Folge einen Fusionsalgorithmus zur Peilung mit Antennenarrays auf einer unbemannten Flugplattform entwickelt. Die Idee dabei war, die Peilung der Funksignale zu verbessern, indem man noch Kamerabilder hinzunimmt.

Auch dafür gab es einen Preis?

Ja, 2009 hat mir das Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung (AFCEA) den Studienpreis für meine Bachelor-Arbeit verliehen.

Medizintechnik und Fusionsalgorithmen: Was hat das miteinander zu tun?

Während meines Medizintechnik-Studiums habe ich die naturwissenschaftlichen Grundlagen erworben, die ich später gut einsetzen konnte. Schließlich fand ich die Vielfalt der Sensoren und die Möglichkeiten, damit zu arbeiten, in der Abteilung Sensordatenfusion des FKIE so spannend, dass ich mich dort beworben habe. Allerdings kannte ich das Institut schon vorher, das frühere FGAN-Institut hatte hier in der Gegend einen guten Namen. 2005 habe ich am Institut schon mal ein Praktikum absolviert und so kam der erste Kontakt zustande. Wenn man in ein fachfremdes Gebiet einsteigt, ist das natürlich erst mal ungewohnt. Aber ich habe schnell gemerkt habe, dass man sich in neue Themenbereiche einarbeiten kann.

Eine beliebte Frage aus Bewerbungsgesprächen: Wo sehen Sie sich in fünf Jahren?

Ich fühle mich in der Forschung sehr wohl und könnte mir vorstellen, noch einige Zeit hier am FKIE zu arbeiten. Vielleicht bietet sich auch die Möglichkeit einer Promotion an. Ein genaues Thema steht noch nicht fest, aber ich stehe mit meinem möglichen Betreuer Dr. Wolfgang Koch in engem Austausch. Ich könnte mir außerdem noch einen Forschungsaufenthalt im Ausland vorstellen.

Miriam Häge
Telefon +49 228 9435-816
miriam.häge@fkie.fraunhofer.de

DIE MASSE MACHT´S

Flache Hierarchien sind nicht nur im Management gut – auch Kommunikationsnetze sind leistungsfähiger, wenn man die Aufgaben gleichmäßig auf alle Schultern verteilt. Das Fraunhofer FKIE entwirft solche Infrastrukturen für die Bundeswehr.

Weihnachten 2010: Millionen Menschen wollten ihren Verwandten via Skype ein frohes Fest wünschen. Doch das Netz des beliebten Videochatdienstes war dem Ansturm nicht gewachsen. Bei Nutzern, die mit veralteter Skype-Software arbeiteten, stürzte die Software ab und ließ sich nicht mehr starten. Weil deshalb Datenströme umgeleitet wurden, erhöhte sich die Last auf die übrigen Rechner mit Skype-Programmen, die nun ihrerseits wegen Überlastung streikten. Zeitweise stieg der Datenverkehr über bestimmte Verbindungen auf das Hundertfache des normalen Werts an. Dieser Dominoeffekt legte Skype schließlich für 24 Stunden lahm.

Hierarchisch organisierte Kommunikationsnetze sind preiswert, sie sind aber auch anfällig. Wenn der Datenverkehr eines Dienstes von nur einem oder wenigen zentralen Rechnern organisiert wird, führt ein Ausfall dort zu einem Kollaps des gesamten Dienstes – wie bei Skype. Auch so genannte Publish-Subscribe-Dienste (Publizieren-Abonnieren) sind immer mal wieder betroffen. Damit sind alle Dienste im Internet gemeint, bei denen Informationen über eine zentrale Stelle verteilt und von vielen Nutzern abonniert werden. Das kann die Seite mit der Wettervorhersage sein, ein soziales Netzwerk wie Facebook, aber auch E-Mail-Dienste wie GMX oder Google-Mail.

Publish-Subscribe-Dienste gibt es auch für militärische Anwendungen. Sie übermitteln zum Beispiel Lagebilder mit Informationen über den Standort der eigenen Kräfte über solche hierarchisch organisierten Infrastrukturen. Ihr Einsatz ist dort aber noch kritischer. Einerseits hängen vom reibungslosen Datenverkehr Menschenleben ab, andererseits sind diese Infrastrukturen häufig mobil und damit anfällig gegen schlechtes Wetter oder Bedrohungen durch Gegner.

Auf viele Schultern verteilt

Die Alternative: Peer-to-Peer-Netze was man mit »Gleiche unter Gleichen« übersetzen könnte. Dort gibt es keine zentralen Rechner mehr, alle Computer, die den Dienst nutzen, sind gleichberechtigt und arbeiten sowohl als Empfänger als auch als Sender von Informationen. Ihr schlechtes Image als Verteiler illegaler Musikdownloads haben Peer-to-Peer-Netze längst abgeschüttelt. Für Computerexperten sind sie eine gute Wahl, wenn es um den Aufbau möglichst robuster Kommunikationsnetze geht. Auch Skype ist im Ansatz so ein verteiltes Netz. Denn der Dienst spannt die PCs seiner Kunden ein, um den gesamten Datenverkehr besser zu verteilen. Wer Skype nutzt, gibt also immer auch etwas Rechenleistung seines PCs für die Allgemeinheit ab. Anfällig ist der Dienst aber trotzdem, weil 20 bis 30 Prozent der Rechner im Skype-Netz übergeordnete Knoten – so genannte Super-Peers – sind, die bei Ausfällen wie ein Nadelöhr wirken.

Was die Arbeitsgruppe »Robuste heterogene Netzwerke« des Fraunhofer FKIE im Auftrag der Bundeswehr untersucht, ist dagegen ein Peer-to-Peer-Netz in Reinkultur. Es wickelt Publish-Subscribe-Dienste ab, die nach dem Standard WS-Brokered Notification arbeiten. Diese Kombination ist neu, denn wie der Name schon sagt: Dieser Standard setzt eigentlich einen „Broker" voraus, also eine zentrale Stelle, die als Umschlagplatz für alle Informationen dient – und damit gerade das Gegenteil eines Peer-to-Peer-Netzes. Weil WS-Brokered Notification ein weit verbreiteter offener Standard ist, den sogar die NATO für Publish-Subscribe-Dienste empfiehlt, setzt auch das FKIE-Team darauf, allerdings erstmals kombiniert mit einem Peer-to-Peer-Netz.

Tobias Ginzler hat dazu die Funktion des zentralen WSN-Brokers aufgeteilt. Auf jedem Rechner im Netz läuft nun ein P2P-WSN-Broker, gemeinsam übernehmen sie die Aufgabe, die früher ein zentraler Broker alleine hatte. Fällt einer aus, ist das nicht tragisch, dann übernehmen die anderen seine Funktion, das Netz organisiert sich automatisch neu. Der Clou: Die Publish-Subscribe-Dienste bekommen davon nichts mit. Für sie erscheint es so, als ob nach wie vor ein zentraler Broker den Datenverkehr koordiniert. Das ist wichtig, damit vorhandene Dienste auch in der neuen dezentralen Infrastruktur weiter funktionieren.

Das militärische Netz der Zukunft

Seine erste Bewährungsprobe hat die Software bereits hinter sich. Tests in einem kleinen Peer-to-Peer-Netz am Fraunhofer FKIE haben gezeigt, dass das Konzept funktioniert und Ausfälle verkraftet. Ob das auch in größeren Netzen gilt, soll ein Test im CoNSIS-Projekt (siehe Seite 36) zeigen. Dort untersuchen Wissenschaftler aus vier Nationen das militärische Netz der Zukunft. Ein Test in einer solchen Umgebung ist eine große Herausforderung, weil unterschiedliche Anforderungen von den Projektpartnern an einen Peer-to-Peer-Abonnentendienst unter einen Hut gebracht werden müssen. Auf die speziellen militärischen Anforderungen wie Robustheit und Mobilität legt CoNSIS besonderes Augenmerk. Ein erfolgreicher Test wäre daher ein großer Erfolg für das Projekt und könnte gezielte Anregungen für die Weiterentwicklung geben.

Für den militärischen Einsatz steckt viel Potenzial im Peer-to-Peer-Konzept, vor allem wenn es um zeitlich begrenzte Datenpakete geht, etwa beim Austausch von Dateien, Lagebildern oder Wetterdaten. Für kontinuierliche Datenströme, etwa zum Telefonieren oder Videochat, sind zentral organisierte Netze bisher nicht zu ersetzen. Gemeinsam mit den Kollegen des CONSIS-Projekts überlegt das Team nun, das Konzept in ein Endgerät – zum Beispiel einen Tabletcomputer – einzubauen.

Dr. Tobias Ginzler
Telefon +49 228 9435-715
tobias.ginzler@fkie.fraunhofer.de

MUT ZUR LÜCKE

Funkgeräte suchen sich in Zukunft automatisch freie Sendefrequenzen. Das Fraunhofer FKIE baut dafür einen Demonstrator.

Im Äther herrscht Hochbetrieb. Sämtliche Funkfrequenzen von der Langwelle bis zum Radar sind für die Übertragung von Radio-, TV-, Mobilfunk- und vielen weiteren Signalen reserviert. Misst man genauer, findet man aber durchaus noch Lücken: Bis zu 95 Prozent der Funkübertragungskapazitäten sind statistisch ungenutzt. Allerdings ändert sich das laufend. Nutzen könnte man diese brachliegenden Kapazitäten mit einer Infrastruktur, bei der die beteiligten Sender und Empfänger nicht feste Frequenzkanäle belegen, sondern blitzschnell auf die Frequenzen hüpfen, die gerade frei sind. Das ist die Idee von Cognitive Radio. Telekommunikationsexperten setzen große Hoffnungen darauf, um künftig weit mehr Datenverkehr per Funk abwickeln zu können, vor allem über mobile Geräte wie Smartphones.

Cognitive Radio ist derzeit ein reines Forschungsthema – es gibt noch keine Geräte zu kaufen. Das liegt zum einen an der komplexeren Hardware. So muss zum Beispiel ein Cognitive-Radio-Handy mehr Frequenzbänder abdecken und braucht dazu eine aufwändigere Elektronik und Antenne. Zum anderen muss es automatisch erkennen, welche Frequenzen gerade frei sind und welche davon eine schnelle und vor allem stabile Verbindung versprechen. Das ist vor allem bei militärischen Einsätzen oder Hilfseinsätzen von Rettungsdiensten nach Naturkatastrophen wichtig, wo die beteiligten Geräte mobil und robust sein müssen und das häufig in Gegenden ohne jede Funkinfrastruktur.

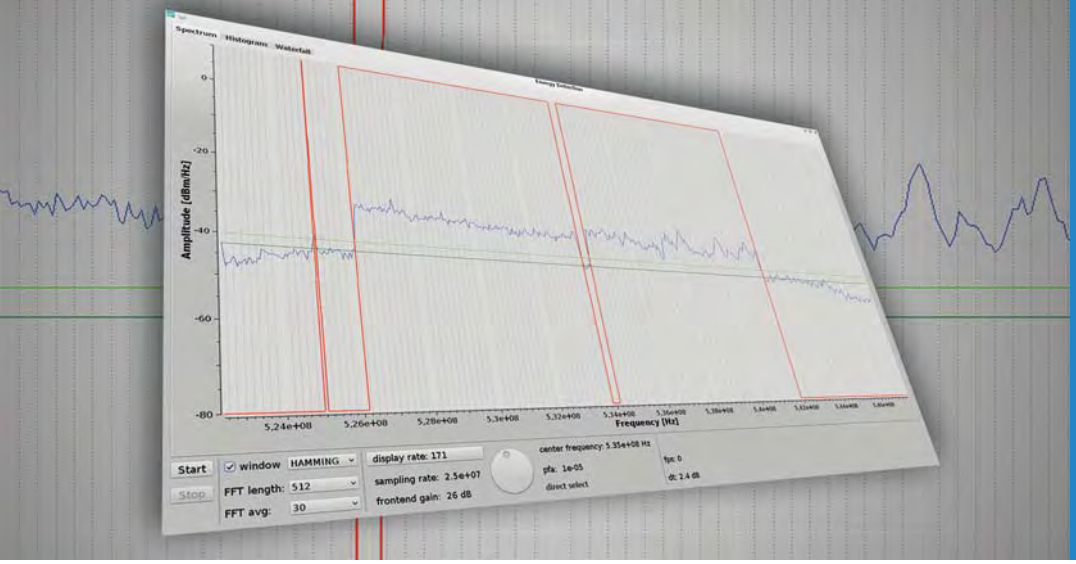
Simulator für den militärischen Einsatz

Weil Cognitive Radio ein völlig neues Prinzip ist, wird es derzeit ausgiebig erforscht – auch beim Militär. Das geht am besten mit einem Simulator. Für den militärischen Einsatz entwickeln sieben Nationen im Projekt Cognitive Radio for Dynamic Spectrum Management gemeinsam einen Simulator. Mit von der Partie sind neben Deutschland noch Belgien, Frankreich, Italien, Polen, Portugal und Schweden. Koordinator ist die European Defence Agency EDA. Gemeinsame Grundlage für alle teilnehmenden Nationen ist ein Simulator, der ganz allgemein Funkverfahren simuliert. Darin wurde für das Projekt ein Funknetz erstellt, das sehr viele Einstellmöglichkeiten bietet und sich somit als Basis für Cognitive Radio eignet. Das Fraunhofer FKIE beteiligt sich als Unterauftragnehmer an dem Projekt.

Sämtliche Partner entwickeln eigene Lösungen für das Dynamic Spectrum Management, aufbauend auf dem gemeinsamen Funknetz, und optimieren verschiedene Bereiche dieses Netzes. Bis Ende 2013 werden alle Arbeiten zu einem Demonstrator zusammengefasst, mit dem die Partner den Einsatz von Cognitive Radio in verschiedenen Szenarien testen wollen. Er soll als Basis für die weitere Entwicklung des Konzepts für militärische Zwecke in Europa dienen. Ein einheitlicher Standard für Cognitive Radios sei derzeit noch nicht geplant, sagt Stefan Couturier, der für den Beitrag des Fraunhofer FKIE verantwortlich ist. Dafür allerdings einheitliche Schnittstellen, so dass die unterschiedlichen Cognitive Radios, die in den Ländern entwickelt werden, dennoch reibungslos zusammenarbeiten.

In seinem Arbeitspaket beschäftigt sich das Fraunhofer FKIE insbesondere mit drei Themen:

- **Cognitive Manager:** Jedes Cognitive Radio enthält ein Spektrum Management, das die optimalen Parameter der Funkverbindung – Fachleute sprechen von einer Wellenform – identifiziert und automatisch umsetzt, ohne dass der Nutzer dies merkt oder eingreifen muss. Stefan Couturier interessiert sich besonders dafür, wie fair solche Entscheidungen sind. Denn wenn Dutzende Funkgeräte gleichzeitig eine freie Frequenz belegen wollen, muss es Regeln geben, wer Vorrang hat.



Energiedetektion im DVB-T Spektrum.

- **Spectrum Sensing:** Ein Gerät mit Cognitive Radio sucht laufend im Frequenzspektrum nach freien Frequenzen. Das FKIE-Team hat verschiedene Sensing-Techniken darauf untersucht, ob sie für Cognitive Radio geeignet sind. Eine Möglichkeit ist, die Belegung einer Frequenz aus der Energie der Funkwellen abzuleiten. Dazu hat das Team einen neuen Algorithmus entwickelt, der die Energie im Funkspektrum anhand von graphischen Verfahren darstellt und daraus ableitet, wo gerade gesendet wird. Der Cognitive Manager passt daran die Parameter der Funkverbindung an.

- **Electronic Warfare:** Hier untersuchen die FKIE-Experten, ob ein dynamisches System wie Cognitive Radio anfällig gegen absichtliche Störversuche ist und wie man es dagegen schützen kann.

Henne-Ei-Problem

Eine vollständige Freiheit im Äther wird es auch mit Cognitive Radio nicht geben. Um das Konzept sinnvoll betreiben zu können, möchte man in einem ersten Schritt bestimmte Bereiche im Spektrum der Funkfrequenzen dafür reservieren. Doch die Frequenzen sind begehrt und keiner der heutigen Nutzer wird das Feld freiwillig räumen, schon gar nicht wenn es noch nicht einmal Geräte gibt, die diese Frequenzen für Cognitive Radio nutzen. Andererseits haben die Hersteller keine große Motivation, solche Geräte anzubieten, wenn die Frequenzen dafür fehlen – ein typisches Henne-Ei-Problem. Mit dem Demonstrator will die European Defence Agency sozusagen das erste Ei legen und zeigen, welche Potenziale in Cognitive Radio stecken. Das soll Hersteller und Militärs davon überzeugen, dass sich der Einstieg in diese Technologie lohnt, weil sie viele Vorteile gerade im militärischen Einsatz bringt.

Stefan Couturier
Telefon +49 228 9435-516
stefan.couturier@fkie.fraunhofer.de

GERÄUSCHE INTELLIGENT ERKENNEN

Mit einer neuen Rechenmethode erkennt und klassifiziert Frank Kurth vom Fraunhofer FKIE Geräusche.

Aus dem Lautsprecher ertönen nacheinander zwei Geräuschsequenzen mit verwandter Klangstruktur. Bei der ersten Abfolge handelt es sich um schnelle Klicklaute, die Delphine zur Kommunikation untereinander einsetzen. Die zweite Sequenz – eine Maschinengewehrsalve – klingt strukturell ganz ähnlich, aber ruft ganz andere Assoziationen hervor.

Für Soldaten im Einsatz ist es überlebenswichtig, einen Feuerstoß schnell zu lokalisieren und zwischen den Schüssen eigener Kameraden und gegnerischer Kämpfer zu unterscheiden. Frank Kurth von der Abteilung Kommunikationssysteme des Fraunhofer FKIE und außerplanmäßiger Professor an der Universität Bonn erforscht, ob sich akustische Signale schnell und sicher genug klassifizieren lassen, um im Ernstfall wertvolle Informationen zu liefern.

Navi für U-Boote

Im Rahmen eines Forschungsprojektes mit der US-Marine hat Kurth eine Technologie entwickelt, um Wale und andere Meeressäuger aufzuspüren. Wenn U-Boote durch die Ozeane kreuzen, treffen sie hin und wieder mit solchen Tieren zusammen. Um künftig mögliche Störungen der Tiere zu vermeiden, benötigen die U-Boote ein passives System, also ohne Aussenden verräterischer Echosignale. Das soll die Tiere rechtzeitig aufspüren und die Richtung ihrer Wanderung erkennen, damit das U-Boot sie umfahren kann. Ist da was? Diese Frage zu beantworten ist aber gar nicht so einfach angesichts des Geräuschpegels unter Wasser, der von Schiffen oder vom U-Boot selbst stammt. Mit der Entwicklung aus der Abteilung Kommunikationssysteme geht das. Sie ist neu und auf dem besten Weg, ein universelles Konzept zur Erkennung von Geräuschen zu werden, das bereits zum Patent eingereicht ist.

Frank Kurth deutet auf den Bildschirm, wo die bunten Geräuschprofile der Delphingesänge und des Maschinengewehrs zu sehen sind. Sie ähneln sich, weil sie regelmäßig sind. Bei den Meeressäugern wiederholt sich das Klicken etwa alle fünf Millisekunden, beim Maschinengewehr ist es der Mündungsknall, der etwa alle 50 Millisekunden entsteht. Diese strukturelle Ähnlichkeit macht sich der Erfinder zunutze.

