FFG

KIRAS Sicherheitsforschung

Wissenschaf(f)t Sicherheit

Geförderte KIRAS-Projekte
2013 – 2015

www.kiras.at

bmvit

Bundesministerium für Verkehr, Innovation und Technologie

Wissenschaf(f)t Sicherheit

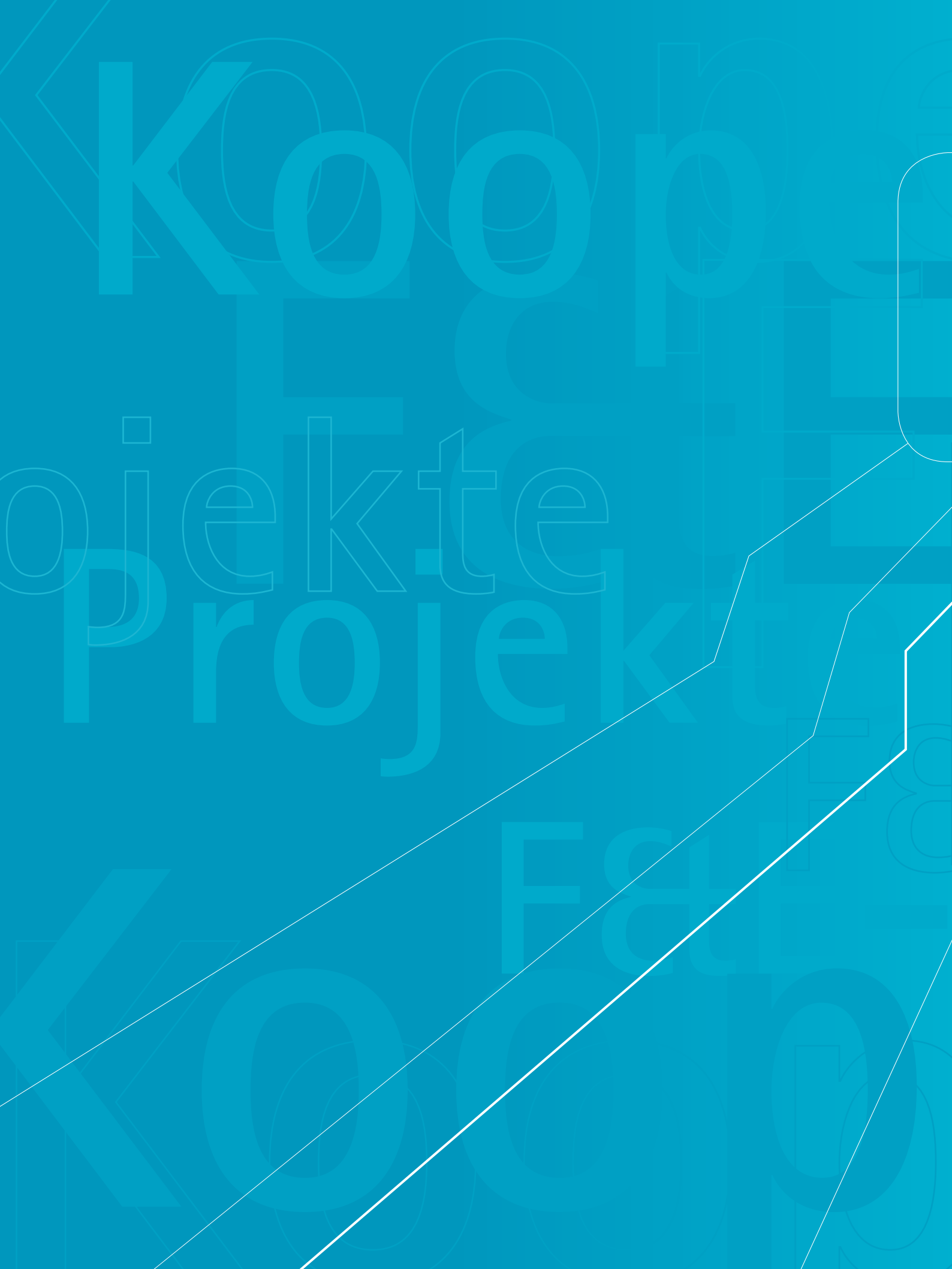
Geförderte KIRAS-Projekte
2013 – 2015

Aktuelle Zahlen KIRAS

- 211 geförderte Projekte bis 2016 (29 % der beantragten Projekte)
- € 71 Mio. Förderbartwert (budgetäre Leistung des bmvit) bei einem Projektgesamtvolumen von fast € 102 Mio. - Gesamtförderquote von 70 % von 2006 bis 2016
- € 141 Mio. Wertschöpfungsvolumen (direkte, indirekte und induzierte Effekte) durch den Förderbarwert generiert
- € 32,4 Mio. Sozialversicherungsabgaben wurden generiert
- € 36 Mio. Steuereinnahmen für den öffentlichen Haushalt
- € 485.000 durchschnittliche Projektkosten mit € 148.000 als durchschnittlichem Eigenanteil
- An den 116 Kooperativen F&E- Projekten waren bzw. sind 202 Bedarfsträger beteiligt (durchschnittliche Einbindung von 1,74 Bedarfsträgern pro Projekt)
- 389 der 930 Antragsteller – rund 42 % – hatten sich bereits in früheren Ausschreibungen beteiligt
- 89 % der Bedarfsträger sahen positive Auswirkungen auf die Sicherheit im öffentliche Raum (Zielwert von >60 % deutlich erreicht)
- Durchschnittlich waren 1,15 GSK-Partner pro Projekt eingebunden
- 86 % der Unternehmen bzw. 79 % der Forschungseinrichtungen haben zumindest teilweise neue Forschungsbereiche erschlossen
- 809 hochqualifizierte Arbeitsplätze wurden gehalten und 589 hochqualifizierte Arbeitsplätze geschaffen