Training mit bekannten Geräuschen

Bisher arbeiten Algorithmen zum Aufspüren von akustischen Signalen mit der Autokorrelation. Durch einen Vergleich von mehreren leicht verschobenen Versionen desselben Signals entsteht eine mathematische Funktion, die anzeigt, ob es im Signal Anteile gibt, die sich wiederholen. Das funktioniert sehr gut bei Signalen, in denen das Geräusch oft und lange auftritt. Einen kurzen Feuerstoß aus einem Maschinengewehr erkennt die Autokorrelation aber nicht so gut.

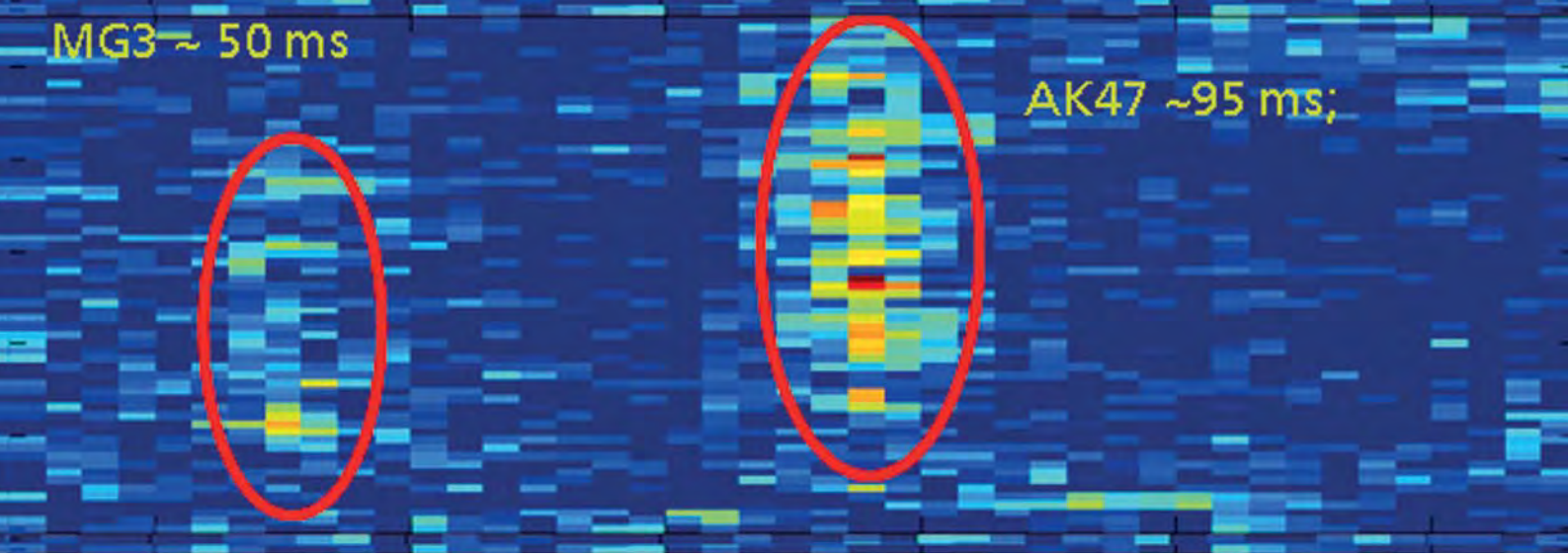
Der Informatiker hat deshalb die Shift-Methode entwickelt, eine Weiterentwicklung der Autokorrelation. Gibt man dem Algorithmus bekannte Signalfolgen vor, trainiert man ihn also darauf, erkennt er auch schwache und kurze Geräuschfolgen deutlich besser, Störgeräusche werden zudem effektiver unterdrückt. Das zeigt die Kurve der Shift-Autokorrelationsfunktion: Wo sich das schwache Krrrrrrt des Tümmlers im lauten Meeresrauschen vorher nur als sanfter Hügel in der Funktion bemerkbar macht, erscheint nun eine hohe, scharfe Spitze. Je mehr Vorwissen – also Training mit Geräuschen – man hineinsteckt, umso schärfer wird die Spitze und umso sicherer die Erkennung. »Das kann man sogar mathematisch beweisen«, sagt Kurth.

Die präzise Erkennung einer Signalfolge mit der Shift-Autokorrelation erlaubt es nun, ähnliche Signalfolgen besser voneinander zu trennen. So ist der Algorithmus in der Lage, die Klickgeräusche mehrerer Tümmler in Unterwasseraufnahmen auseinander zu halten. Und tatsächlich: Was sich für das Ohr wie ein einziges durchgängiges Krrrrrt anhört, sind in Wirklichkeit die Laute von zwei Tieren, die miteinander kommunizieren.

Buckelwal Unterwasser.

Ergebnis einer frequenz-selektiven Shift-Autokorrelation mit markierten, mit den Feuerstößen korrespondierenden Bereichen.

Schießausbildung-
ein Soldat im Anschlag.



Wer schießt auf wen?

Das hilft, auch Maschinengewehre voneinander zu unterscheiden. Zum Beispiel eine Kalaschnikov von einem Modell der Bundeswehr. Das MG3 feuert etwa 20mal pro Sekunde, während die Kalaschnikov etwas langsamer ist. Auch hier zeigt die Shift-Autokorrelationsfunktion: In der Tonaufnahme feuert nicht bloß eine Waffe, in Wirklichkeit sind es zwei. Unter den Feuerstoß des MG3, der etwa vier Sekunden dauert, mischen sich vom Ohr kaum zu unterscheidende Schüsse aus dem anderen Maschinengewehr. Eine solche Situation muss der Algorithmus später im Gefecht blitzschnell erfassen. Schießen, weil man von Heckenschützen angegriffen wird, oder nicht schießen, weil die Schüsse von eigenen Kameraden stammen – von dieser Entscheidung kann das eigene Leben und das der Kameraden abhängen. Bewährt sich das System in Tests, könnten künftig Mikrofone auf Fahrzeugen installiert oder von Bodentruppen im Feld aufgestellt werden.

Gemeinsam mit Kollegen der Abteilung Sensordatenfusion denkt Kurth über ein Konzept nach, wie man diese Informationen mit anderen Daten verbinden kann. Kennt man die Bewaffnung feindlicher Einheiten, könnte man mit der Autokorrelationsfunktion ganze Lagebilder erstellen, also zum Beispiel eine Karte, die den Standort des Gegners zeigt.

Im Grunde lässt sich das Verfahren für alle Geräusche verwenden, die sich regelmäßig wiederholen. Das können Schritte eines Angreifers sein, der nachts auf ein Feldlager in Afghanistan zurennt. Oder Klopfgeräusche von Verschütteten nach einem Erdbeben, ebenso das Rotorgeräusch eines nahenden Hubschraubers. Auch Sprache hat regelmäßige Anteile und so eignet sich der Algorithmus, um bei Lärm Sprachsignale zu erkennen, auch in stark verrauschten Sprechfunksignalen.

Die Natur belauschen

Wie universell die Methode ist, beweist ein Projekt mit Naturkundlern, bei dem es um die Erfassung einer Vogelpopulation ging. Auch Vogelgezwitscher ist regelmäßig und individuell, so dass man die einzelnen Tiere unterscheiden kann. Das machen sich neuerdings Naturschützer zu nutze. Statt tagelang auf der Lauer zu liegen, überlassen sie es dem Algorithmus von Frank Kurth, die Arten und die Zahl der Tiere zu bestimmen. Dass das funktioniert, wurde bereits an einem See in Brandenburg bewiesen. Das Museum für Naturkunde in Berlin hat ein Tierstimmenarchiv mit allein 1800 Vogelarten. Einige davon dienten als Training für eine Software zur akustischen Mustererkennung, die damals noch an der Bonner Informatik entwickelt wurde. Dann ging es hinaus in die Natur. Eine Woche lang sammelten die Mikrofone jedes Geräusch am See, die automatische Auswertung dauerte eine Nacht. Dann war klar: Am See leben drei Uhus und sieben Rohrdommeln. Würde hier jemand bauen wollen, hätte er schlechte Karten.

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

KOMMUNIZIEREN IM KONVOI

Was geschieht, wenn internationale Truppen Fahrzeuge mit unterschiedlicher Funkausrüstung vernetzen wollen? Das Fraunhofer FKIE hat das in einem Feldtest ausprobiert.

Es herrscht Bürgerkrieg im Land. Soldaten einer internationalen Friedensmission sollen die Lage stabilisieren und die Bevölkerung schützen. In den Städten gelingt ihnen das, auf dem Land und in den Bergen ist die Lage aber noch außer Kontrolle: Immer wieder werden dort Konvois angegriffen. Da passiert ein Erdbeben – Dörfer sind von der Außenwelt abgeschnitten und benötigen Hilfe. Doch die läuft wegen der schlechten Sicherheitslage nur schleppend an. Truppen sollen Nichtregierungsorganisationen zum Hilfseinsatz in die Berge geleiten.

Das Beispiel ist fiktiv – und doch typisch für viele Einsätze in Ländern, wo Menschen unter Bürgerkrieg und Naturkatastrophen leiden. Hilfe tut Not. Doch wären internationale Truppen überhaupt in der Lage, ein solches Land zu befrieden und im Katastrophenfall Hilfskonvois zu schützen? Die Frage lässt sich nur eingeschränkt mit Ja beantworten. Vor allem die Kommunikation unter den Verbänden der verschiedenen Nationen und mit den nichtmilitärischen Organisationen stellt sich bislang als problematisch dar. Das hat vor einigen Jahren die NATO Network Enabled Feasibility Study ergeben, die eine bessere Interoperabilität der Kommunikationstechnik verschiedener Nationen fordert. Diese Forderung greift CoNSIS auf. In dem internationalen Forschungsvorhaben »Coalition Networks for Secure Information Sharing« arbeiten Deutschland, Frankreich, Norwegen und die USA an mobiler Kommunikationstechnik für den taktischen Einsatz.

Krisenszenario macht Lücken sichtbar

In der ersten Phase von 2008 bis 2012 beschäftigte sich CoNSIS mit den Grundlagen. Das Projekt wurde 2012 um weitere vier Jahre verlängert. Jetzt sollen Lücken geschlossen und weitere praktische Tests ausgeführt werden. Der erste fand 2012 bei der wehrtechnischen Dienststelle im bayerischen Greding statt. Dieser Test dauerte zwei Wochen und lehnte sich an das eingangs beschriebene Szenario an. Das ist gerade so gewählt, dass es Klippen in der Kommunikation zwischen den Beteiligten des Einsatzes entlarvt. Folgende Teilszenarien und Technologieaspekte betrachten die Partner in CoNSIS:

Teilszenario 0 – Einsatz im Bürgerkriegsland. Die Friedenstruppen stammen aus mehreren Ländern, die Kommunikationstechnik ist folglich nicht aus einem Guss. Trotzdem müssen sich die Nationen ein gemeinsames Bild der Lage machen. Dazu nutzen sie Serviceorientierte Architekturen (SOA), also Softwaremodule, die bestimmte Kommunikationsdienste bereitstellen. Schon in dieser Phase kommt es darauf an, unterschiedliche Netzbereiche gemeinsam zu verwalten, robuste Datenübertragung zu gewährleisten und diese gegen Angriffe zu schützen.

Teilszenario 1 – Zusammenstellen eines Hilfskonvois. Nach dem Erdbeben soll ein Konvoi Fahrzeuge einer humanitären Hilfsorganisation ins Katastrophengebiet eskortieren. Die militärischen Fahrzeuge sind untereinander mit militärischen Funktechnologien verbunden. Mit den Fahrzeugen der Hilfsorganisation besteht ebenfalls Funkverkehr, allerdings über zivile Technologien und strikt abgeschottet vom militärischen Funk, so dass es keine sicherheitskritischen Informationslecks gibt und der neutrale Status der Hilfsorganisation nicht kompromittiert wird.

Teilszenario 2 – Neue Verbände müssen integriert werden. Der Konvoi hat das Hauptquartier verlassen, unterwegs stoßen Fahrzeuge einer anderen Nation hinzu. Diese Fahrzeuge sind mit Funkgeräten ausgerüstet, die nicht kompatibel sind. Die beiden Teile des Konvois sollen ein so genanntes Ad-hoc-Netzwerk bilden, sich also spontan verbinden. Das Netz organisiert sich neu. Heute wird die Interoperabilität auf Funkebene durch den Austausch von Funkgeräten realisiert. Zukünftig ist eine gemeinsame Breitband-Wellenform (COALWNW) geplant, die in neuartige Funkgeräte, die als Software Defined Radios realisiert sind, geladen werden kann und für Interoperabilität sorgt. Eine entsprechende Liaison mit dem Projekt COALWNW ist geplant. Zusätzliche SOA-Dienste sollen automatisch erkannt werden, die Überwachung des Netzwerks stellt sich darauf ein.

Störsender voraus

Teilszenario 3 – Jammerangriff. Während der Fahrt wird plötzlich die Funkkommunikation gestört. Schuld ist ein Angriff mit einem Störsender, einem so genannten »Jammer«. Der Konvoi muss diesen Angriff erkennen und über die intakte Satellitenverbindung an das Hauptquartier melden. Um die Funkverbindung zu stabilisieren, wechseln die Teilnehmer des Konvois die Frequenz oder die Kodierung oder konfigurieren das Netz neu.

Teilszenario 4 – Reaktion auf den Jammer. Der Konvoi übermittelt Lageinformationen an das Hauptquartier. Das schickt Flugzeuge los, die den Jammer neutralisieren.

Das vollständige Szenario enthält noch weitere Elemente, etwa den Einsatz eines unbemannten Flugzeugs zum Aufspüren des Jammers. Diese Teilszenarien waren aber nicht Teil des Feldtests in Greding.

Herz von CoNSIS ist ein Konfigurationsmechanismus, der unterschiedliche Kommunikationstechnologien, Anwendungen, Netzwerkstrukturen und Sicherheitsbedürfnisse verwaltet. Es sorgt automatisch dafür, dass Verbindungen nicht unter Überlastung zusammenbrechen und erlaubt, Nutzer oder Daten je nach ihrer Rolle im Konvoi ein- oder auszuschließen, etwa wenn die Mitarbeiter der Hilfsorganisation keine militärisch Daten empfangen dürfen.

Wölfe in Bayern

Bisher war CoNSIS mehr Theorie als Praxis. Die beteiligten Nationen entwickeln Konzepte und Software für flexible Kommunikationsinfrastrukturen bei Einsätzen in Krisengebieten. Seit Sommer 2012 ist CoNSIS aber auch ein sehr praktisches Projekt. Bei der WTD81 in Greding spielten die Partner das CoNSIS-Szenario durch. Zehn »Wölfe« – kompakte Geländewagen der Bundeswehr – ausgerüstet mit Funkgeräten übten die Kommunikation in flexiblen Netzwerken. Fünf der Fahrzeuge waren mit deutscher und amerikanischer Funktechnik ausgerüstet, die anderen fünf mit Technik der Norweger. In einige Fahrzeuge wurden gemischte Varianten verbaut.

Diese gemischte Ausrüstung führte in der Vergangenheit immer wieder zu Problemen beim Datenaustausch. Dies betrifft insbesondere die koordinierte Nutzung unterschiedlicher Kommunikationstechnologien wie terrestrischer Funk und Satellitenkommunikation in einem gemeinsamen Ad-hoc-Netzwerk. Noch dazu beim mobilen Einsatz, wo die Netzwerke sich ständig neu konfigurieren müssen. Dank CoNSIS ist das nun anders. Alle Ziele wurden erreicht, etwa das automatische Auffinden eines Störsenders, der am Straßenrand aufgebaut war. »Der Zeitplan in den zwei Wochen war stramm«, sagt Christoph Barz, Teilprojektleiter von CoNSIS am FKIE. Zunächst unternahmen die Partner Teilexperimente, die beiden letzten Tage waren dann dem Gesamttest vorbehalten, bei dem auch Gäste des Bundesministeriums für Verteidigung anwesend waren.

Alle Teilnehmer werten CoNSIS als vollen Erfolg. Erkenntnisse daraus sollen in den künftigen mobilen Kommunikationsserver der Bundeswehr einfließen, den das Fraunhofer FKIE mitentwickelt.

Der Feldtest deckte aber auch auf, woran es noch hapert. So ist beispielsweise der technische Aufwand so hoch, dass die Stromversorgungen in den Fahrzeugen stark belastet werden. Die Motoren der Fahrzeuge mussten deshalb ständig laufen und Strom liefern. Die gewonnenen Erkenntnisse haben auch zu einem Anforderungskatalog für zukünftige Funksysteme geführt.

Peter Sevenich
Telefon +49 228 9435-317
peter.sevenich@fkie.fraunhofer.de

BAUM DER ERKENNTNIS

Welche Anforderungen muss ein neues IT-System erfüllen? Das zu überblicken, ist für Leiter von Ausrüstungsprojekten bei der Bundeswehr eine herausfordernde Aufgabe. Deshalb hat das Fraunhofer FKIE ein Modell entwickelt, das dabei hilft, die zahlreichen Anforderungen zu erfassen und gezielt in die Umsetzung in Projekten einbzubringen.

Ein Besprechungsraum in der Abteilung Informationstechnik für Führungssysteme des Fraunhofer FKIE in Wachtberg. Markus Esch rollt ein Poster im A1-Format auf dem Tisch aus. Trotz der Größe ist beim ersten Hinsehen kaum etwas darauf zu erkennen, nur hunderte Kästchen, die über viele Linien miteinander verbunden sind. Erst wenn sich das Auge an die kleine Schrift in den Kästchen gewöhnt hat, werden Begriffe wie »Informationssicherheit«, »Interoperabilität« oder »Standardisierung« erkennbar. »Das ist der Graph der Querschnittsanforderungen an die einsatzbezogenen IT-Systeme der Bundeswehr«, sagt Esch.

Der »Anforderungsgraph« ist beeindruckend umfangreich, man muss aber zunächst einmal in die Systematik hineinfinden. Markus Esch kennt diese Reaktion und erzählt, wie es zu diesem Projekt kam. Das ist Teil des Projekts Harmonisierung der Führungsinformationssysteme – auch HaFIS genannt –, mit dem die Bundeswehr die Vereinheitlichung ihrer Informations- und Kommunikationssysteme vorantreibt. Das ist eine wahre Sisyphosaufgabe, denn im Lauf der Jahrzehnte wurden für die Truppe zahlreiche Informationssysteme und Funkausrüstungen angeschafft, die es zu pflegen und betreiben gilt und die teilweise nicht vollständig aufeinander abgestimmt waren.

Die Bundeswehr ist da kein Einzelfall. Auch viele Unternehmen kämpfen mit einem Mix alter und neuer IT-Systeme, in Banken etwa arbeiten teilweise noch Systeme aus den Anfangszeiten der PC-Ära. Eine zu große Vielfalt heterogener Systemkomponenten erschwert die Konzeption und Erreichung zukunftsträchtiger Lösungen und natürlich auch das Einhalten verfügbarer Budgets. Daher will die Bundeswehr die Landschaft der Führungsinformationssysteme harmonisieren und setzt dabei auf die Expertise des Fraunhofer FKIE.

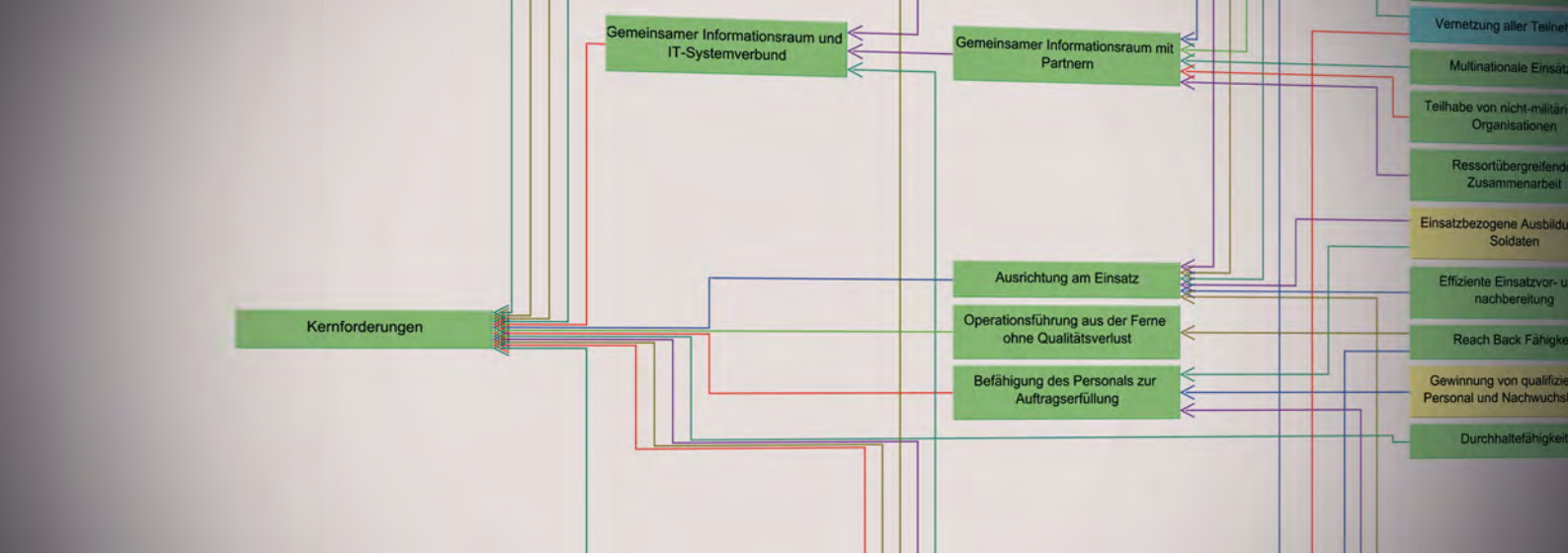
Nutzen wichtiger als Technik

Ein Aspekt, dem nach Einschätzung der Fraunhofer-Mitarbeiter zu wenig Beachtung geschenkt wird, sind die bisweilen nicht ausreichend klaren Anforderungen an die Eigenschaften eines IT-Systems. Oft wurden früher insbesondere funktionale Eigenschaften beachtet, während operativen Anforderungen weniger Beachtung geschenkt wurde. Hier setzt der Anforderungsgraph an: Er fasst die querschnittlichen Eigenschaften und Bedarfe zusammen, die die Bundeswehr von einem einsatzbezogenen IT-System erwartet und die für das korrekte Zusammenspiel aller IT-Systeme Grundvoraussetzung sind. Die Betonung liegt also nicht auf spezifischen Einzelforderungen, sondern auf den abstrahierten – eben querschnittlichen – Anforderungen, die für grundsätzlich mehrere Systeme relevant sind.

Der Anforderungsgraph ist aber nicht bloß eine Sammlung dieser Eigenschaften und Bedarfe. Bei näherem Hinsehen erkennt man auf dem Poster eine baumartige Graphstruktur, die alle Textkästchen miteinander verbindet. Denn technische Fähigkeiten und Lösungen sind immer verknüpft mit operationellen Anforderungen. So muss zum Beispiel eine Datenbank bestimmte Informationen gut dokumentieren, sie muss mit vielen Datenformaten zurechtkommen und sie muss interoperabel sein. Und sie muss dem Operateur einen Nutzen für seine Arbeit bringen.

Verkehrte Sichtweise

Der Anforderungsgraph geht über diese technischen Fähigkeiten hinaus, indem er systematisch auch die operationellen Fähigkeiten einbezieht. Ein IT-System ist schließlich kein Selbstzweck, sondern es muss Führungs- und Einsatzkräfte bei ihrem Auftrag möglichst gut unterstützen. Diese Sichtweise,



erst vom operationellen Nutzen zu denken und daraus auf technische Fähigkeiten, daraus auf technische Lösungen und daraus erst am Ende auf ein konkretes Produkt zu schließen, müsse zukünftig stärker ausgeprägt sein, hat Esch festgestellt. Dabei ist diese Sichtweise in vielen Dokumenten bereits angelegt, etwa in der IT-Strategie der Bundeswehr oder in Teilkonzeptionen. Allerdings nicht zusammenhängend und auf so vielen Seiten, dass es für Projektleiter schwer zu überblicken und umzusetzen ist. Der Anforderungsgraph enthält alle diese Aspekte in leicht verdaulicher Form. Dazu haben die Teammitglieder Hanna Geppert, Michael Gerz und Markus Esch zahlreiche Dokumente der Bundeswehr nach querschnittlichen Anforderungen an die einsatzbezogenen IT-Systeme durchforstet und diese systematisiert in ein Modell übersetzt. Das Poster auf dem Besprechungstisch ist der Ausdruck aller Elemente in diesem Modell.

Projektleiter, die zum Beispiel einen IT-Service für das harmonisierte Führungsinformationssystem beschaffen, bekommen dieses Poster allerdings nicht zu sehen. Sie arbeiten mit einer Software, die sie durch die Verknüpfungen des Graphen lotst – von der operationellen Anforderung bis zu den Eigenschaften des Produkts. Die Software blendet automatisch alle Eigenschaften aus, die für dieses Projekt unwichtig sind. Beim Ausdruck bleibt so ein übersichtlicher Graph von Anforderungen übrig.

Unterstützung für Projektleiter

Erst kürzlich hat das FKIE gemeinsam mit dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr mithilfe des Anforderungsgraphen ein konkretes Projekt durchgespielt. »Das hat sehr gut geklappt, auch wenn der Projektleiter anfangs etwas skeptisch war«, berichtet Esch. Dank des Anforderungsgraphen hätte er gemerkt, dass die bestehende Anforderungslage noch einiges Optimierungspotential hatte. Teilweise war nicht vollständig klar, welche Missionen eigentlich erfüllt werden sollte und manche Aspekte waren nicht ohne Widersprüche.

Das Ergebnis des Interviews kann den Projektleiter erheblich bei der Umsetzung des Projektes unterstützen, da alle relevanten Anforderungen herausgearbeitet wurden. Die gefundenen technischen Lösungen können als eine Art Blaupause für die Umsetzung des Entwicklungsauftrags dienen. Vom Erfolg ist Esch überzeugt: »Das wird die Tätigkeit der Projektleiter merklich beeinflussen und erleichtern.«

Beendet ist die Arbeit dennoch nicht. Als nächstes möchte das Team laufende und bereits abgeschlossene Projekte mit dem Anforderungsgraphen evaluieren. Eine große Chance, schließlich bietet es die Möglichkeit, eine Vielzahl von Einzelmaßnahmen auf ein gemeinsames Ziel auszurichten.

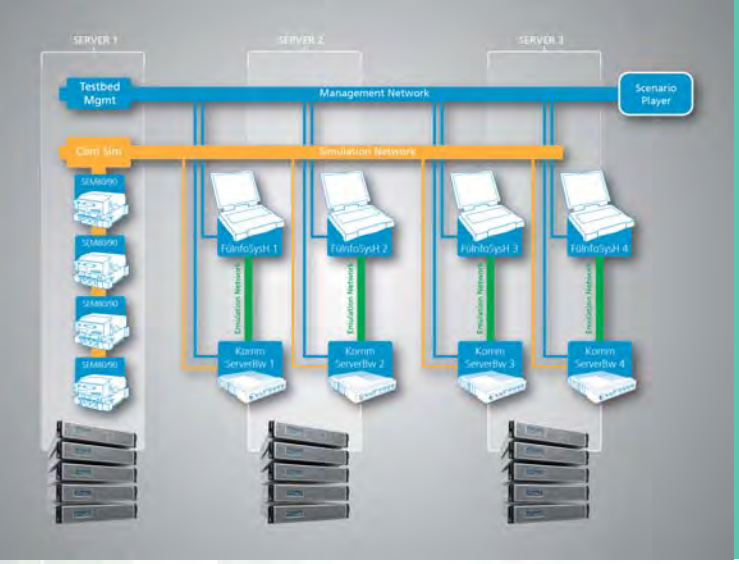
Dr. Markus Esch
Telefon +49 228 9435-421
markus.esch@fkie.fraunhofer.de

FELDTEST IM TESTBED

Ein Testsystem des Fraunhofer FKIE hilft Bundeswehr und Herstellern, ihre Funk- und Computerausrüstung auf Herz und Nieren zu prüfen, bevor sie in den Einsatz geht.

35 Grad im Schatten, die Hitze im Fahrzeug ist kaum zu ertragen, durch alle Ritzen dringt der Staub, der von der Straße aufgewirbelt wird. Die ist mit Schlaglöchern übersät und die Soldaten werden mächtig durchgerüttelt. Einsätze in Afghanistan sind eine enorme Belastungsprobe für Mensch und Material. Kommt es jetzt zu einem Angriff durch Talibankämpfer, muss trotzdem alles wie am Schnürchen klappen, insbesondere der Sprechfunk und Datenaustausch der Fahrzeugbesatzungen untereinander sowie mit der Einsatzzentrale im Camp.

Den Aufbau der Kommunikationsverbindung haben die Soldaten tausendmal geübt – in deutschen Kasernen, also in einer Umgebung, die längst nicht so hohe Anforderungen an Mensch und Material stellt. In Afghanistan ist alles anders: Nicht nur Hitze und Staub machen den



Vier virtualisierte Instanzen der IT-Ausstattung kommunizieren über ein emuliertes Funknetz.

Einsatzkräften zu schaffen, eine für militärische Zwecke nutzbare Kommunikationsinfrastruktur fehlt fast völlig. Die Bundeswehr muss deshalb die komplette Infrastruktur für Sprechfunk und Datenaustausch mitbringen. Funkverbindungen funktionieren meistens, aber nicht immer. Berge, die Funkverbindungen unterbrechen, Terroristen, die Sendestationen lahmlegen, machen die Kommunikation schwierig. Nicht alles lässt sich vorhersehen und üben.

Virtualisierung spart Ressourcen

Wie kann man solche Kommunikations- und Informations-Infrastrukturen verbessern, also gegen Ausfälle wappnen? Mit dieser Frage beschäftigt sich die Abteilung Informationstechnik für Führungssysteme des Fraunhofer FKIE. Eine Lösung wäre: Mehr Testen mit genau der gleichen Ausrüstung, wie sie auch in Afghanistan im Einsatz ist. Doch die Ressourcen sind knapp und es ist schwierig, die notwendigen Ausrüstungskomponenten für Tests verfügbar zu machen. Die Idee des FKIE: Man bildet die raren Kommunikations- und Informations-Systeme einfach im Rechner nach. Virtualisierung nennen das die Informatiker. In der IT-Branche ist Virtualisierung gang und gäbe, Rechner simulieren Infrastrukturen, die es eigentlich gar nicht gibt. Ein einfaches Beispiel, das viele kennen: Cloud Computing. Viele PC-Nutzer synchronisieren ihre Urlaubsbilder oder Termine zwischen PC, Tablet und Smartphone. Früher brauchte man dazu ein Kabel, heute läuft das übers Internet und Dienstleister, ohne dass sich der Kunde um die Hardware kümmern muss.

Die Virtualisierung beim FKIE geht weit darüber hinaus. Sie schafft eine Umgebung – ein so genanntes Testbed –, in dem die echte Software aus den Computern in den Einsatzfahrzeugen so läuft, als wäre sie tatsächlich im Einsatz. Bei Funkgeräten liegt der Fall etwas anders: Ihre Hardware ist so speziell, dass die Software nur auf dieser Hardware laufen kann. Deshalb wird die Virtualisierung durch einen Simulator ergänzt, der die Funktionen der Funkgeräte so wirklichkeitsnah wie möglich nachbildet. Dieser Simulator wurde über die Bundeswehr vom Hersteller des Funkgeräts zur Verfügung gestellt. Das Testbed ist skalierbar: 20 oder mehr Kommunikationsknoten beziehungsweise Fahrzeuge im Konvoi kann das Testbed nachbilden. Die Konfiguration für die Testläufe erfolgt weitgehend automatisiert.

Konvoi im Computer

Die Software im Testbed und der Simulator laufen in Echtzeit. Das heißt: Eine Testperson kann die Einrichtung so nutzen, wie sie es aus ihrem Fahrzeug kennt. Das geht so weit, dass hin und wieder auch absichtliche Fehler durchgespielt werden. Die Testumgebung bezieht zum Beispiel die Umwelt ein. Schlechtes Wetter oder eine hügelige Landschaft, die die Funkverbindung beeinträchtigen, kommen ebenso vor, wie ein Ausfall einer Sendestation, die von Gegnern zerstört wurde. Regelmäßig brechen Funkverbindungen zusammen, müssen Rechner neu gestartet oder neue Netzwerkknoten einbezogen werden, etwa wenn sich der Konvoi vergrößert. Außerdem bewegt sich der Konvoi – natürlich nicht wirklich, sondern virtuell, indem die Software im Testbed mit Daten aus der Satellitennavigation gespeist wird, die eine Bewegung des Fahrzeugkonvois vortäuschen.

Die Bundeswehr hat ihr Interesse an dem Testbed signalisiert und beabsichtigt, die entwickelten Technologien und Verfahren auch in eigenen Testeinrichtungen einzusetzen. Eine Idee des Fraunhofer FKIE ist, damit künftig neue Computer- und Funkausrüstung auf Herz und Nieren zu testen, bevor die Ausrüstung angeschafft wird. FKIE-Projektleiter Marc Spielmann: »Wir überlegen, unsere Testkapazitäten vernetzt in einem Testverbund der Bundeswehr bereitzustellen, damit Industrie und Bundeswehr sie ebenfalls nutzen können.«

Dr. Marc Spielmann
Telefon +49 228 9435-640
marc.spielmann@fkie.fraunhofer.de

Die Arbeit in der Operationszentrale der Korvette K130 wird durch moderne Computersysteme unterstützt.

FORSCHER AUF GROSSER FAHRT

Die neuen Fregatten der Marine sollen mit halber Besatzung fahren. Das Fraunhofer FKIE untersucht, wie sich der neue Schichtplan auf die Leistungsfähigkeit der Mannschaft auswirkt.

Effizienz liegt im Trend – das gilt in Unternehmen ebenso wie in öffentlichen Verwaltungen. Und das gilt zunehmend auch bei der Bundeswehr. Angesichts sinkender Truppenstärken und Sparauflagen muss auch das Militär Konzepte entwickeln, um mit weniger Personal eine gleichbleibende Leistungsfähigkeit zu gewährleisten. Ein Beispiel ist die im Bau befindliche neue Fregatte der Deutschen Marine. Die neuen Schiffe sind so ausgelegt, dass die Mannschaftsstärke im Vergleich zu eingerüsteten Schiffen ähnlichen Funktionsumfangs deutlich reduziert ist. Weil die Aufgaben an Bord aber nicht weniger, sondern zum Teil noch komplexer werden und sich die Besetzung pro Schicht nicht beliebig verringern lässt, hat die Marine ein neues Schichtsystem eingeführt. Statt Acht-Stunden-Schichten mit drei Schichtteams, soll die Besatzung auf den neuen Fregatten Sechs-Stunden-Schichten mit zwei Schichtteams schieben. Bei sechs Stunden Wache und sechs Stunden Pause ist die Besatzung also zwölf Stunden pro Tag im Einsatz, vier Stunden länger als bisher. Und das bis zu 21 Tage, bis es wieder für ein paar Tage in einen Hafen geht.

Auch bei der Marine gibt es Zweifel, ob diese Mehrbelastung nicht vielleicht zu einer geringeren Leistungsfähigkeit führt, die im Ernstfall – zum Beispiel wenn das Schiff angegriffen

wird – zu verzögerten und falschen Reaktionen führen könnte. Die Marine wollte es genauer wissen und beauftragte die Abteilung Ergonomie und Mensch-Maschine-Systeme des Fraunhofer FKIE mit einer Studie, die die Leistungsfähigkeit der Besatzung mit einem theoretischen Modell und mit praktischen Tests untersucht.

Simulierter Schlaf

Um ein Gefühl zu bekommen, wie sich die Leistung der Besatzung in dem geänderten Schichtkonzept ändern könnte, setzte das Team eine Simulationssoftware ein, die ursprünglich für die U.S. Air Force entwickelt wurde. Diese wollte wissen, wie die Leistungsfähigkeit der Besatzung von Langstreckenbombern schwankt, die bis zu 36 Stunden in der Luft sein können. Das Simulationsmodell basiert auf Erkenntnissen der Schlafforschung und dem circadianen Rhythmus, der unsere Hochs und Tiefs im Lauf des Tages bestimmt. So sind die meisten Menschen vormittags besonders leistungsfähig, danach folgt eine Delle nach dem Mittagessen, zum späten Abend sinkt die Leistung dann deutlich ab, um sich im Schlaf zu erholen. Deutlich niedriger als 90 Prozent sollte die kognitive Leistungsfähigkeit jedoch bei der Arbeit nicht fallen. Liegt der Wert bei 77 Prozent, entspricht dies der Leistungsfähigkeit bei einem Blutalkoholgehalt von 0,5 Promille, bei dem eine Bedienung von komplexen und sicherheitskritischen Apparaten bereits eingeschränkt ist.

Das Team fütterte die Simulation mit dem neuen Schichtmodell der Marine. Ergebnis: Die Besatzung erreicht laut Modellierung nicht während der gesamten Arbeitszeit eine gute kognitive Leistungsfähigkeit von mindestens 90 Prozent. Die Leistungsfähigkeit sinkt innerhalb der ersten Tage deutlich ab, um sich dann in Folge des Gewöhnungseffekts auf niedrigem Niveau einzupendeln, allerdings nicht auf dem Niveau eines Dreier-Schichtmodells. Bei längeren Ausfahrten bis zu drei Wochen ist also damit zu rechnen, dass die Müdigkeit der Besatzung steigt und die Leistungsfähigkeit sinkt. Besonders kritisch: Laut Modell steigt das Risiko, für Sekunden kurz einzunicken, um 41 Prozent gegenüber einem ausgeruhten Menschen.

Mit der Korvette auf die Kanaren

Doch das ist Theorie, ein Simulationsmodell bildet die Realität nie vollständig ab. Deshalb unternahmen die FKIE-Mitarbeiter eine Messkampagne und zwar im richtigen Einsatz: Sven Fuchs, wissenschaftlicher Mitarbeiter in dem Projekt, fuhr mit Kollegen auf der Korvette »Ludwigshafen am Rhein«. Die neuntägige Reise führte von Recife in Brasilien nach Las Palmas auf den Kanarischen Inseln. Die nagelneue »Ludwigshafen am Rhein« ist eine von fünf neuen Korvetten, die die Marine gerade für küstennahe Einsätze etwa zur Überwachung von Seeblockaden anschafft. Das Schiff ist kleiner als die im Bau befindlichen Fregatten, der Schichtbetrieb und die Arbeitsbelastung sind aber vergleichbar. Etwa ein Drittel der Besatzung nahm an der Untersuchung teil, gleichmäßig verteilt auf die zwei Schichtteams.