- Schaffung von nachhaltiger Beschäftigung für neu eingestelltes Personal
- 88 % der Unternehmen und 70 % der Forschungseinrichtungen konnten sich neue Kompetenzen aneignen

Aktuelle Zahlen des KIRAS Evaluierungsberichts 2016

Inhalt


Kooperative
Projekte


Kooperative
F&E-
Projekte

3B3M

Bezahlbetrugsbekämpfung bei modernen, mobilen Methoden

Das Projekt 3B3M schafft zum einen eine digitale Meldestelle, die die Bekanntgabe von Betrug und Betrugsversuchen („Fraud") in zeitgemäßer, einfacher und einheitlicher Weise ermöglicht, zum anderen alle Voraussetzungen für die Analyse, Aufbereitung und weitergehende Interpretation der gesammelten Daten durch verschiedene berechtigte Interessensgruppen.

Der verstärkte Gebrauch kontaktloser Technologien (z. B. NFC, QR-Code) zum Bezahlen am Point-Of-Sale stellt Sicherheitskräfte und Industrie gleichermaßen vor neue Herausforderungen, wenn es um die Abwehr krimineller Handlungen geht. Auf Grund der physischen Distanz und Reichweite beim Datenaustausch sowie durch die sehr unterschiedlichen neuen Anbieter und deren neue Infrastrukturen eröffnen sich neue Szenarien des Missbrauchs. Die sich abzeichnende Diversität der auf den Markt drängenden Bezahlsysteme, deren Vernetzung und übergreifende Verwendung erhöhen durch die individuelle Fehleranfälligkeit der Systeme die Komplexität der Betrugsbekämpfung. Zum Schutz der BürgerInnen ist ein Mitwachsen des Wissens über solche Bedrohungsszenarien essentiell.

Durch die Sammlung und intelligente Interpretation der Informationen kann ein tiefgehendes Verständnis über Angriffsvektoren und Denkansätze der TäterInnen entwickelt werden. Diese ermöglichen in weiterer Folge die umgehende Ergreifung der bestgeeigneten Maßnahmen z. B. gegen organisierte Kriminalität, sowohl reaktiv auf Akutfälle als auch als Präventivmaßnahme zur Schadensvermeidung. Das Kernsystem ist dabei so gebaut, dass in Zukunft auch dynamische Daten integriert und „on-the-fly" berücksichtigt werden können. 3B3M wird damit von der digitalen Meldestelle zur digitalen 24/7-Einsatzzentrale der Betrugsbekämpfung erweitert.

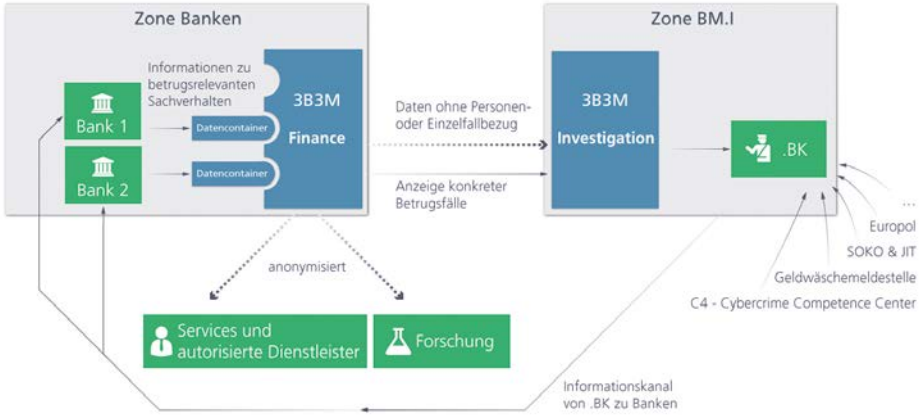
Die sichere gemeinsame Nutzung der gesammelten Daten und Strategien durch verschiedene Gruppen wird in 3B3M durch ein durchdachtes Zonenkonzept mit unterschiedlichen Zugriffsrechten und Aktionsmöglichkeiten umgesetzt. Dieses gewährleistet die Einhaltung von Compliance- und Strukturregeln, denen die verschiedenen zugriffsberechtigten Stellen, sowohl auf Seite der Daten-Einmeldung (z. B. Banken) als auch der Datenauswertung (z. B. öffentliche Stellen) unterliegen. So ist sichergestellt, dass Finanzinstitutionen ausschließlich auf den eigenen Datenbestand und dazugehörige Dokumente Zugriff haben.

Damit leistet 3B3M einen essentiellen Beitrag, um das Ziel „Prevention & Detection" zu erreichen und möglichst sichere Rahmenbedingungen im Umgang mit diesen neuen Bezahltechnologien zur Verfügung zu stellen. Die Betrugsplattform wird zur Gänze in Österreich geplant, erdacht, erbaut und erprobt. Das so gebündelte und zugänglich gemachte Wissen nützt auch den Herstellern, die bereits in der Entwicklung und später in der Fertigung ihre Systeme und die Daten ihrer KundInnen besser schützen können. Ein nachhaltiger Aufbau von spezifischem Wissen, Know-How und Erfahrungen anhand der Vernetzung einschlägiger ExpertInnen wird dadurch gefördert.

Nicht nur wegen seines Ansatzes „Prevention & Detection" ist 3B3M ein richtungsweisender, globaler Schritt in der österreichischen Sicherheitsforschung. Auch der Informationszugang und das Reporting für ein erfüllendes Berichtswesen an Behörden zur Täterverfolgung ist besonders innovativ. Bei strikter Erhaltung der rechtskonformen Verwendung und der Datensicherheit können im Rahmen der jeweiligen Rechte und Pflichten Daten ausgetauscht werden. Die Plattform 3B3M sieht dafür eine Trennung in 2 Module vor, die miteinander nur über dedizierte, gesicherte Schnittstellen kommunizieren, nach aktuellen Standards und Best Practices hochsicher aufgesetzt sind und den Grundsätzen und Konzepten von Privacy by Design folgen.