Das FKIE-Team brachte eine ganze Wagenladung Ausrüstung mit: 12 Computer wurden im Hangar des Schiffes aufgebaut. Vor und nach jeder Schicht musste die Wachmannschaft an den Computern einen Test absolvieren. Die Software dazu stammt ebenfalls aus den USA. Sie wurde ursprünglich für die Weltraumbehörde NASA entwickelt, die damit die Leistungsfähigkeit von Astronauten während einer bemannten Marsmission überwachen möchte, die länger als ein Jahr dauern wird. Die Tests, die wie Computerspiele aufgemacht sind, bestimmen unter anderem das Reaktionsvermögen und kognitive Leistungen wie Merkfähigkeit und räumliches Denkvermögen, funktionieren also ähnlich wie die Tests, die Bewerber etwa zur Pilotenausbildung absolvieren müssen. Die Tests dauerten pro Messzeitpunkt nur eine Viertelstunde, um die ohnehin knapp bemessenen Ruhezeiten nicht weiter zu verkürzen und die Ergebnisse nicht zu verfälschen.

Korvette »Ludwigshafen am Rhein« bei voller Fahrt.

Künstliche Wachmacher

Allein auf die Tests am Computer wollten sich die Experten vom FKIE aber nicht verlassen. Deshalb mussten die Probanden regelmäßig Fragebögen ausfüllen, wo sie über ihr Allgemeinbefinden, Müdigkeit und die gefühlte Belastung Auskunft gaben. Auch nach Kaffee- und Nikotinkonsum oder der Einnahme von Medikamenten wurde gefragt. Solche Aspekte sind interessant, weil das o.a. Simulationsmodell darauf nicht eingeht. Das Modell berücksichtigt weder die Art und Dauer der Arbeit noch den Konsum von Kaffee oder Energy-Drinks, sondern orientiert sich allein an einem idealisierten Schlaf-Wach-Rhythmus.

Eines können aber auch die Fragebögen nicht erfassen: Wie lange schlafen die Probanden wirklich und wie erholsam ist dieser Schlaf? Die Fragebögen geben nur Auskunft, wann eine Person ins Bett gegangen und wann sie aufgestanden ist. Die eigentliche Schlafdauer kann aber viel kürzer sein. »In einer sechsstündigen Schichtpause sind maximal vier Stunden Schlaf realistisch«, sagt Sven Fuchs. Und selbst da gibt es große Unterschiede. Während sich manche Probanden in jeder freien Minute auch in der Schichtpause am Tag aufs Ohr legten, schliefen andere grundsätzlich nur nachts. Um die tatsächliche Schlafdauer zu erfassen, trug jede Testperson einen Aktigraphen, ein Armband, das die Bewegungen der Versuchsteilnehmer aufzeichnet und daraus ableitet, ob diese aktiv waren, nur geruht oder tatsächlich geschlafen haben. Sven Fuchs ergänzt: »So können wir genau sehen, wie lange die Leute zum Einschlafen brauchen und wie oft sie in der Nacht aufgewacht sind, auch wenn sie sich vielleicht nicht mehr bewusst daran erinnern.«

Auch wenn die Auswertung noch nicht vollständig abgeschlossen ist, so lassen sich doch schon Trends erkennen und Empfehlungen ableiten. Eine Empfehlung betrifft die Dauer eines Schichtplans. Um die Mannschaft möglichst

Das papierlose Schiff

Das papierlose Büro wird seit vielen Jahren propagiert, Realität wurde es bis heute nicht. Noch länger wird es beim papierlosen Schiff dauern. Gibt es auf den Fregatten der Marine ein Ereignis, das gemeldet werden muss – zum Beispiel ein Schaden am Schiff – wird das über eine Sprechstelle gemeldet, dort auf eine Tafel geschrieben, weiter gemeldet, wieder aufgeschrieben und so weiter: Bis zu sechs Schritte durchläuft jede Meldung bis zum verantwortlichen Offizier und dann wieder sechs Schritte zurück bis zu der Person, die die Instandsetzung ausführt. Dokumentiert wird jeweils mit Fettstift und laminierten Tabellen oder Schiffsplänen. »Das ist ineffizient«, findet Sven Fuchs von der Abteilung Ergonomie und Mensch-Maschine-Systeme des Fraunhofer FKIE. Er möchte wichtige Informationen gern sofort schiffsweit verfügbar machen. Dafür hat die Abteilung im Auftrag der Marine ein Konzept entwickelt, das mit Tabletcomputern arbeitet. »Damit lässt sich der Kommunikationsaufwand auf die Hälfte reduzieren«, verspricht der Medieninformatiker. Das innovative Konzept wird traditionelle Kommunikationswege aber nicht vollständig ersetzen, weil die Marine auf Redundanz setzt. Auch im Falle eines Stromausfalls muss die Kommunikation funktionieren – zur Not mit den guten alten Kurbeltelefonen.

gleich und gerecht zu behandeln, tauschen viele Kommandanten die Schichten, teilweise rotieren die Wachen täglich. Die Wach- und Ruhephasen verschieben sich also in dem geplanten Schichtmodell der Marine um sechs Stunden. Aus wissenschaftlicher Sicht ist das aber ungünstig. Dank des Gewöhnungseffekts passt sich der Organismus bis zu einem gewissen Maß auch an einen anstrengenden Schichtplan an. Tauscht man die Schichten oft, fällt der Gewöhnungseffekt weg und die Mannschaft kämpft mit zusätzlicher Müdigkeit.

8-4-4-8 besser als 6-6-6-6

Ob diese Erkenntnis der Wissenschaft berücksichtigt wird, hängt immer vom Kommandanten ab. Der entscheidet auch, ob ein ganz anderes Schichtmodell als der Sechs-Stunden- oder der Acht-Stunden-Rhythmus eingeführt wird. Theoretisch gibt es 168 Möglichkeiten, wie man Schichtarbeit im Zweiwachenbetrieb organisieren kann, alle wurden vom FKIE in der Simulation nachgebildet. Eine ist das 7-5-5-7-Modell mit sieben Stunden Wache, fünf Stunden Ruhe, fünf Stunden Wache und sieben Stunden Ruhe. Das 8-4-4-8-Modell mit einem Wachwechsel um 1 Uhr nachts hat sich in den Simulationen als das Schichtmodell empfohlen, das den Organismus am wenigsten belastet und über einen längeren Zeitraum die höchste Leistungsfähigkeit sichert. Das Sekundenschlafrisiko ist zudem nur minimal. Das System hat den Vorteil, dass es an jedem Tag eine achtstündige Ruhepause gibt, die dem Organismus genug Zeit lässt, sich zu erholen. Eine längere ununterbrochene Schlafphase hat einen deutlich höheren Erholungseffekt als mehrere kürzere Schlafpausen, das hat die Schlafforschung eindeutig ergeben. Die kanadische Marine hat dieses Schichtmodell erprobt und gute Erfahrungen damit gemacht.

Solche Schichtmodelle erfordern allerdings eine ganz neue Organisation auf dem Schiff. Während einer Acht-Stunden-Wache muss die Mannschaft eine Mahlzeit zu sich nehmen, kann dazu aber nicht eigens in die Kantine gehen. Das bedeutet, dass eine Zwischenmahlzeit an den Arbeitsplatz gebracht werden müsste. Auch für das Reinschiff machen, also den Putzdienst an Bord, müsste es neue Regelungen geben.

Doch hier begibt sich das Team um Annette Kaster auf unbekanntes Terrain. »Um praktikable Verbesserungsvorschläge machen zu können, mussten wir zunächst den Alltag an Bord besser kennenlernen«, sagt die Leiterin der Forschungsgruppe Mensch-Maschine-Systemtechnik. In einer Folgestudie möchte das Team dann testen, ob das 8-4-4-8-Modell tatsächlich besser ist und wie die organisatorischen Änderungen umgesetzt werden könnten. Grundsätzlich denken die FKIE-Experten in alle Richtungen. Am Ende könnte eine Empfehlung auch lauten, dass die Besatzung der neuen Fregatten zu knapp bemessen ist und dass vielleicht ein paar Personen mehr nötig sind, die als Springer fungieren, wenn ihre Kameraden während der Wache kurz zum Essen gehen. Kaster: »Ob das dann umgesetzt wird, ist allerdings die Entscheidung der Marine.«

Dipl.-Ing. Annette Kaster, M.Sc.
Telefon +49 228 9435-492
annette.kaster@fkie.fraunhofer.de

Trotz des hohen Automationsgrads bleiben auch auf modernsten Einheiten viele Aufgaben an Bord »Handarbeit«.

MIT SMARTPHONE AUF PATROUILLE

Der Soldat kommuniziert bereits heute mit modernster Technik. Damit er nicht von der komplexen Bedienung überfordert wird, erforschen und testen Ergonomie-Experten des Fraunhofer FKIE neue Benutzungskonzepte.

Der Einsatz von Ein- und Ausgabegeräten wie Smartphones oder HMDs kann in der Virtuellen Umgebung unter kontrollierten Bedingungen beurteilt und optimiert werden.

Gut, dass das Fraunhofer FKIE in Wachtberg so bekannt ist. Sonst hätten sich einige Anwohner bestimmt sehr gewundert, als im letzten Sommer mehrere Personen mit merkwürdigen Apparaturen auf dem Kopf, einem Smartphone und verschiedenen Kabeln am Körper vor dem Institut unterwegs waren und dabei konzentriert Eingaben tippten. Hier wurden jedoch keine Machenschaften geplant. Das Auf- und Abgehen auf einer abgemessenen Strecke diente allein der Wissenschaft und dem Soldaten bei seinen zukünftigen Einsätzen.

Die Bundeswehr betreibt aktuell entsprechende Entwicklungen eines Modernisierungsprogramms, bei dem der einzelne Soldat in typischen Einsätzen, bspw. bei Patrouillen und Aufklärungseinsätzen, durch innovative IKT-Technologien unterstützt wird. Der Soldat wird unterschiedliche technische Ausrüstungskomponenten mit sich führen, um zu navigieren, die Lage zu erfassen oder sich mit Kameraden und dem Hauptquartier in Verbindung zu setzen. Dies geschieht sowohl per Sprechfunk als auch mittels des Austauschs digitaler Lagedaten. Erste Beispiele dieser Ausrüstung werden bereits eingesetzt.

Tippen bei Patrouille und Überwachung

Die tragbaren Systeme werden künftig komplexer gestaltet sein und mehr Funktionen bieten. Die Kehrseite ist, dass ihre Bedienung damit komplexer wird. Damit der Soldat seine persönliche IT-Ausrüstung auch dann noch schnell, sicher und zuverlässig bedienen kann, wenn er voll ausgestattet im Einsatz unterwegs ist, muss die Ergonomie stimmen. Denn jeder weiß: Schon beim langsamen Gehen oder in der ruckelnden Straßenbahn tippt man auf dem Handy häufiger daneben. Das ist dort unproblematisch – für den Soldat kann es aber über Leben und Tod entscheiden.

Deshalb die Untersuchungen vor dem FKIE in Wachtberg. Sie sind Teil mehrerer Forschungsprojekte der Abteilung Ergonomie und Mensch-Maschine-Systeme. Sie sollen klären, welche Informationen eine Person unter Belastung erfassen kann und wie Benutzungsschnittstellen von mobilen Eingabegeräten aussehen müssen, damit die Person sie möglichst zuverlässig bedienen kann. Bei den eingangs genannten Versuchen liefen beispielsweise Versuchsteilnehmer mit unterschiedlichem Tempo und gaben Informationen in ein Smartphone ein.

Das war aber nur ein Teil des umfangreichen Versuchsprogramms, das die Versuchsteilnehmer absolvierten. »2012 haben wir fast 250 Teststunden mit 80 Personen durchgeführt«, sagt Jessica Conradi, die Leiterin eines Projekts im Versuchsprogramm. Viel Zeit verwendeten die Ergonomie-Experten für die Frage, wie man ein Smartphone am besten bedient, um möglichst wenig Fehler bei der Eingabe zu machen und die Belastung möglichst gering zu halten.

Finger, Daumen oder Spielecontroller?

Ein Smartphone kann man nämlich auf verschiedene Weise bedienen:

- mit zwei Händen: Eine Hand hält das Smartphone, die Finger der anderen Hand tippen. Das ist die meistverwendete Bedienvariante;
- mit einer Hand: Das Smartphone liegt auf der Handfläche und der Daumen tippt auf das Display. Diese Bedienvariante ist nur etwas für Personen mit großen Händen und/oder kleinen Smartphones;
- mit Arm und Hand: Das Smartphone wird wie eine Uhr mit einem Band am Arm befestigt. Jogger nutzen so etwas beispielsweise, um den Musikplayer zu fixieren. Getippt wird mit der Hand am anderen Arm.

Innovativ ist eine vierte Eingabemethode, die noch weiterentwickelt wird: Als Display dient eine Datenbrille, ein so genanntes Head-Mounted-Display, das die Anzeige ins

Teilnehmer bei der Durchführung einer Versuchsaufgabe in einer Virtuellen Umgebung.

rechte Auge spiegelt. Als Eingabegerät dient ein Controller, wie er für gängige Spielekonsolen verwendet wird.

Vor den Versuchen im Freien wurde ein aufwändiges Experiment in einem Labor der Abteilung Ergonomie und Mensch-Maschine-Systeme durchgeführt. In einem abgedunkelten Raum steht ein Laufband vor einer großen Leinwand und Lautsprecher sorgen für eine realistische Geräuschkulisse. Die Leinwand zeigt Szenen eines virtuellen Dorfes, durch das der Teilnehmer geht, während er Informationen am Smartphone lesen und seine Antworten eingeben muss. Das Gehtempo ist variabel.

Datenbrille erweist sich als vielversprechend

Positiv: Alle vier Eingabemethoden sind generell geeignet für die Nutzung sowohl beim Stehen als auch beim Gehen. Doch es gibt Unterschiede: Bei der Bedienung des Smartphones mit zwei Händen passieren wenige Fehler, die körperliche Belastung ist relativ gering. Auch bei der Bedienung mit einer Hand und Daumen kommt es zu wenigen Fehlern, die muskuläre Belastung liegt aber etwas höher. Am höchsten ist die Gefahr von Fehlhaltungen, die zu muskulären Verspannungen führen können, bei der Befestigung des Smartphones am Arm. Die geringste körperliche Belastung hatten die Testpersonen mit der Datenbrille, in Verbindung mit dem Spielecontroller erfolgte die Eingabe auch sehr schnell, allerdings lagen die Fehlerhäufigkeit und damit die Zahl der Korrekturen höher. Dass die Variante mit der Datenbrille so gut abschnitt, liege daran, dass man die Tasten bei dem Spielecontroller – im Gegensatz zu einem Smartphone – fühlen kann, vermutet Jessica Conradi.

Welche Eingabemethode letztlich für die Ausrüstung des Soldaten die beste ist, kommt besonders auf die Rahmenbedingungen des Einsatzes an. Hier gilt es, die passende Variante für die geforderte Aufgabe zu finden. So kann es durchaus sein, dass der Soldat mehrere Eingabemethoden zur Wahl hat, je nachdem welche Situation er gerade bewältigen muss.

Das Testprogramm hat aber auch eindeutig kritische Ergebnisse gebracht, vor allem was die Sehschärfe betrifft. Weil die Auflösung der Smartphone-Displays immer höher und das Gerät, sowie die Schrift immer kleiner werden, sind Informationen vor allem beim Gehen häufig nur schwer aufzunehmen. Das FKIE-Team hat dazu einen mobilen Sehtest mit Landoltringen entwickelt, wie ihn jeder vom Sehtest bei der Führerscheinprüfung kennt: kleine Ringe mit einer Öffnung, deren Orientierung der Versuchsteilnehmer dem Zifferblatt einer Uhr zuordnen muss. Untersucht wurde die maximale Sehleistung wieder bei verschiedenen Geschwindigkeiten.

Beim Gehen ist die Schrift häufig zu klein gewählt

Die Vermutung bewahrheitete sich: Durch die schwankende Kopf- und Handbewegung beim Gehen nimmt die Sehleistung stark ab. Beim schnellen Gehen mit fünf Kilometern pro Stunde müssen Zeichen bis zu 43 Prozent größer dargestellt werden als beim Stehen. Das bestätigte sich bei einem zweiten Test, bei dem die Wörter in unterschiedlichen Schriftgrößen angezeigt wurden.
Die schlechteren Sehleistungen bei Bewegung haben Konsequenzen für die Größe von Schrift und Symbolen künftiger Displays und Eingabegeräte für Soldaten. Die

Messung der muskulären Ermüdung und der Bewegung des Hand-Arm-Systems bei einem Versuch zur Nutzung von Tablet-PCs.

Zeichen werden größer, was aber auch die gleichzeitig darstellbare Informationsmenge reduziert. Das Team arbeitet deshalb an Verfahren, um die Datenmenge automatisch zu verringern. Eine Option wäre ein adaptives Display, das die Schrift vergrößert, entweder auf Veranlassung des Benutzers oder teilautomatisch.

Welche Informationen in einer bestimmten Situation notwendig sind und welche man weglassen kann, ist ebenfalls eine Frage, mit der sich das FKIE beschäftigt. So nahm ein Kollege des Ergonomie-Teams an einer Übung teil, bei der die Bundeswehr den Häuserkampf in einem Dorf durchspielte. Resultat ist ein Baumdiagramm, das die einzelnen Handlungen etwa beim Stürmen eines Gebäudes detailliert aufschlüsselt und Informationsengpässe aufdeckt. Ein Beispiel: Wenn zwei Teams unterwegs sind, müssen die Soldaten wissen, ob die Personen hinter einer Tür zum anderen Team gehören oder ob sie feindliche Kämpfer sind. Wenn die Soldaten ein Display hätten, auf dem die eigene Position und die des zweiten Teams markiert wären, würde das möglicherweise fatale Fehlentscheidungen verhindern.

Davon könnten auch Polizei und Feuerwehr profitieren. Auch sie brauchen Informationen, wer oder was sich wo in einem Haus befindet. »Wir sind mit Polizei und Feuerwehr im Gespräch und es gibt großes Interesse an unseren Arbeiten«, sagt Thomas Alexander, Leiter der Forschungsgruppe Human Factors am FKIE. Leider erlaubten deren knappe Finanzmittel häufig nicht die Durchführung eigener Schwerpunktprojekte.

Balanceakt mit Tablet

Noch ganz am Anfang stehen die Arbeiten der Forschungsgruppe Human Factors bei Untersuchungen zur muskulären Ermüdung beim Einsatz von Tabletcomputern im Gehen oder Stehen. Das Team hat die Aktivität der Muskeln von Versuchsteilnehmern mittels Elektromyographie gemessen, einer Methode, um die elektrische Aktivität in Muskeln zu bestimmen. Ist der Einsatz eines Tablet-PCs auf Dauer ungesund? »Das ist noch nicht ganz klar«, sagt Thomas Alexander nach der ersten Auswertung der bisherigen Daten. Ein Physiotherapeut unterstützt das Team nun, um diese Frage zu klären.

Der Anblick von Versuchen, die vor dem FKIE im Freien durchgeführt werden, bleibt den Nachbarn in Zukunft aber vermutlich erst einmal erspart. Ein erfreuliches Ergebnis des Programms war nämlich, dass es zwischen dem Test auf dem Laufband in einer virtuellen Umgebung und demselben Test im Freien keine signifikanten Unterschiede gibt.