Im Modul 3B3M-Finance können die Finanzinstitutionen ihre Daten in Bezug auf konkrete Betrugssachverhalte (auch Bagatellfälle) erfassen, sammeln und sicher ablegen. Zusätzlich bietet 3B3M-Finance die Möglichkeit einer Unterstützung bei der direkten digitalen Anzeige einzelner Sachverhalte an das österreichische Bundeskriminalamt (.BK). Durch diese Herangehensweise werden die Dateneingabe und die Erstattung von Anzeigen vereinheitlicht und erheblich vereinfacht. Durch die geordnete, gerichtete Übermittlung der relevanten Informationen werden die Transaktionskosten sowohl für die meldenden Stellen als auch für das .BK minimiert. Darüber hinaus ermöglicht 3B3M-Finance das Generieren von Trenddaten zur einschlägigen Betrugskriminalität. Da diese Daten keine konkreten Anhaltspunkte für das Vorliegen einer Straftat beinhalten, zieht dies auch keine unmittelbare Verfolgungspflicht der BeamtInnen nach sich. Diese anonymisierten Trenddaten

Schematische Datenschutz- und Bank-Compliance-korrekte Darstellung der Systeme und Informationskanäle zwischen .BK und Banken



Schematische Darstellung der 3B3M-Plattform

können exportiert und institutionsübergreifend dem .BK oder für unterschiedliche Dienstleistungen und Forschung zugänglich gemacht werden.

Das Modul 3B3M-Investigation ist direkt im .BK angesiedelt und importiert automatisch die im Modul 3B3M-Finance generierten, allgemeinen Trenddaten. Den MitarbeiterInnen des .BK werden die Daten entsprechend ihrer Zuständigkeit und Rolle aufbereitet und für die Prävention und Bekämpfung von Betrugskriminalität zur Verfügung gestellt. Zusätzlich kann das .BK ausgewählte Informationen, die es aus erweiterten Kreisen wie Europol, Interpol usw. erhalten hat, über einen entsprechenden Kanal angebundenen Finanzinstitutionen zur Verfügung stellen.

Durch die forschungsbegleitende Entwicklung, die starke Einbindung von FachexpertInnen sowie das regelmäßige Feedback der späteren AnwenderInnen wird der größtmögliche Mehrwert für alle Beteiligten erreicht. Die Plattform soll nach Ende des Forschungsprojekts weiter ausgebaut und kontinuierlich verbessert werden. Durch eine stetig steigende AnwenderInnenzahl sollen die Reichweite und der Impact weiterwachsen. Durch die Erweiterung um dynamische Daten sollen zudem Echtzeitanalyse und -bewertung sowie automatisierte Reaktionen auf erkannte Gefahren zu einer modernen Betrugsbekämpfung integriert werden.

Projektleitung
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH

Projektpartner
- Bundesministerium für Inneres
- Bundeskriminalamt
- TU Wien, Fachbereich Rechtswissenschaften
- Karl-Franzens-Universität Graz, Institut für Soziologie
- PayLife Bank GmbH
- Erste Bank der österreichischen Sparkassen AG

Kontakt
DI Florian Fankhauser, Dr. Christian Schanes
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F, 2320 Schwechat
Tel.: +43 1 9049007-0
E-Mail: florian.fankhauser@rise-world.com, christian.schanes@rise-world.com
www.rise-world.com

3F-MS

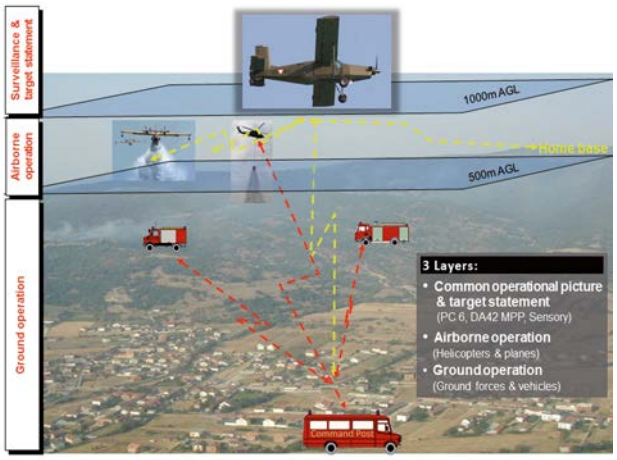
Multi-Level „ForestFireFighting-Management System" zur optimierten Einsatzführung von Boden- und Luftkräften in Waldbrandsituationen