Der Trend zur Brille

Datenbrillen – so genannte Head-Mounted Displays – sind schon seit vielen Jahren auf dem Markt, durchgesetzt haben sie sich aber noch nicht. Zu unbequem und zu teuer, finden viele. Das könnte sich mit kommerziellen Datenbrillen, die für einen Massenmarkt ausgelegt sind und derzeit die Marktreife erlangen, ändern. Damit wird das Thema auch für die Industrie interessanter. Zahlreiche Firmen vor allem aus der Automobil- und Flugzeugindustrie experimentieren schon lange mit Augmented Reality. Hier blenden Datenbrillen Informationen ein, die eine Person etwa beim Einbau eines Bauteils in ein Auto unterstützen. Der Blick und die Hände bleiben dadurch frei.

Doch die Datenbrillen könnten zu Verspannungen der Nackenmuskulatur und zu einer höheren Beanspruchung der Augen führen, vermutet die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin BAuA. Sie hat die Abteilung Ergonomie und Mensch-Maschine-Systeme des Fraunhofer FKIE gebeten, das genauer zu untersuchen. Die Bundesanstalt möchte Empfehlungen für den Einsatz der Datenbrillen aussprechen. Auch hier gab es 2012 am FKIE erste Tests »Allerdings ist es derzeit noch zu früh, um eindeutige Aussagen zu treffen.«, so Thomas Alexander, Leiter der Forschungsgruppe. »Bis zum Ende unserer größeren Versuchsreihe müssen wir leider noch warten«.

NICHT MEHR LESBAR

Thomas Alexander, Leiter der Forschungsgruppe Human Factors am Fraunhofer FKIE, über den Trend zu Displays mit immer höherer Auflösung und Googles Datenbrille.

Sind Retina-Displays auf mobilen Smartphones wie iPhone und Android-Systemen sinnvoll?

Die Auflösung dieser Displays liegt mittlerweile bereits über der visuell möglichen Auflösung des Auges. Das bringt keinen Nutzen mehr. Im Gegenteil: Mit höherer Auflösung wird häufig auch die Schrift immer kleiner, viele, besonders ältere Personen, können das gar nicht mehr lesen.

Was sagen die Entwickler von Smartphone-Herstellern dazu?

Die Entwickler dort interessieren sich sehr für unsere Arbeiten. Wir treffen uns auf Konferenzen und sind im Gespräch.

Ist das Halten eines Tabletcomputers ungesund?

Vor allem beim Gehen ist die Beanspruchung hoch, weil man ständig das Gewicht balancieren und die Bewegungen ausgleichen muss, damit Informationen noch lesbar und Eingaben noch möglich sind. Man merkt es bei kurzer Benutzung kaum, aber wir können das messen, indem wir die Aktivität der Muskeln bestimmen. Deshalb sind verschiedene Institutionen auch kritisch, was den Einsatz von Tablets in der Industrie angeht.

Und was sagen die Arbeitsmediziner zu den Datenbrillen, die demnächst auf den Markt kommt?

Sie streben Regeln an, etwa wie lange man so eine Datenbrille bei der Arbeit tragen darf. Der Vorteil ist, dass man bei der Arbeit die Hände frei hat, aber bereits nach vier Stunden könnten schon Verspannungen auftreten. Bisher haben wir natürlich größere und schwerere Head Mounted Displays getestet, da die leichte Datenbrillen derzeit erst verfügbar werden, und der Marktstart auf 2014 verschoben wurde. Wir werden aber sicher mit die ersten sein, die sich Datenbrillen besorgen und ausprobieren.

Jessica Conradi
Telefon +49 228 9435-472
jessica.conradi@fkie.fraunhofer.de

WÄRME WEIST DEN WEG

Wie erkennt ein Roboter Personen? Am besten durch eine Kombination mehrerer Algorithmen, sagt FKIE-Experte Achim Königs.

80 Prozent: So hoch ist die Erkennungsrate eines Algorithmus zu Personenerkennung, den die Forschungsgruppe Unbemannte Systeme entwickelt hat. So stand es im Jahresbericht 2011 des Fraunhofer FKIE. Berichtet wurde von einem Teilprojekt im Forschungsprojekt ARMINIUS (Assistenzfunktionen für Teilautonomie in mobilen unbemannten Systemen). Wissenschaftlicher Mitarbeiter Achim Königs von der Forschungsgruppe hat darin eine Software entwickelt, die Personen in Videobildern anhand von Merkmalen wie Körpermaßen oder Kleidung erkennt und verfolgt. Das soll eines Tages Roboter befähigen, hinter Soldaten herzufahren und ihre Ausrüstung zu transportieren. 80 Prozent, das ist für einen Roboter gut, für diese Aufgabe aber nicht gut genug. Vor allem im Wald, wenn Bäume den Algorithmus verwirren, verliert das Vehikel Personen aus dem Blickfeld. »Hier könnten Wärmebildkameras helfen, die Mensch und Hintergrund auseinanderhalten«, vermutete Achim Königs damals.

Diese Vermutung wurde 2012 überprüft. Königs hat eine weitere Variante der Personendetektion entwickelt, die mit Wärmebildern arbeitet. Die Idee ist eigentlich nicht neu, hat aber ihre Tücken. Denn die Annahme, dass Personen immer wärmer sind als ihre Umgebung und dass sie damit im Bild als heller Fleck vor dunklem Hintergrund erscheinen, stimmt nur für Aufnahmen in Gebäuden. Außerhalb von Gebäuden, wenn die Sonne scheint, heben sich Personen kaum vom Hintergrund ab, zum Teil erscheinen heiße Oberflächen etwa von Autos oder Mauern heller als Personen. Ein Algorithmus, der auf eine Entweder-Oder-Entscheidung setzt – Person=heiß, Hintergrund=kalt – liefert deshalb im Freien ungeeignete Erkennungsraten. Das hat Achim Königs in Experimenten nachgewiesen.

Thermalbild von drei Personen in einem Waldgebiet.

Möglicher Einsatz: Roboter als »helfende Hand«. Hier im Bereich Lager- und Material-Logistik.

Weniger Erkennungsfehler bei Erschütterungen

Königs verfolgt deshalb eine andere Strategie – eine Strategie, die er schon 2010 verwendet hat, damals allerdings für Bilder, die mit einer herkömmlichen Videokamera aufgenommen wurden. Der Algorithmus nutzt „Implicit Shape Models" (ISM), also eine Sammlung typischer Gestaltmerkmale. Er hat hohe Erkennungsraten, auch wenn Personen durcheinanderlaufen und sich zeitweise verdecken, ebenso bei schlechter Beleuchtung und außerhalb von Gebäuden. Nachteil dieser Methode: Sie benötigt ein Bewegungsmodell, schätzt also ständig, wohin eine Person voraussichtlich gehen wird. Das ist ungünstig, wenn die Bilder von einer Kamera auf einem Roboter stammen, der im Gelände über Stock und Stein holpert und verwackelte Bilder aufnimmt. Dann ist nämlich nicht immer klar, ob sich gerade die Person bewegt oder der Roboter. Deshalb hat Königs 2011 die bereits erwähnte Personenverfolgung ohne Bewegungsmodell entwickelt, die sich allein auf Merkmale von Person und Kleidung verlässt.

Doch mit der Erweiterung um Wärmebilder kommt nun auch wieder die alte ISM-Methode zum Einsatz. Sie erkennt Personen anhand von Kantenmerkmalen. Das funktioniert sowohl für herkömmliche Videoaufnahmen als auch für Wärmebilder. Der Algorithmus sucht also nicht mehr nur nach heißen oder kalten Bildbereichen. Der Clou: Dem Algorithmus ist es damit egal, ob er mit Bildern aus einer normalen Videokamera gefüttert wird oder mit Bildern aus einer Wärmebildkamera. Beide Videoströme lassen sich also prima kombinieren.

Aber steigert das auch die Erkennungsrate? »Ja, und zwar deutlich«, sagt Achim Königs. Er hat Tests mit Datensätzen unternommen, die einmal im Gebäude und ein andermal im Freien bei Temperaturen von 15 beziehungsweise 25 Grad Celsius aufgezeichnet wurden. Diese Daten fütterte er sowohl jedem der Algorithmen allein als auch in Kombinationen von Video- und Wärmebilderkennung über den ISM-Algorithmus – insgesamt prüfte der FKIE-Forscher acht Varianten von Erkennungsalgorithmen.

20 Prozent bessere Erkennungsrate

Die Ergebnisse entsprechen Königs Erwartungen. Wärmebilder allein sind im Freien nicht der Weisheit letzter Schluss, sobald die Sonne scheint. Kombiniert man sie aber mit den Videobildern über den ISM-Algorithmus, steigt die Erkennungsrate um bis zu 20 Prozent, sie liegt dann bei über 90 Prozent. Vor allem reduziert die Hinzunahme der Wärmebilder die Fälle, wo Personen erkannt werden, die gar nicht da sind. Ein Erkennungsplus gibt es auch beim Einsatz im Wald. Im Wärmebild erscheinen Bäume als homogener, kalter, dunkler Hintergrund, vor dem sich warme Personen deutlich abheben.

Neues Jahr, neue Ideen: Als nächstes möchte Achim Königs untersuchen, ob sich die Wärmebilder auch eignen, Personen zu unterscheiden. Das leistet eigentlich der Algorithmus, den Königs 2011 entwickelt hat, doch auch hier könnte die Kombination die Erkennungsrate steigern. Jeder Person würde zusätzlich zu den bis zu 60 Körpermerkmalen noch eine Temperatursignatur zugeordnet. Außerdem arbeitet der Algorithmus derzeit nur mit dem aktuellen Bild, das gerade von der Kamera kommt. Vorteil: Erschütterungen des Roboters spielen keine Rolle. Nachteil: Die Bewegungsrichtung von Personen wird ignoriert, was dazu führen kann, das der Algorithmus von einer Person zur anderen springt. Helfen würde, wenn die Software Bilder der letzten Sekunden speichern und sich die Veränderung der Position von Personen relativ zum Roboter merken würde. Achim Königs: »Dazu greife ich auf die Kompetenz in der Abteilung Sensordatenfusion des FKIE zurück.«

Achim Königs
Telefon +49 228 9435-751
achim.koenigs@fkie.fraunhofer.de

ROUTENPLANUNG FÜR ROBOTER

Sicher von A nach B: Eine Software des Fraunhofer FKIE lotst Roboter durch unwegsames Gelände.

Zentimeter für Zentimeter tastet sich der Marsroboter Curiosity vorwärts. Wo das Gelände eben ist und eine geringe Gefahr besteht, dass der Roboter umkippt, darf das Vehikel fahren. Korrekturen sind schwierig – die Latenz der benötigen Befehle vom Kontrollzentrum auf der Erde zum roten Planeten ist hoch. Ein Überschlag würde den Totalverlust der teuren Mission bedeuten.

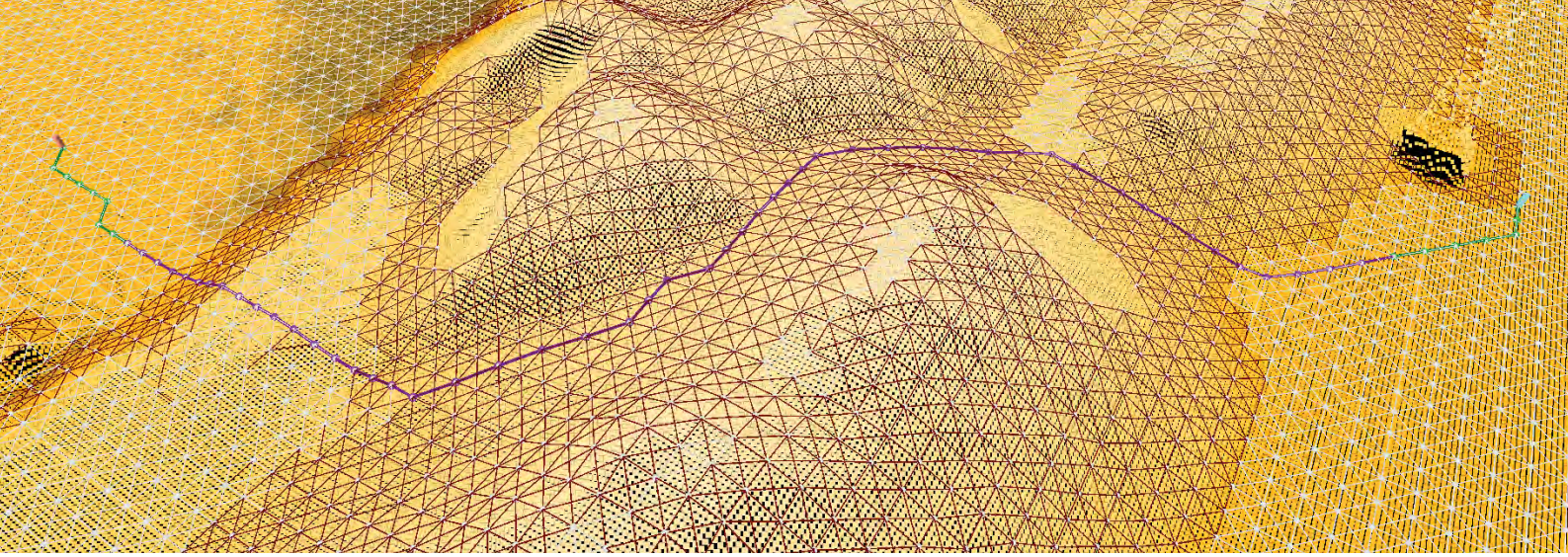
Beim Einsatz von Robotern auf der Erde kann ein umgekipptes Vehikel geborgen werden, zumindest theoretisch. Denn wenn der Roboter über das Gelände eines havarierten Atomreaktors fährt oder Soldaten im Gefecht Ausrüstung hinterherfahren soll, ist auch hier eine Bergung schwierig und mit großer Gefahr verbunden. Für beide Einsatzszenarien ist es also besser, der Roboter fährt eine Route, die ihn sicher von A nach B bringt.

Michael Brunner von der Forschungsgruppe Unbemannte Systeme des Fraunhofer FKIE beschäftigt sich in seiner Promotion mit der Frage, wie ein autonomer Roboter diese sichere Route bestimmen kann. Einfach ist das nicht und häufig nutzen Konstrukteure eine Methode, die auf Nummer Sicher geht. Sie vermessen das Gelände aus der Luft dreidimensional und suchen eine Route, die nur Steigungen oder Stufen enthält, die das Fahrzeug gefahrlos überwinden kann.

Nach einer Katastrophe sucht der Roboter in einer Gebäuderuine nach Opfern.

Die Abbildung zeigt den Bewegungsgraphen und einen bereits in Segmente zerlegten vorläufigen Pfad.

Der Telemax Roboter während der Fahrt über den Schotterhügel.



Mit Flippern über Stock und Stein

Ein Beispiel ist der Telemax-Roboter. Er hat vier Räder und zusätzlich vier so genannte Flipper, das sind keilförmige Raupen. Die Flipper verleihen dem Gefährt eine gute Geländegängigkeit, sogar Treppenstufen überwindet es. Dazu schwenkt Telemax jeden seiner vier Flipper in jede beliebige Position. Allerdings macht das auch die Routenplanung komplizierter. Normale Verfahren der autonomen Routenplanung berücksichtigen diese Beweglichkeit nicht, sie arbeiten zudem nach dem Prinzip Entweder-Oder. Überschreitet ein Höhenunterschied einen bestimmten Wert, sucht sich das Fahrzeug eine andere Route – selbst wenn die Stufe nur wenige Zentimeter zu hoch ist und der Telemax sie mit seinen Flipperraupen bewältigen könnte.

Michael Brunner hat sich deshalb ein neues Konzept für die Routenplanung ausgedacht. Seine Arbeit ist Teil des ARMINIUS-Projekts (Assistenzfunktionen für Teilautonomie in mobilen unbemannten Systemen) der Arbeitsgruppe »Unbemannte Systeme« des Fraunhofer FKIE. In dem Konzept müssen Hindernisse nicht vor der Fahrt explizit identifiziert werden, ebenso setzt es keine vordefinierten Bewegungen für bestimmte Hindernisse voraus.

Die Routenplanung erfolgt in mehreren Stufen: In der ersten Stufe erstellt die Software eine Risikoanalyse auf Basis der Karte. Je größer der Höhenunterschied zwischen zwei Zellen ist, umso riskanter ist es für den Roboter, hier zu fahren. Mit dieser Risikokarte errechnet die Software im zweiten Schritt einen vorläufigen Pfad, den der Roboter auf jeden Fall sicher befahren kann, wo dieser also weder umkippt noch die Haftung am Hang verliert. In der dritten Planungsphase verfeinert die Software diesen Pfad und berechnet die Stellung der Flipper. Weil dieser Schritt komplex und rechenintensiv ist, erfolgt er nur an den Stellen des Pfades, wo es für den Roboter kritisch werden könnte und wo er die Flipper verstellen muss, um vorwärts zu kommen. Brunner arbeitet bereits an einer verfeinerten Routenplanung, die auch scharfe Kanten etwa an Mauern oder Treppen berücksichtigt. Dazu hat der FKIE-Experte einen Algorithmus entwickelt, der die Routenplanung anhand einer Menge zufällig bestimmter Wegpunkte ermittelt.

Sicher über den Schotterhügel

Brunners Konzept hat mehrere Vorteile. Es ist für verschiedene Roboter einsetzbar, weil die Risikoanalyse und die Bewertung der Lage des Roboters unabhängig vom Modell sind. Der Operateur hat zudem immer im Blick, welchem Risiko er den Roboter aussetzt und wie lange das Vehikel für die geplante Route unterwegs sein soll. Mehr Bewegungen der Flipper bedeuten in der Regel ein höheres Sicherheitsniveau, aber auch eine längere Fahrzeit. Was das in der Praxis bedeutet, hat Michael Brunner auf einem großen Schotterhügel untersucht. Der Telemax-Roboter brauchte für die autonome Fahrt über Stock und Stein etwa zwei Minuten, die Planung dauerte deutlich weniger als eine Minute.

In der Regel erfolgen solche Fahrten aber teleoperiert, also ferngesteuert. Das ist heute Stand der Technik, etwa wenn Roboter nach einem Erdbeben oder nach einem Unfall wie im Atomkraftwerk Fukushima zwischen den Trümmern unterwegs sind. »Die Technik ist oft noch nicht so weit, dass Roboter das autonom bewältigen«, sagt Michael Brunner. Die Routenplanung aus dem FKIE wäre aber auch für die Operateure dieser ferngesteuerten Fahrzeuge nützlich, sie schlägt vor, welche Route die sicherste ist.

Michael Brunner
Telefon +49 228 9435-427
michael.brunner@fkie.fraunhofer.de

ROUTINGPOLIZEI IM RECHNER

Die Forschungsgruppe Cyber Defense des Fraunhofer FKIE entwickelt Methoden, um Manipulationen beim Datenverkehr im Internet auf die Schliche zu kommen.