Auf Grund des dramatischen Anstiegs von Waldbränden in Europa und auch weltweit sowie deren Folgeschäden ist eine optimierte Waldbrandbekämpfung ein wichtiges nationales aber auch internationales Thema, um Menschenleben und Ressourcen besser schützen und die Umweltauswirkungen von Waldbränden möglichst gering halten zu können. Erforderlich ist daher eine innovative, echtzeitnahe Lagebilderfassung sowie eine rollen- und szenarienoptimierte Managementlösung, um vorhandene Ressourcen effizient und mit bestmöglicher Interaktion einsetzen zu können. Die Waldbrandbekämpfung unterscheidet sich wesentlich durch die Art des Brandes und erfordert unterschiedliche Strategien, welche durch die Managementlösung unterstützt werden müssen. Neben der optimierten Einsatzführung während der Brandsituation ist eine wesentliche Aufgabenstellung eine Beobachtung großer Flächen über mindestens 36 Stunden nach Abschluss der Löscharbeiten, um eine etwaige Wiederentfachung rasch erkennen und gezielt bekämpfen zu können.

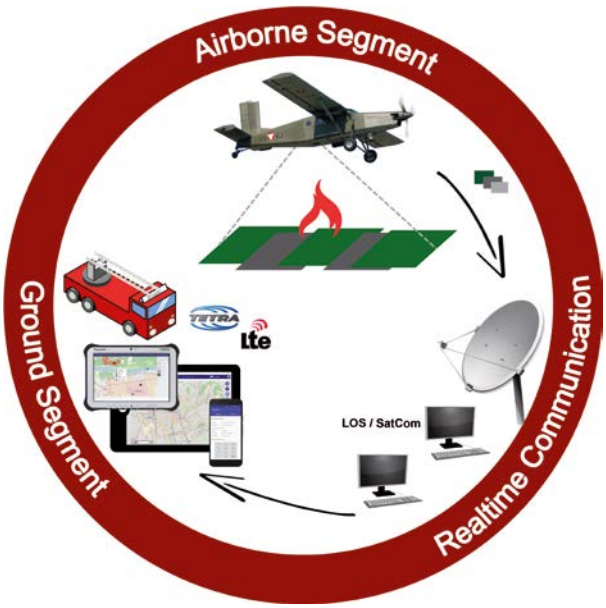
Der Schlüssel eines optimalen Einsatzes bzw. einer optimalen Einsatzführung verfügbarer Kräfte ist ein aktuelles, umfassendes Lagebild sowie eine Managementlösung, die es ermöglicht, Ressourcen wie Fahrzeuge/Ausrüstung am Boden, Löschtrupps und Rettungsteams sowie Löschflugzeuge und Helikopter effizient einzusetzen. Das Einbeziehen und die Koordination der einzelnen Ebenen (großräumige Überwachung zur Lagebilderstellung, Luftkräfte für den Lösch- und Transporteinsatz sowie der Bodenkräfte) sind essentielle Inhalte eines umfassenden und optimierten Waldbrandmanagements großer Flächen. Basierend auf dem im Rahmen des Projekts AIRWATCH entwickelten, luftgestützten, multi-funktionalen Führungsunterstützungssystem ARGUS werden in 3F-MS folgende Themen fokussiert:

- Optimierung der Aufnahme mit Thermalsensoren für großflächige Bereiche mit Fokus auf ein rotierendes Spiegelsystem und die erforderlichen geometrischen Verfahren
- Analysen verschiedener Brandarten auf Basis thermaler Signaturen zur automatischen Klassifikation
- Simulation und Impactevaluierung effizienter Ressourceneinsätze, abgestimmt auf die Anforderungen verschiedener Waldbrandszenarien
- Unterstützung der Aufgabenverteilung und Erweiterung von Statusinformationen verbundener Einheiten
- Unterstützung von Bodenteams und Integration mobiler Informationssysteme und Feuerwehrfahrzeuge.