Welche Route führt am kürzesten von A nach B? Navigationsgeräte im Auto beantworten diese Frage in Sekunden. Wenn irgendwo ein Stau ist, sucht das Navi automatisch eine Umleitung. Im Internet ist das ganz ähnlich. Damit Datenpakete, etwa eines Videos, ihren Weg von einem Rechner in den USA auf den PC in Deutschland finden, hangeln sie sich von einem Rechnerknoten im Internet zum nächsten und wenn einer ausfällt, springt ein anderer ein. Welche Route die Daten nehmen, ist für den Betrachter des Videos egal, Hauptsache es geht schnell und das Bild ruckelt nicht.

Sicherheitsexperten ist das nicht egal. Das so genannte Routing ist ein potenzielles Angriffsziel für Cyberkriminelle. Sie nutzen aus, dass die Strecken der Daten von A nach B nicht ein für alle Mal festgelegt sind, sondern sich ständig ändern und Daten im Internet meistens nicht den kürzesten Weg nehmen. Das hat bizarre Folgen: So kann es vorkommen, dass Videos, die von einem Anbieter in den USA zu einem Nutzer ebenfalls in den USA gespielt werden, über Netzknoten in einem anderen Landübermittelt werden. Bei einem Video ist das wahrscheinlich egal, handelt es sich aber um sensible Unternehmensinformationen, können Angreifer das für Industriespionage ausnutzen. Es kann aber auch zu massiven Ausfällen führen. Als die Pakistan Telecom vor einiger Zeit innerhalb des eigenen Netzes alle Youtube-Inhalte sperrte, brachen viele Verbindungen zusammen, weil die Konfiguration zur Sperrung versehentlich an andere Internet-Teilnehmer weitergereicht wurde und so große Teile des Youtube-Datenverkehrs im asiatischen Raum Internet Routen nach Pakistan nahmen, wo sie ins Leere liefen.

Viele Wege nach Rom

Beim Routing im Internet gibt es kein Richtig oder Falsch. Über welche Knoten ein Datenpaket läuft, entscheiden die Knoten selbst anhand von Routingtabellen. Darin steht, welche Nachbarn verfügbar sind. Dabei gibt es unzählige Möglichkeiten, so wie viele Wege nach Rom beziehungsweise von A nach B führen. Die Tabellen sind nicht statisch, sondern passen sich ständig an. Damit sind sie leicht zu manipulieren und schwierig zu kontrollieren.

»Eine Routingpolizei gibt es leider nicht«, klagt Matthias Wübbeling, wissenschaftlicher Mitarbeiter am Fraunhofer FKIE. Eine Prüfung, die das Routing auf Plausibilität testet und erkennt, wenn Datenströme zu Spionagezwecken umgeleitet werden, gibt es ebenso wenig. Dafür gibt es aber die Forschungsgruppe Cyber Defense am Fraunhofer FKIE. Die beschäftigt sich mit der Frage, ob und wie man Manipulationen von Routingtabellen zuverlässig erkennen und verhindern kann. In dem vom BMBF geförderten Projekt MonIKA (Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung) entwickeln die FKIE-Experten im Teilprojekt EvA (Erkennung von Anomalien) Verfahren, um angebotene Routen der Netzknoten zu klassifizieren und falschen Routen auf die Schliche zu kommen.

Doppelgänger im Netz

Anomalien können zum Beispiel Konflikte sein, wenn mehrere Netzknoten sich als ein und derselbe Endpunkt ausgeben, etwa wenn plötzlich zwei Knoten behaupten, derselbe Anbieter zu sein. Oder wenn ein Knoten vorgibt, eine schnellere Verbindung etwa zu einem E-Mail-Anbieter zu haben. Das kann sein, wenn der Betreiber des Knotens eine Geschäftsbeziehung zu diesem Anbieter unterhält, es kann aber auch ein Schwindel sein, um Informationen abzugreifen. Verdächtig ist, wenn regelmäßig dieselben Adressbereiche betroffen sind.

Das Problem: Das Internet ist kein monolithisches Konstrukt, sondern ein loser Verbund von sogenannten Autonomen Systemen. Jeder Betreiber von Internet-Knoten oder Teilnetzen hat eine andere Sicht auf das Internet. Blickt ein Netzbetreiber wie zum Beispiel die Deutsche Telekom auf sein eigenes Netz, können die Routen der Datenströme darin

plausibel erscheinen. Aus der Vogelperspektive des gesamten Netzes betrachtet, können die Routen aber Anomalien enthalten, die auf eine Manipulation hindeuten. »An diesem Problem haben sich schon viele Wissenschaftler die Zähne ausgebissen«, sagt Michael Meier vom Fraunhofer FKIE. So haben sich Konzepte, das Routing mittels Signaturen – versteckten »Stempeln« in den Datenpaketen – sicherer zu machen, nicht durchgesetzt. Mangels Erfolg haben viele Experten das Thema Routingmanipulation ad acta gelegt. »Aber wir holen es wieder auf den Schirm«, sagt Meier, der auch Professor für IT-Sicherheit an der Universität Bonn ist.

Sein Team hat sich einen neuen Ansatz ausgedacht. Die Idee: Routing-Anomalien lassen sich nur aufspüren, wenn die Netzbetreiber kooperieren und ihre Daten austauschen. Doch das wollen und dürfen sie zum Teil nicht, so dass alle bisherigen Versuche gescheitert sind. Denn die Informationen können personenbezogene Informationen von Kunden enthalten, und somit dem Datenschutz unterliegen. Ziel von MonIKA ist deshalb ein Software-Rahmenwerk, das nur solche Informationen berücksichtigt, die für das Aufspüren von Routingmanipulationen notwendig sind. Netzbetreiber wie die Deutsche Telekom und Konkurrent Vodafone könnten dann Netzwerkdaten bereitstellen, in denen das Fraunhofer FKIE Anomalien finden und klassifizieren kann. Auch Botnetze, gekaperte Rechner, über die Cyber-Kriminelle Spam-Mails verschicken, lassen sich zum Teil damit aufspüren.

Juristisch wasserdicht

Die MonIKA-Partner entwickeln derzeit eine Werkzeugbibliothek für Unternehmen der Internetbranche. In den Daten werden personenbezogene Informationen durch Pseudonyme ersetzt. Eine vollständige Anonymisierung ist nicht möglich, weil die Analyse sonst Angriffe nicht erkennen würde. Um nicht an den Bedürfnissen der Netzbetreiber vorbei zu entwickeln und eine juristisch wasserdichte Lösung zu erzielen, haben sich die FKIE-Forscher Expertise anderer Disziplinen gesichert. So ist mit der EADS Tochter Cassidian Cybersecurity ein Industrievertreter ebenso im Boot, wie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und die zivilrechtliche Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster, die sich mit dem Thema Haftung befasst.

Eile ist geboten. Mit der Einführung des neuen Internet-Protokolls 6 werden die Adressen, die den Datenpaketen ihr Ziel zuordnen, deutlich länger. Damit steigt die Anzahl der Routen und Cyberkriminelle haben es noch leichter, Manipulationen zu verschleiern.

Prof. Dr. Michael Meier
Telefon +49 228 73 54-249
michael.meier@fkie.fraunhofer.de

QUARANTÄNE FÜR DIGITALE QUÄLGEISTER

Die Forschungsgruppe Cyber Defense des Fraunhofer FKIE rückt Viren, Trojanischen Pferden und Botnetzen mit trickreichen Analysemethode zu Leibe.

Früher waren Berichte über Computerviren Nischenthemen in Fachmedien. Warum sollte man auch groß darüber berichten? Wer sich einen Virus oder ein Trojanisches Pferd einfängt, ist doch selbst schuld. Man öffnet schließlich nicht Dateianhänge von E-Mails eines unbekannten Absenders. Das hat sich geändert: Berichte über Viren und Hackerangriffe schaffen es mittlerweile in die 20-Uhr-Nachrichten. Betroffen sind nämlich nicht mehr nur Surfer, die »ausversehen« Sexseiten anschauen, sondern Konzerne wie Microsoft oder Facebook. In den letzten Monaten häuften sich Berichte von Angriffen auf die Datenbanken großer US-Konzerne. Ziel der Attacken: Informationen über Strategien und Produkte abzugreifen, Industriespionage also. Wer vermutlich dahinter steckt, erörterte jüngst ein Report eines US-Beratungsunternehmens. Die Berater hatten die Angriffe auf große US-Konzerne bis in ein Gebäude in Shanghai zurückverfolgt. Dort würden Hacker arbeiten, die auf Veranlassung der chinesischen Regierung Industriespionage betrieben, behauptet der Report.

Der Bericht mag zwar schockieren – er untertreibt jedoch noch. Denn Hackerangriffe sind keineswegs nur ein Problem großer US-Unternehmen, die auf staatlichen Befehl ausspioniert werden. Betroffen ist jeder fünfte PC weltweit – vielleicht also auch Ihrer, ohne dass Sie es wissen. Wer Rechner von Privatpersonen kapert, interessiert sich vielleicht für Kreditkartendaten oder Homebanking-PINs, viel wahrscheinlicher ist allerdings, dass der Rechner Teil eines so genannten Botnetzes ist. Das sind mächtige Netzwerke von Computern, die mit einem Trojanischen Pferd infiziert und dann vom Botmaster ohne das Wissen der Besitzer ferngesteuert werden. Der Botmaster nutzt die geballte Rechenkraft tausender Computer, um massenhaft Spam-E-Mails zu verschicken. Das kostet praktisch nichts und macht die Botmaster reich. Laut Symantec, einem Anbieter von Antiviren-Software, richtete Schadsoftware 2011 Schäden von 388 Milliarden Euro an. Konsequenzen müssen die Cyber-Kriminellen kaum fürchten. Eine wirkungsvolle Strafverfolgung gibt es kaum, auch Deutschland tut sich schwer mit der Anwendung von Gesetzen, die den Kriminellen die Geschäftsgrundlage entziehen und mit Gefängnisstrafen abschrecken sollen.

Dreifach-Strategie gegen Cyber-Kriminelle

Das heißt nicht, dass Behörden und Wissenschaftler dem Problem machtlos gegenüberstehen. In den letzten Jahren hat die Cyber-Abwehr deutliche technische Fortschritte gemacht und auch personell aufgerüstet. Wie auch am Fraunhofer FKIE. Gemeinsam mit der Abteilung für Kommunikation und Vernetzte Systeme der Universität Bonn untersuchen Wissenschaftler der Forschungsgruppe Cyber Defense des FKIE die Methoden der Angreifer und entwickeln Gegenmaßnahmen. Die Experten haben drei Strategien entwickelt, um Angreifer in die Zange zu nehmen:

- **Honeynet:** Damit sind Rechner gemeint, die Schadsoftware anlocken, indem sie Angreifern ein vermeintlich leicht zu kaperndes Opfer vorgaukeln. In Wirklichkeit wird die Schadsoftware im »Honigtopf« abgekapselt und untersucht, um der Angriffsstrategie auf die Schliche zu kommen.

- **Digitale Forensik:** Hier entwickelt die Forschungsgruppe Verfahren für das Auswerten von Datenträgern, Speicherinhalten und Netzwerkdaten, um herausfinden zu können, was bei Vorfällen passiert ist.

- **BOTMAN®:** Die »BOTnet and Malware Analysis« ist der Schwerpunkt der Forschungsgruppe. Hier werden systematisch Botnetze und Malware analysiert. Eigens zu diesem Zweck hat das Team ein spezielles Labor eingerichtet. Hier arbeiten zwar keine Personen in Schutzkleidung unter Quarantänebedingungen, denn die Viren und Schädlinge, die hier untersucht werden, existieren rein digital, können also nicht in die Luft ent-

wischen. Dennoch ist der Vergleich gar nicht so abwegig, denn auch in diesem Labor wird Schadsoftware von der Außenwelt abgekapselt und so untersucht, dass sie keinen Schaden anrichten kann.

Aufwendiges Reverse-Engineering

Die Analyse von Schadsoftware kann statisch oder dynamisch erfolgen. Das BOTMAN-Labor erlaubt es, anhand eines systematischen Prozesses mehreren Wissenschaftlern parallel und kooperativ beide Ansätze zu nutzen. Bei der statischen Analyse sezieren die FKIE-Experten den Programmcode der Schadsoftware. Die enthält den Programmablauf allerdings nicht in einer lesbaren Programmiersprache, sondern in Maschinencode. Das Reverse-Engineering, bei dem aus den Nullen und Einsen des Maschinencodes die Programmfunktionen rekonstruiert werden, ist darum sehr aufwendig, zum Teil ist es auch Handarbeit. Komplexe Schadsoftware hat mitunter 1000 Funktionen und mehr, die unter anderem die Verschlüsselung oder das Kommunikationsprotokoll steuern. »Im Prinzip können wir alles herausfinden, aber bei komplexen Exemplaren erfordert das einiges an Zeit«, sagt Elmar Gerhards-Padilla, der Leiter des Teams zur Analyse und Bekämpfung von Schadsoftware.

Um das Reverse-Engineering zu beschleunigen, hat die Forschungsgruppe IDAscope entwickelt, ein Erweiterungsmodul für die kommerzielle Software IDA Pro, die unter Experten weit verbreitet ist. IDAscope erleichtert unter anderem die Zuordnung der Funktionen des Programms zu bestimmten Kategorien wie Dateizugriff, Netzwerk oder Verschlüsselung. Der Analyst muss dank IDAscope viel weniger Stellen im Programmcode von Hand untersuchen.

Gelingt das Reverse-Engineering, liefert es detaillierte Informationen zur Schadsoftware. Manchmal gelingt es, aus diesen Merkmalen Infektionsmarker abzuleiten, also im Programmcode versteckte Abfragen, mit denen die Schadsoftware feststellt, ob ein Computer bereits befallen ist. Falls ja, wird die Schadsoftware nicht ausgeführt, um den Kommunikationsaufwand gering zu halten. Das kann man für eine Impfung nutzen, indem man der Schadsoftware vorgaukelt, sie sei bereits früher schon installiert worden.

Labor für Botnetze

Manchmal entpackt sich die Schadsoftware aber erst zur Laufzeit. Dann ist sie nicht vorab mittels statischer Analyse zu untersuchen. Dann hilft die dynamische Analyse, bei der die Schadsoftware in Aktion beobachtet wird, der Virus wird sozusagen zum Leben erweckt. Darüber lassen sich weitere wichtige Erkenntnisse gewinnen, zum Beispiel über Speicher- und Registerinhalte sowie den Netzwerkverkehr.

Allerdings nur hochgesichert, so dass der Schädling nicht aus den Rechnern des BOTMAN-Labors entwischen kann. Die Schadsoftware, die auf den PCs der FKIE-Mitarbeiter ruht, wird von dort auf einen so genannten Hop-Rechner geschoben, eine Art demilitarisierte Zone, die wie ein undurchdringliches Tor wirkt. Von dort gelangt der Schädling ins eigentliche Labor. Geriete er dort außer Kontrolle, könnte er trotzdem über den Hop-Rechner nicht zurückgelangen, eine direkte Verbindung zum Internet hat das BOTMAN-Labor nämlich nicht.

Das Labor ist wie eine Spielwiese, auf der die FKIE-Experten Gegenmaßnahmen ausprobieren können. Diese Spielwiese ist sehr flexibel, das heißt, die vernetzten Rechner können automatisiert zu beliebigen virtuellen Netzwerken verbunden werden. So wird der Schadsoftware mal ein riesiges Konglomerat aus weltweit verstreuten PCs vorgegaukelt, ein andermal ein paar PCs in einem mittelständischen Unternehmen, wo ein Mitarbeiter ahnungslos einen verseuchten USB-Stick eingeschleppt hat. Dank der virtuellen Rechner lässt sich das Verhalten von Schadsoftware in einer Umgebung testen, die größer scheint, als sie tatsächlich ist.

Die Falle schnappt nicht immer zu

Das funktioniert aber nicht immer. Manche Schadsoftware verhält sich anders, je nachdem, ob sie auf virtuellen Rechnern ausgeführt wird oder nicht. Nicht alle Schädlinge fallen auf die Köder herein, die ihnen die FKIE-Arbeitsgruppe vorsetzt. Doch die Mitarbeiter wissen auch darauf eine Antwort. Mitunter helfen einfache Eingriffe in die Programmbefehle, um die Schadsoftware zur Mitarbeit zu zwingen. Wenn das nicht hilft, lässt man sie auf nicht virtualisierten Computern laufen – die Experten nennen das Bare-Metal-Rechner, also Rechner, die nicht vorgeben, etwas anderes zu sein als sie sind.

An Nachschub an Schadsoftware mangelt es nicht. Seit 2005 ist die Zahl neuer Malware-Varianten geradezu explodiert, auf rund 17 Millionen im Jahr 2011, sagt das AV-Test-Institut. Die Arbeitsgruppe am FKIE bedient sich aus verschiedenen Quellen, etwa aus eigens eingerichteten Virenarchiven oder aus dem Fundus der Anbieter von Antivirensoftware. »Wir bekommen mehr Beispiele für Schadsoftware, als uns lieb ist«, sagt Gerhards-Padilla.

Auch Beispiele für Botnetze findet man leicht. Beispielsweise durch Hinweise des Bundesamts für Sicherheit in der Informationstechnik, von Organisationen wie Shadowserver oder von Herstellern von Antiviren-Software. Auch dem Honeynet des FKIE gehen öfter Botnetze in die Falle. Taucht ein neues Botnetz auf, rekonstruieren die Analysten zunächst den Infektionsweg. Häufig wird die Botsoftware durch eine Datei eingeschleppt, zum Beispiel ein PDF, die die eigentliche Schadsoftware von einem anderen Rechner nachlädt.

Kontrollierte Selbstzerstörung

Die Schadsoftware ist analysiert, der Infektionsweg bekannt – was dann? Um den Schädling loszuwerden, könnte man die infizierten Rechner impfen, indem man Updates aufspielt, die dem Schädling befehlen: Zerstöre dich selbst. Doch das ist illegal, wenn es ohne das Wissen des Besitzers passiert. Denn juristisch gesehen ist eine (eigentlich sinnvolle) Desinfektionsmaßnahme genauso ein Eingriff in die Selbstbestimmung des Nutzers über seinen Rechner wie der Virus. Theoretisch könnte eine ferngesteuerte Desinfektion eines befallenen Rechners auch ungewollte Kollateralschäden auslösen.

Ohne das Einverständnis des Nutzers geht es also nicht. Informieren und Hilfe beim Aufräumen und Desinfizieren des PCs anbieten, ist deshalb der bessere Weg. Softwareanbieter, Behörden und Medien appellieren seit langem unisono, dass jeder PC einen Virenschutz braucht. Doch allen Appellen zum Trotz lassen viele Käufer eines neuen PCs die meist vorinstallierte Testversion des Virenscanners nach den 30 kostenlosen Tagen auslaufen. Wo die sanfte Methode nicht hilft, hält Elmar Gerhards-Padilla drastischere Maßnahmen für möglich: »Der Internetanbieter könnte den Kunden darauf hinweisen, dass sein Computer infiziert ist und dann den Zugang ins Netz so lange beschränken, bis der Computer wieder viren- und botnetzfrei ist.«

Auch die Politik muss sich bewegen und für eine bessere Durchsetzung der Strafverfolgung sorgen. Derzeit ist das Risiko für Botnetzbetreiber, erwischt zu werden, zu gering. Dieses Risiko müsse steigen, mahnt Gerhards-Padilla, damit die enormen Gewinne nicht mehr so leicht zu erwirtschaften seien. Auch wenn das Bundeskriminalamt ab und zu

Rechner beschlagnahmt, so muss irgendjemand die Daten auswerten und das dauert oft Monate – wenn überhaupt genug Fachpersonal vorhanden ist. Die Experten des BOTMAN-Labors arbeiten deshalb eng mit den Strafverfolgungsbehörden zusammen, um den Druck auf die Kriminellen zu erhöhen.

EU zieht an einem Strang

Das hat aber nur Erfolgschancen, wenn alle an einem Strang ziehen, auch international. Die Aussichten auf EU-Ebene stehen gut. Denn im Gegensatz zu vielen strittigen Themen in der Gemeinschaft sind sich beim Thema Cyber-Kriminalität alle Mitgliedsstaaten einig, dass etwas getan werden muss – schließlich sind alle mehr oder weniger betroffen. Geplant ist eine Behörde, die alle Kompetenzen zur Bekämpfung von Botnetzen in der EU – also auch die Kompetenzen des Fraunhofer FKIE – bündelt und den anderen Mitgliedern zur Verfügung stellt. Vorbereitet wird dies in dem Projekt ACDC (Advanced Cyber Defense Center), das von der Europäische Union gefördert wird. ACDC soll eine zentrale Datenbank erstellen, in der das ganze Wissen über das Verhalten von Schadsoftware enthalten ist. Rund 40 Partner aus 14 Ländern sollen dafür eine länderübergreifende Strategie entwerfen und bei den Ländern, die noch nicht dabei sind, die Werbetrommel rühren. Mit von der Partie sind Forschungsinstitute wie das FKIE, aber auch Firmen wie Microsoft und Polizeibehörden wie Europol oder das Landeskriminalamt Baden-Württemberg.

Deutschland hat einiges in die Partnerschaft einzubringen. So betreibt das Bundesamt für Sicherheit in der Informationstechnik die Webseite Botfrei.de, auf der die Behörde Informationen bereitstellt, wie man sich vor Botnetzen schützen und diese im Notfall entfernen kann. Diese Informationsplattform soll auf EU-Ebene in ACDC übernommen werden.

Trotz des gemeinsamen Interesses an einer wirksamen Cyber-Abwehr ist der EU-Plan kein Selbstläufer. 2015 läuft ACDC aus, »das ist ein kritischer Zeitpunkt«, sagt Elmar Gerhards-Padilla. »Bis dahin muss es ein tragfähiges Weiterführungsmodell geben, damit die Beteiligten nicht das Interesse verlieren.«

Dr. Elmar Gerhards-Padilla
Telefon +49 228 73 54-227
elmar.gerhards-padilla@fkie.fraunhofer.de

ZUKUNFT - SICHERHEIT - BONN

2012 fand die Future Security erstmals in Bonn statt – mit einer beeindruckenden Themenpalette und zufriedenen Teilnehmern und Ausstellern. Viele Medien berichteten über die Konferenz – vor allem über das Thema Internetsicherheit.

Die »Future Security« ist für Sicherheitsexperten ein Fixpunkt im Jahreskalender. Nationale und internationale Fachleute treffen sich, um über Bedrohungen der öffentlichen Sicherheit zu diskutieren und wie man diesen begegnen kann. Veranstaltet wurde die Konferenz vom Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung im Jahr 2012 zum siebten Mal. Waren die Jahre davor die Fraunhofer-Kollegen anderer Institute federführend für die Veranstaltung, so war im vergangenen Jahr zum ersten Mal das Fraunhofer FKIE Gastgeber. Das World Conference Center Bonn mit dem ehemaligen Plenarsaal des Deutschen Bundestages war ein würdiger Rahmen für die 360 Teilnehmer aus 18 Nationen.

Ein Blick ins Tagungsprogramm zeigt: Nie war das Themenspektrum einer Future Security vielfältiger. Neben vielen exzellenten wissenschaftlichen Vorträgen waren es vor allem die Diskussionsrunden mit namhaften Sicherheitsexperten, die über den Tellerrand einzelner technischer Entwicklungen hinausschauten und Sicherheitsrisiken ganzheitlich als Bedrohung für Freiheit und Demokratie diskutierten. »Ohne Sicherheit gibt es keine Freiheit«, sagte Professor Peter Martini, Institutsleiter des Fraunhofer FKIE und gemeinsam mit Professor Klaus Thoma, dem Vorsitzenden des Fraunhofer Verbunds, Gastgeber der Konferenz. Professor Wolf-Dieter Lukas, Abteilungsleiter im Bundesministerium für Bildung und Forschung, ergänzte: »Sicherheit bedeutet auch soziale Sicherheit.« Auch Stéphane Beemelmans, Staatsekretär im Bundesministerium der Verteidigung, hob hervor, dass die Gewährleistung von Schutz eine zentrale Aufgabe der Politik und eine gemeinsame Herausforderung für alle staatlichen Akteure sei. Sicherheit sei aber keine Konstante: »Dem Fortschritt im Schlechten muss der Fortschritt im Guten entgegengestellt werden.«


Fraunhofer
VVS

Ballungsräume müssen widerstandsfähiger werden

Bis 2050 werden rund 70 Prozent der Weltbevölkerung in Städten leben – eine enorme Herausforderung für Mobilität, Energieversorgung, Kommunikation und Gesundheitsversorgung. Weil Vernetzung der Infrastrukturen zunimmt, haben kleine Störungen große Auswirkungen. Fällt zum Beispiel das Internet aus, würde das auch Ausfälle des intelligenten Stromnetzes nach sich ziehen – mit gravierenden Auswirkungen auf alle Bereiche des Lebens vom Kochen und Heizen bis hin zur Einsatzfähigkeit von Polizei und Feuerwehr.

Damit dies nicht passiert, arbeiten Wissenschaftler, Stadtplaner, Politiker und Architekten an der Vision einer sicheren Stadt. Schon bei der Planung von Stadtquartieren wollen die Experten potentielle Schwachstellen entdecken und kritische Bauwerke wie Kraftwerke, Flughäfen oder Kliniken schützen und die Kommunikation aufrecht erhalten.

Cyber-Sicherheit im Fokus der Öffentlichkeit

Besondere Aufmerksamkeit erfuhr das Thema Cyber-Security, dem das Konferenzprogramm mehrere Vorträge einräumte. Das Fraunhofer FKIE hat eine eigene Forschungsgruppe und möchte verstärkt auf Themen wie Internetsicherheit aufmerksam machen. Die Konferenz hat eines ihrer Ziele erreicht: Die Öffentlichkeit dafür zu sensibilisieren, dass Attacken von Schadsoftware jeden treffen können. Denn hier lockt das große Geld: Statt wie früher Computer nur aus Spaß zu kapern, würden Hacker heute vor allem aus Profitsucht arbeiten, warnte Richard Kemmerer von der University of California in Santa Barbara, der die Konferenz mit seinem Vortrag eröffnete.

Im Konferenzprogramm finden sich aktuelle Themen wie Datensicherheit, Datenschutz, rechtliche Aspekte bei Cloud Computing, Internetkriminalität und Wirtschaftsspionage sowie IT-Krisenmanagement. So beschäftigte sich der Bundesdatenschutzbeauftragte Peter Schaar im Panel »Cloud and Law« unter anderem mit Risiken, rechtlichen Fragen, Datenschutz und Datensicherheit des Cloud Computing.

Auch in den Pausen herrschte reges Treiben im Foyer. Dort präsentierten ein Dutzend Aussteller Exponate und Forschungsprojekte zu den Konferenzinhalten, darunter Fraunhofer-Institute, die TU Ilmenau, EADS Deutschland oder T-Systems International. Eine Etage höher zeigte eine Posterausstellung neueste Forschungsergebnisse.

Lob von allen Seiten

Teilnehmer und Veranstalter waren hoch zufrieden mit der Future Security 2012. »Wir haben großes Lob bekommen von hochrangigen Vertretern aus Bundes- und Landesministerien, aus Unternehmen und von den vielen weiteren Tagungsteilnehmern«, so FKIE-Institutsleiter Peter Martini.

Der Tagungsband zur Konferenz inklusive CD ist beim Springer-Verlag erschienen und im Buchhandel oder unter **www.springer.com** erhältlich (Englisch, mehr als 500 Seiten). Infos im Internet: **www.future-security-2012.de.**

DAS KURATORIUM

Das Kuratorium begleitet unsere Forschungsarbeit und berät Institutsleiter und den Vorstand der Fraunhofer-Gesellschaft. Die Mitglieder unseres Kuratoriums aus Industrie, Wissenschaft und Ministerien sind:

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

Prof. Dr. Armin B. Cremers
Rheinische Friedrich-Wilhelms-Universität,
Bonn

Dipl.-Ing. Thomas Dittler, MBA
Dittler & Associates
International Management Consultants GmbH,
Schondorf

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

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

Dr.-Ing. Hans-Joachim Kolb
MEDAV GmbH,
Uttenreuth

Dipl.-Ing. Herbert Rewitzer
ROHDE & SCHWARZ GmbH & Co. KG,
München

STELLVERTRETENDER VORSITZENDER DES KURATORIUMS

Dr. Uwe Wacker
EADS – Deutschland GmbH,
Ulm

MinDirig Dr. Dietmar Theis
BMVg – Bundesministerium der Verteidigung,
Bonn

Dipl.-Ing. (FH) Thomas Tschersich
Deutsche Telekom AG,
Bonn

Prof. Dr. Stefan Fischer
Universität zu Lübeck,
Lübeck

MinR Dipl.-Ing. Norbert Michael Weber
BMVg – Bundesministerium der Verteidigung,
Bonn

Prof. Dr.-Ing. Klaus Wehrle
RWTH Aachen,
Aachen

Dr. Thomas H. G. G. Weise
Rheinmetall AG,
Düsseldorf

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 66 Institute und selbstständige Forschungseinrichtungen. Rund 22 000 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 1,9 Milliarden Euro. Davon fallen 1,6 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Über 70 Prozent dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Knapp 30 Prozent werden von Bund und Ländern als Grundfinanzierung beigesteuert, damit die Institute Problemlösungen entwickeln können, die erst in fünf oder zehn Jahren für Wirtschaft und Gesellschaft aktuell werden.

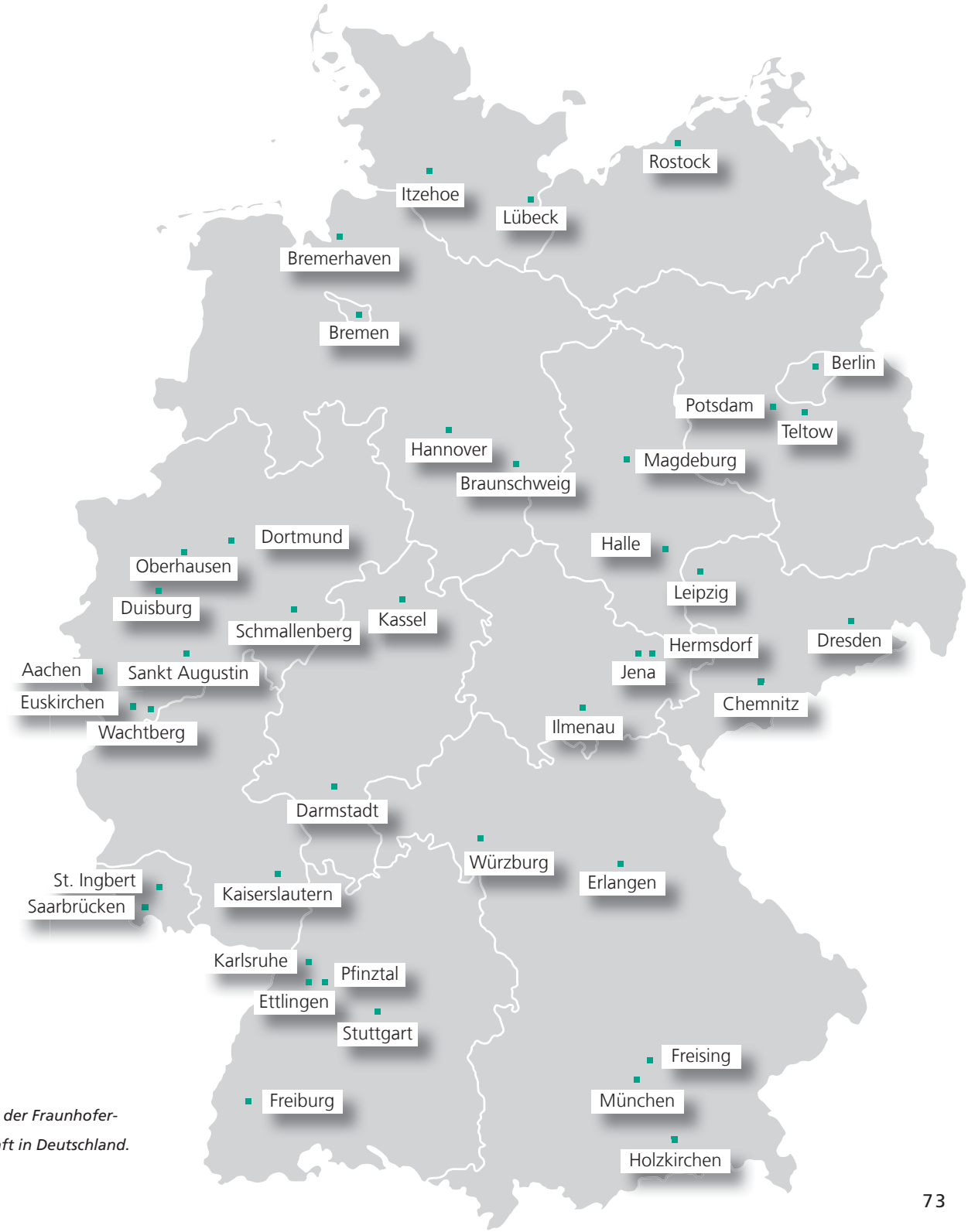
Internationale Niederlassungen sorgen für Kontakt zu den wichtigsten gegenwärtigen und zukünftigen Wissenschafts- und Wirtschaftsräumen.

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.

www.fraunhofer.de



Standorte der Fraunhofer-Gesellschaft in Deutschland.

WISSENSCHAFTLICHE BERICHTE

FKIE-Bericht-Nr.	Titel	Verfassung
224	Detektion geometrischer Formprimitive in unsortierten 3D Punktwolken	Gaspers, B.
225	FOD Detection on Runways using Multiple Sensors	Bhat, S.; Schikora, M.
226	Vom Korpus zur statistischen maschinellen Übersetzung – eine Evaluierung der Nutzung militärisch-relevanter Trainingsdaten für das Sprachenpaar Arabisch und Deutsch	Krautz, M.
227	The Shift-Method for Enhancing Repeated Signal Componenty – VS-NfD –	Kurth, F.
228	Entwurf und Implementierung einer modularen Anwendung zur Aufbereitung, Analyse und Visualisierung von Datenströmen aus der Luftraumüberwachung	Saul, R.
229	Abschlussbericht der Studie »Interoperabilitätexperiment 5 Power 2012«	Bau, N.; Schüller, H.; Gerz, M.
230	3D Visualisierung von Flugbewegungen für das Luftraumüberwachungssystem AIMS	Owega, A.
231	Intelligentes und effizientes Störverfahren gegen UMTS – VS-NfD –	Gläsel, D.; Bogenfeld, J.; Stuch, H.P.; Antweiler, M.
232	Middleware für Militärische Kommunikationsnetze – Projektbereich zu Abschnitt IV	Barz, C.; Jansen, N.; Krämer, D., Spielmann, D.

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

SDF

Verfasser	Titel
Daun, D.; Nickel, U.; Koch, W.	*Tracking in Multistatic Passive Radar Systems Using DAB/ DVB-T Illumination.* EURASIP Signal Processing, 92(2012) pp. 1365 – 1386.
Govaers, F.; Koch, W.	*An Exact Solution to Track-to-Track-Fusion at Arbitrary Communication Rates.* IEEE Transactions on Aerospace and Electronic Systems, 48(2012)3, pp. 2718 – 2729
Hörst, J.; Mertens, M.; Ulmke, M.; Wild, K.	*Sensordatenfusion für Agile UAV in vernetzter Umgebung.* Wehrwissenschaftliche Forschung 12 : Jahresbericht 2012. BMVg, Rü IV, 2013
Mertens, M., Feldmann, M.; Ulmke, M.; Koch, W	*Tracking and Data Fusion for Ground Surveillance.* In: Mallick, Mahendra ; Krishnamurthy, V. ; Vo, B.-N. (Eds.): Integrated Tracking, Classification, and Sensor Management: Theory and Applications. Wiley – IEEE Press, 2012, pp. 203 – 254. (ISBN 978-047-063905-4)
Schikora, M.; Koch, W.; Streit, R.; Cremers, D.	*A Sequential Monte Carlo Method for Multi-Target Tracking with the Intensity Filter.* In: Georgieva, Petia; Mihaylova, L.; Jain, L. C (Eds.): Advances in Intelligent Signal Processing and Data Mining. Springer, 2012, pp. 55 – 87. (Studies in Computational Intelligence ; 410) (ISBN 978-3-642-28695-7)
Schikora, M.; Neupane, B.; Madhogaria S.; Koch, K.; Cremers, D.; Hirt, H.; Kogel, K.-H.; Schikora, A.	*An Image Classification Approach to Analyze the Suppression of Plant Immunity by the Human Pathogen Salmonella Typhimurium.* BMC Bioinformatics, (2012)13:171 (pp. 14) http://www.biomedcentral.com/1471-2105/13/171
Svensson, D.; Ulmke, M.; Hammarstrand, L.	*Multitarget Sensor Resolution Model and Joint Probabilistic Data Association.* IEEE Trans. on Aerospace and Electronic Systems, 48(2012)4, pp. 3418 – 3434

KOM

Verfasser	Titel
Adrat, M., Osten, T., Leduc, J.,Antweiler, M., Elders-Boll, H.	*Legacy Waveforms on Software Defined Radio: Can Hierarchical Modulation offer an Added Value to SDR Operators.* In: MCC 2012. Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012. Military University of Technology, 2012, Vol. 1, pp. 171–186 (ISBN 978-83-62954-51-3).
Barz, C.; Diefenbach, A.; Abut, F.; Wilmes, M.; Sevenich, P.; Simon, P.; Bret, N.	*The CoNSIS approaches to network management and monitoring.* In: MCC 2012 : Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012, Military University of Technology, 2012, Vol. 1, pp. 161–178 (ISBN 978-83-62954-31-5)

KOM

Verfasser	Titel
Barz, C.; Rogge, H	*Improved community network node design using a DLEP based radio-to-router interface.* In: Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on … Barcelona: 8.–10. October 2012. IEEE Press, 2012, pp. 636–642 (ISBN 978-1-4673-1429-9)
Damm, D. ; Häge, M. ; Kurth, F. ; Oispuu, M.; Zeddelmann, D. von	*A System for Audio Summarization in Acoustic Monitoring Scenarios.* In: Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European … Bucharest: 27.–31. August 2012. IEEE Press, pp. 1279–1283 (ISBN 978-1-4673-1068-0)
Damm, D.; Fremerey, C.; Thomas, V.; Clausen, M.; Kurth, M.; Müller, M.	*A digital library framework for heterogeneous music collections: from document acquisition to cross-modal interaction.* *International Journal on Digital Libraries, 12(2012)2-3, pp. 53–71*
Ginzler, T.:	*A robust and scalable peer-to-peer publish/subscribe mechanism.* In: MCC 2012: Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012, Military University of Technology, 2012, Vol. 1, pp. 253–264 (ISBN 978-83-62954-31-5)
Kurth, F.; Lehn, H.-G.; Parting, R.	*Verfahren zur Erkennung eines oder mehrerer Nutzsignale innerhalb eines Quellsignals.* München: Deutsches Patentamt, 2012. Deutsches Patent, DE 10 2009 035 524
Leduc, J., Antweiler, M., Maseng, T.	*Spectrum Issues of NATO Narrowband Waveform, on the Spectral Efficiency of Continuous Phase Modulation (CPM) with small Modulation Indices.* In: MCC 2012: Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012, Military University of Technology, 2012, Vol. 2, pp. 161–170 (ISBN 978-83-62954-51-3)
Otnes, R.; Asterjadhi, A.; Casari, P.; Goetz, M.; Husøy, T.; Nissen, I.; Rimstad, K.; Van Walree, P.; Zorzi, M.	*Underwater Acoustic Networking Techniques.* Springer, 2012 (SpringerBriefs in Electrical and Computer Engineering) (ISBN 978-3-642-25223-5).