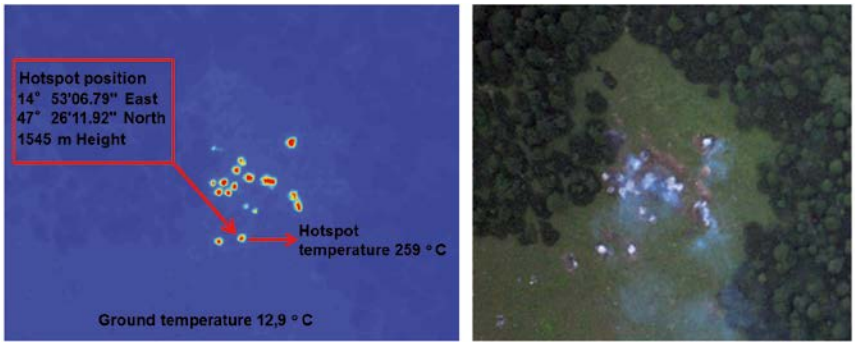
Neben der Unterstützung verschiedener Phasen des Waldbrand-Management-Konzepts zielt 3F-MS auf den gezielten Einsatz in konkreten Waldbrandsituationen ab. Dies umfasst speziell die Entwicklung einer Multi-Level-Managementlösung zur Koordination von Einsatzkräften, Steuerung aller 3F-MS-Luftaufklärungs- und Prozessierungsmodule zur optimierten Einsatzführung in Waldbrandsituationen sowie die



Multi-Layer Waldbrandmanagementkonzept



3F-MS Systemkonzept



Thermales Bild (li.) inkl. georeferenzierter Hot-Spot-Analyse und optisches Bild (re.)

gezielte Datenverteilung an involvierte Bodenteams, Fahrzeuge und Organisationen. Die Entwicklung einer flächenoptimierten Steuerung des Thermalsensors sowie einer echtzeitnahen on-board Geo-Prozessierung von thermalen Bilddaten im 3F-MS-Flugmodul zielt auf die Reduktion der benötigten Bandbreite und somit auf optimierte, gezielte Datenerhebung ab. Neben einer echtzeitnahen, automationsgestützten Datenanalyse zur Erstellung eines zeit- und situationsoptimierten Lagebildes ist auch die Integration eines Simulationsmoduls zur Entscheidungsunterstützung in Hinblick auf die Planung und Evaluierung des Ressourceneinsatzes sowie der Effektivität durchgeführter Bekämpfungsstrategien ein wichtiger Faktor. Dieses Modul arbeitet mit existierenden Services zur Prognose der Ausbreitung von Waldbränden zusammen und erlaubt eine deutlich verbesserte Einsatzplanung sowie Wirkungsanalyse.

Ein Entwicklungsschwerpunkt liegt in der Integration von körpergetragenen Assistenzsystemen für die Bodenteams sowie einer mobilen und fahrzeuggebundenen Informationslösung in innovative Kommando- und Waldbrandlöschfahrzeuge. Hierbei erfolgt auch der gezielte Einsatz des Digitalfunk-Standards TETRA. Durch Internationale Kooperationen sowie die Durchführung eines internationalen 3F-MS-Workshops 2016 in Österreich im Rahmen des EU-Programms „Exchange of Experts" erfolgte eine starke internationale Vernetzung und ein erheblicher Wissenstransfer. Auch sozialwissenschaftliche Aspekte hinsichtlich der Akzeptanz und des praktischen Gewinns der entwickelten Lösungen im realen Einsatzfall, relevante Unterschiede/Aspekte im nationalen und internationalen Einsatz sowie Untersuchungen zur Einbindung von „Public Information" im Fall von Wandbränden stellen einen Teil der Arbeiten im Projekt dar.