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

	Verfasser	Titel
KOM	Seifert, H.; Franke, M.; Diefenbach, A.; Sevenich, P.	*SOA in the CoNSIS coalition environment: Extending the WS-I Basic Profile for using SOA in a tactical environment.* In: MCC 2012: Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012, Military University of Technology, 2012, Vol. 1, pp. 105–116 (ISBN 978-83-62954-31-5)
	Steinmetz, P.	*Use of cross domain guards for CoNSIS network management.* In: MCC 2012: Military Communication and Information Technology. A Trusted Cooperation Enabler. Gdansk/Danzig: 8.–9. October 2012, Military University of Technology, 2012, Vol. 1, pp. 149–160 (ISBN 978-83-62954-31-5)

	Verfasser	Titel
ITF	Gerz, M.; Bau, N.	*A Platform-Independent Reference Data Model for a Future Interoperability Solution.* In: 17th International Command and Control Research and Technology Symposium (ICCRTS). Fairfax, VI: : 19. – 21. June 2012.18 pp. http://www.dodccrp.org/events/17th_iccrts_2012/post_conference/papers/097.pdf
	Haarmann, B.; Sikorski, L.; Gottsmann, F.	*Knowledge for Information Systems Acquired from a Co-Created Text Collection.* In: International Conference on Business Information Systems. Paris: June 2012. In: WASET World Academy of Science, Engineering & Technology. Issue 66. Art. 193, pp. 1092-1095. (ISSN: 2010-376X) http://media.wix.com/ugd/292010_34689dd5deefdb0795e116d39212a983.pdf
	Haarmann, B.; Gottsmann, F.; Schade, U.	*How to make Ontologies self-buildings from Wiki-Texts.* In: WORLDCOMP - IKE 2012. 2012 World Congress in Computer Science, Computer Engineering and Applied Computing. Las Vegas: 16. – 19. July 2012. CSREA Press, 2012, pp. 16 – 20 (ISBN 1-60132-222-4). http://media.wix.com/ugd/292010_467e86680e863f4e5db21d59fc1a49bd.pdf
	Langerwisch, M.; Ax, M.; Thamke, S.; Remmersmann, T.; Tiderko, A.; Wagner, B.	*Realization of an Autonomous Team of Unmanned Ground and Aerial Vehicles.* In: Intelligent Robotics and Applications. 5th International Conference. (ICIRA 2012). Montreal: 3.–5. October 2012. Springer, 2012, pp. 302–312 (Lecture Notes in Computer Science; 7506) (ISBN 978-3-642-33509-9)
	Rein, K.; Schade, U.; Remmersmann, T.	*Using Battle Management Language for Information Advantage.* In: IEEE ICC 2012. International Conference on Communications. Ottawa: 10. – 15. June 2012. IEEE Press, 2012, pp. 3432 – 3436. http://www-mobile.ecs.soton.ac.uk/home/conference/ICC2012/symposia/SA-TCO.html

ITF

Verfasser	Titel
Remmersmann, T.; Tiderko, A.; Langerwisch, M.; Thamke, S.; Ax, M.	*Commanding Multi-Robot Systems with Robot Operating System using Battle Management Language.* In: IEEE 2012 Communications and Information Systems Conference (MCC), Gdansk: 8. - 9. October 2012. IEEE Press, 2012, 6 pp. (ISBN 978-1-4673-1422-0)
Remmersmann, T.; Schade, U.; Schlick, C.	*Supervisory control of multi-robot systems by disaggregation and scheduling of quasi-natural language commands.* IEEE 2012 Communications and Information Systems Conference (MCC), Gdansk: 8.–9. October 2012. IEEE Press, 2012, Vol. 1, pp. 305–316 (ISBN 978-1-4673-1422-0)
Schade, U.; Haarmann, B.	*Complementing Battle Management Language by Ontological Means.* In: 2012 Spring Simulation Interoperability Workshop (Spring SIW 2012). Orlando: 26.–30. March 2012. Curran Ass., 2012, pp. 45–53 (Paper 12S-SIW-006) (ISBN: 978-1-61839-719-5)
Schade, U.; Remmersmann, T.; Khimeche, L.; Gautreau, B.; El Abdouni Khayari, R.	*Lessons Recognized: How to Combine BML and MSDL.* In: 2012 Spring Simulation Interoperability Workshop (Spring SIW 2012). Orlando: 26. – 30. March 2012. Curran Ass., 2012, pp. 102 – 109 (Paper 12S-SIW-012) (ISBN: 978-1-61839-719-5)
Wunder, M.	*Concept for a Social C2IS – Bridging the Heterogeneity of People and IT.* In: Social Media: Risks and Opportunities in Military Applications. RTO HFM Meeting. Tallinn: 16. – 18. April 2012. NATO, RTO, 2012, pp. 8-1 – 8-12. RTO-MP-HFM-201. (ISBN 978-92-837-0165-1)

EMS

Verfasser	Titel
Alexander, T.	*Analysis of the Effect of an Information Processing Task on Goal-Directed Arm Movements.* *In: Duffy, Vincent (Ed.): Advances in Applied Human Modeling and Simulation. CRC Press, 2012, pp. 103–112 (ISBN 978-1-439870-31-0)*
Alexander, T.	*Enhancing Human Effectiveness through Embedded Virtual Simulation.* In: Interservice/Industry Training, Simulation and Education Conference (I/ITSEC). Proceedings of the … Orlando, FL.: 4.–6. December 2012. Arlington, VA : National Training and Simulation Association, 2012, http://ntsa.metapress.com/link.asp?id=f4223m01206m4045
Alexander, T.; Paul, G.	*Digitale Menschmodelle – Werkzeuge zur Systemsimulation in der Arbeitswissenschaft.* In: Schütte, Martin (Hrsg.): Gestaltung nachhaltiger Arbeitssysteme – Wege zur gesunden, effizienten und sicheren Arbeit. Dortmund: GfA-Press, 2012, S. 165–168 (ISBN 978-3-936804-12-6)

AUSGEWÄHLTE VERÖFFENTLICHUNGEN

	Verfasser	Titel
EMS	Conradi, J.; Alexander, T.	*On the effect of free vs. restricted interaction during the exploration of virtual environments.* *Work: Journal of Prevention, Assessment and Rehabilitation, 41(2012) Supplement 1, pp. 2201–2207 (ISSN 1051-9815 print) – (ISSN 1875-9270 online)*
	Flemisch, F.; Meier S.; Neuhöfer J.; Baltzer M.; Altendorf, E.; Özyurt, E.	*Kognitive und kooperative Systeme in der Fahrzeugführung: Selektiver Rückblick über die letzten Dekaden und Spekulation über die Zukunft.* In: Kognitive Systeme: Mensch, Teams, Systeme und Automaten. 2. Interdisziplinärer Workshop. Duisburg: 18.–20. September 2012
	Kaster, A., Witt, O. & Schlick, C.M	*Operationszentrale der Zukunft.* Europäische Sicherheit und Technik, (2012)7, pp. 66-69
	Neuhöfer, J.; Govaers, F.; Elmokni, H.; Alexander, T.	*Adaptive Information Design for Outdoor Augmented Reality.* Work: Journal of Prevention, Assessment and Rehabilitation, 41(2012) Supplement 1, pp. 2187–2194 (doi:10.3233/WOR-2012-0441-2187) (ISSN 1051-9815 print) – (ISSN 1875-9270 online)
	Özyurt, E. ; Döring, B.; Flemisch, F..	*Vorgehensweise zur simulationsbasierten Entwicklung eines kognitiven Assistenzsystems für Marineschiffe.* In: Kognitive Systeme: Mensch, Teams, Systeme und Automaten. 2. Interdisziplinärer Workshop. Duisburg: 18.–20. September 2012
	Schlick, C.; Winkelholz, C.; Ziefle, M.; Mertens, A.	*Visual Displays.* In: Jacko, Julie A. (Ed.): The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications. CRC Press, 2012, pp. 157–191 (ISBN 978-1-4398-2943-1)
	Schwarz, J.; Witt, O.	*Design of a Touch-based User Interface for Naval Command and Control and Comparison with a Current Onboard System in a Scenario-based Usability Test.* In: Advances in Usability Evaluation. Part I. Rebelo, Franscisco (Ed.). CRC Press, 2012, pp. 23 –32 (ISBN: 978-1-4398-7024-2)

	Verfasser	Titel
US	Brunner, M.; Brüggemann, B.; Schulz, D.	*Autonomously Traversing Obstacle: Metrics for Path Planning of Reconfigurable Robots on Rough Terrain.* In: ICINCO 2012. Proceedings of the 9th International Conference on Informatics in Control, Automation and Robotics. Rome: 28.–31. July 2012. 2012, Vol. 2, pp. 58–69 (ISBN 978-989-8565-22-8)
	Fiolka, T.; Stückler, J.; Klein, D. A.; Schulz, D.; Behnke, S.	*Place Recognition using Surface Entropy Features.* In: Proceedings of the 2nd IEEE ICRA Workshop on Semantic Perception, Mapping, and Exploration. Saint Paul, MN: 14. May 2012. IEEE, 2012, 7 pp. http://www.ais.uni-bonn.de/papers/ICRA_WS_SPME_2012_Fiolka_et_al.pdf

US

Verfasser	Titel
Königs, A.; Schulz, D.	*Evaluation of Thermal Imaging for People Detection in Outdoor Scenarios.* In: SSRR 2012: 10th IEEE International Symposium on Safety, Security, and Rescue Robotics. College Station, TX: 5.–8. November 2012. IEEE Press, 2012
Schneider, F. E.; Wildermuth, D.	*Influences of the robot group size on cooperative multi-robot localisation — Analysis and experimental validation.* *Robotics and Autonomous Systems, 60(2012)11, pp. 1421–1428*
Soldan, S.; Welle, J.; Barz, T.; Kroll, A.; Schulz, D.	*Towards Autonomous Robotic Systems for Remote Gas Leak Detection and Localization in Industrial Environments.* *In: Proceedings of the 8th International Conference on Field and Service Robotics (FSR2012).* Matsushima: 16.–19. July 2012. 2012, Vol. 8

CD

Verfasser	Titel
Apel, M.; Meier, M.	*Generalizing Behavioral Signatures for Detecting Unknown Malware Variants and Early Warning.* PIK Praxis der Informationsverarbeitung und Kommunikation, 35(2012)1, pp. 17–24
Aschenbruck, N.; Martini, P.; Meier, M.; Tölle, J. (Eds.)	*Future Security 2012. Proceedings of the 7th Security Research Conference.* Bonn: 4.–6. September 2012. Springer, 2012 (Communications in Computer and Information Science; 318) (ISBN 978-3-642-33160-2)
Eschweiler, S.; Gerhards-Padilla, E.	*Platform-Independent Recognition of Procedures in Binaries Based on Simple Characteristics.* it – Information Technology, 54(2012)2, pp. 64–70
Flegel, U.; Meier, M.	*Modeling and Describing Misuse Scenarios Using Signature-Nets and Event Description Language.* it – Information Technology, 54(2012)2, pp. 71–81
Gassen, J.; Gerhards-Padilla, E.; Martini, P.	*Current Botnet-Techniques and Countermeasures.* PIK Praxis der Informationsverarbeitung und Kommunikation, 35(2012)1, pp. 3–10
Günther, H.; Jahnke, M.	*Automatic Generation of Extended Dependency Graphs for Network Security.* In: LCN 2012. 37th IEEE Conference on Local Computer Networks. Clearwater, FL: 22.–25. October 2012. IEEE Press, 2012, pp. 136–139 (ISBN 978-1-4673-1565-4)
Klein, G.; Hunke, S.; Günther, H.; Jahnke, M.	*Model-based Cyber Defense Situational Awareness.* PIK – Praxis der Informationsverarbeitung und Kommunikation, 35(2012)1, pp. 46–53

AUSGEWÄHLTE TÄTIGKEITEN IN GREMIEN

Beitragende	Tätigkeit
Adrat, M.	Advisory Council of the Coordinating Committee of International SDR Standards of the Wireless Innovation Forum.
Adrat, M.; Leduc, J.; Couturier, S.	EDA Ad-hoc Working Group on SDR Standardization Strategic Guidance.
Alexander, T.	EDA: CAPTECH ESM 04 (Human Factors & CBR Protection), CGE.
Alexander, T.	NATO STO HFM RT G-216 on Synthetic Environments for HSI Application, Assessment, and Improvement, national speaker.
Alexander, T.; Conradi, J.	EDA: CEDS-Study Bio Sensor Information Demonstrator, EMG – government experts.
Antweiler, M.	Technical Program Committee Member und Session Chairman, Military Communication and Information Systems Conference, Danzig, 8.–9.10.2012.
Aurisch, T.	NATO-STO IST-103 RTG-043: Task Group on Selected Aspects of PCN.
Barz, C.	NATO STO IST-909 on »SOA-Challenges for Real-Time and Disadvantaged Grids«.
Barz, C.; Jansen. N.	NATO-STO IST-RT G-118: Research Task Group on SOA recommendations for disadvantaged grids in the tactical domain.
Barz, C.; Rogge, H.	EU FP7 ICT Large-Scale Integrated Projekt CONFINE Community Networks Testbed for the Future Internet.
Bau, N.; Schüller, H.	Teilnahme am 5 Power Net-Centric Project Arrangement (5P NC PA).
Bosch, T.	NATO IST ET-065: Dynamic Wireless Network Cross-layer Security and Security Awareness in Coalition Environments.
Brüggemann, B.	Teilnahme SCI-251 ET on Multi-National Interoperability between multiple Manned and Unmanned Systems (MaUS).
Brüggemann, B.; Königs, A.	Teilnahme an der NATO NIAG Studie SG-157.

Beitragende	Tätigkeit
Charlish, A.	Mitglied der NATO RT G SET-ET-075 on »Evaluating the effectiveness of coordination methods for distributed mobile sensors«.
Couturier, S.	NATO STO IST-077 RTG-035: Cognitive Radio.
Couturier, S.	NATO-STO IST-104: Research Task Group on Cognitive Radio II.
Couturier, S.; Adrat, M.; Liedtke, F.	NATO-STO SCI-222 Task Group on Electronic Warfare Issues of Software Defined Radios.
Flemisch, F.	NATO Science & Technology Organisation, deutscher Vertreter im IST-Panel.
Günther, H.; Jahnke, M.	NATO IST ET-066: Future Concepts & Tools for Cyber Defence.
Hecking, M.	NATO IST-078 RTG-036: Machine Translation for Coalition Operations.
Hunke, S.	NATO STO IST: Research Group on Dynamic Wireless Network Cross-layer Security and Security Awareness in Coalition Environments.
Kaster, J.; Schüller, H.; Huy, S.	Deutsche Arbeitsgruppe im Rahmen des internationalen Coalition Warrior Interoperability Exercise (CWIX 2012).
Kleiber, M.	NATO IST-085: Interactive Visualisation of Network Dynamics.
Koch, W.	Lecturer bei der NATO LS SET-157 on »Multisensor Fusion: Advanced Methodology and Application«.
Koch, W.	Chairman der NATO RTG IST-106 Research Task Group on »Information Filtering and Multi Source Information Fusion«.
Leduc, J.; Couturier, S.; Adrat, M.	EDA Project Team on Software Defined Radio.
Leduc, J.; Escudero, H.	NATO Line Of Sight Communications Capability Team.
Oispuu, M.	Mitglied der NATO RTG SET-189 on »Battlefield Acoustics, Multi-modal Sensing, and Networked Sensing for ISR Applications«.

Beitragende	Tätigkeit
Schade, U.; Rein, K.; Remmersmann, T.	NATO RTO MSG-085: Standardization of C2-Simulation Interoperability.
Schneider, F. E.	IST-107-RT G-052 on Standards Promoting Interoperability for Coalition UGVs.
Sevenich, P.	NATO-STO IST: Exploratory Team on Heterogeneous Networks.
Tölle, J.	NATO-IST-091/RT G-039: Task Group on Computer Network Defence Common Operational Picture.
Tschauner, M.; Bongartz, H.	NATO-STO IST ET-068: Exploratory Team on LTE versus WiMAX for Military Applications.
Winkelholz, C.; Kleiber, M.:	NATO IST-110: Visualization for Analysis.
Wunder, M.	NATO Science & Technology Organisation, deutscher Vertreter im IST-Panel.
Wunder, M.	Chairman der NATO-Arbeitsgruppe IST-094/RT G-044 Framework for Semantic Interoperability.
Wunder M.; Tölle, J.	Organisation und Durchführung IST-Symposium IST-111/RSY-026 on Information Warfare and Assurance – Cyber Defence, Koblenz.

IMPRESSUM

HERAUSGEBER
Fraunhofer-Institut für Kommunikation,
Informationsverarbeitung und Ergonomie FKIE

Fraunhoferstraße 20
53343 Wachtberg

Tel.: +49 (0)228 9435-287
Fax: +49 (0)228 9435-685

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

REDAKTION
Bernd Müller, Bernhard Kleß

LAYOUT, SATZ, LEKTORAT
Volker Kurzidim, FKIE-Stabstelle

FOTOGRAFIE
Uwe Bellhäuser / das bilderwerk

BILDQUELLEN
Bilder © Fraunhofer FKIE

AUSNAHMEN:
// S.6 Business Diagram on White. File #23293712, istockphoto

// S.18/19 Scharfschütze G82. Fotograf: Bjoern Trotzki, Medienzentrale der Bundeswehr

// S.22 Foto Sensor Arrays. Carsten Siering, Mainz

// S.24/25 Barracuda beim Landeanflug auf dem Flughafen Goose-Bay, Kanada. Erhalten von Christian Albert, Cassidian

// S.28/29 Interconnecting social network users on a bright blue network system. File #21071098, istockphoto

// S.33 Buckelwal Unterwasser in Maui hawaii. Bildnummer: 6090331, 123 RF®

// S.34 Wehrbereichsmeisterschaft der Reservisten 2012: Station Schießausbildung-ein Soldat im Anschlag. Fotograf: Tino Arnold, Medienzentrale der Bundeswehr

// S.42/43 Mitfahrt des kroatischen BFH Marine auf der Korvette BRAUNSCHWEIG in Begleitung des BFH der deutschen Marine Vizeadmiral Stricker. Medienzentrale der Bundeswehr

// S.61 Biometrics. File #2631931, istockphoto

// S.63 binary computer code and the warning messages that a virus is detected. File #23620220, istockphoto

// S.72/73 A boardroom table with world clocks above. File #865752, istockphoto

HINWEISE
BOTMAN® ist eine Marke der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., München.