Projektleitung
JOANNEUM RESEARCH Forschungsges.mbH, DIGITAL

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Amt der Niederösterreichischen Landesregierung
- Karl-Franzens-Universität Graz, Institut für Soziologie
- Ing. Richard Feischl, IFR
- Magirus Lohr GmbH
- Berufsfeuerwehr Graz
- Berufsfeuerwehr Berlin
- Freiwillige Feuerwehr Gumpoldskirchen
- Firefighting Association Primorsko-Goranska Country, Kroatien
- European Commission Joint Research Centre, IES
- Forest Resources and Climate Unit, Italien

Kontakt
DI Alexander Almer
JOANNEUM RESEARCH – DIGITAL
Institut für Informations- und Kommunikationstechnologien
Steyrergasse 17, 8010 Graz
Tel.: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital

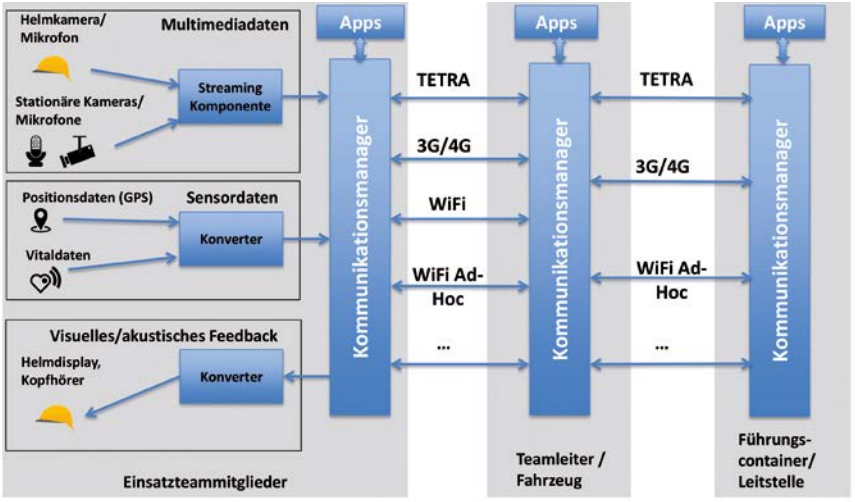
4C4FirstResponder

Flexible multifunktionale Kommunikations- und Informationslösungen für eine optimierte Einsatzführung von Interventionskräften

Komplexe Anforderungen an Einsatzkräfte durch unterschiedliche und sich oft dynamisch verändernde Sicherheitslagen, bei gleichzeitiger Anforderung eines effizienten Personaleinsatzes, erfordern einen gezielten Einsatz von neuen Informations- und Kommunikationslösungen. Die mit einer veränderten Sicherheitslage verbundenen Ereignisse können z. B. Massenveranstaltungen sein, welche (sequentiell) unterschiedliche Orte betreffen (Bahnhof, Veranstaltungsort, Innenstadt, etc.). Dies stellt eine Herausforderung dar, da die Dynamik solcher Ereignisse nicht vorhersagbar ist und den Führungs- und Einsatzkräften notwendige Informationen (zeitnah und von hinreichender Qualität) zur effizienten Einsatzdurchführung fehlen.

Das Hauptziel von 4C4FirstResponder ist die dynamische und echtzeitnahe Erzeugung eines besseren Lagebildes zur verbesserten Interaktion zwischen Teams und Einsatzleitung. Die echtzeitnahe Erstellung eines aktuellen Lagebildes, mobile multisensorale Assistenzlösungen (basierend auf Audio-, Bild, Video- und Körpersensoren) sowie eine stabile Sprach- und Datenkommunikation unterstützen das koordinierte Zusammenwirken unterschiedlicher Einheiten bzw. Einsatzkräfte. Als Kern des Projekts wird daher eine flexible, multimediale Kommunikationslösung angestrebt, die neben TETRA auch Breitband-Technologien wie UMTS/LTE und WiFi einbindet.

Aus der Erfahrung anderer Projekte hat sich gezeigt, dass eine frühe Einbindung der Endanwender (Feuerwehr, Polizei, Rettungskräfte etc.) wichtig ist, daher wird ein agiler Entwicklungsansatz verfolgt. Zu Beginn des Projektes fand ein halbtägiger Workshop statt, bei dem die Endanwender die aus ihrer Sicht wichtigsten Anwendungsfälle, Szenarien und Anforderungen darlegen konnten. Dabei hat sich herausgestellt, dass Sprechfunk immer noch die wichtigste Form der Kommunikation ist und TETRA für die Kommunikation sensibler Daten zwingend gefordert wird. Daher wird im Gegensatz zu anderen Lösungsansätzen bei der 4C4FirstResponder-Architektur TETRA berücksichtigt und mit Breitbandtechnologien erweitert. Darüber hinaus sehen die Einsatzkräfte einen zusätzlichen Nutzen durch multisensorale Daten von (Video)Kameras oder Körpersensoren, um die Lagebilderstellung und Einsatzführung zu unterstützen.



4C4FirstResponder-Systemkomponenten

Mobile Multi-Sensor-Assistenzsysteme

Zur Unterstützung der Einsatzkräfte in Lagebilderstellung und Mission können diverse mobile Geräte verwendet werden; darunter sind mobile Kamerasysteme, „Smart Glasses" und tragbare Körpersensoren/-kameras. Mobile Sicherheitskräfte werden hierbei als „Human Sensor" eingebunden und haben auch die Möglichkeit, auf Sensorinformationen zuzugreifen. Die Evaluierung von geeigneter Hardware auf Basis der definierten Nutzeranforderungen sowie Usability-Tests in spezifischen Einsatzszenarien sind dabei wichtige Voraussetzungen.

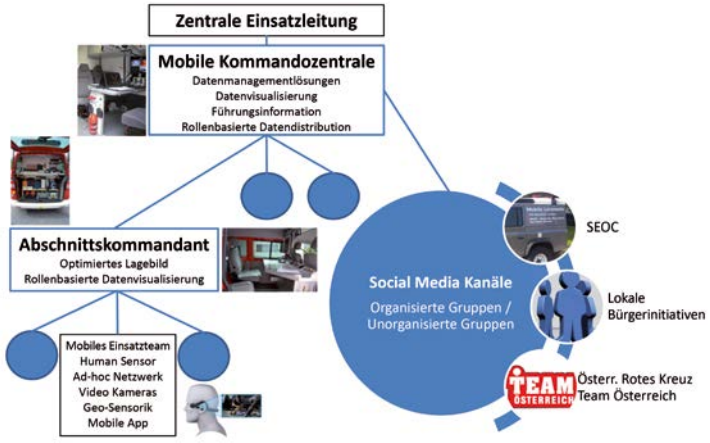
Dynamische Erstellung und Verteilung von lokalen Lagebildern

Im Verlauf des Projekts 4C4FirstResponder werden innovative Ansätze entwickelt und getestet, die eine effizientere Interaktion zwischen Einsatzzentrale und mobilen Einsatzteams ermöglichen. Dafür ist ein kontextsensitives Augmented-Reality-Assistenz- und Feedbacksystem geplant, welches sich dynamisch an die individuelle Einsatzsituation der Nutzer anpasst und bedarfsorientiert aktuell relevante Informationen anzeigt.
Das Lagebild entsteht aus Multi-Sensor-Daten wie Bildern, Videos, Text und Ton in Kombination mit situationsbezogenen Informationen (Position, Status, Kontext etc.) und kartographischen Referenzdaten.

Kommunikationsmanager

Eine wichtige Komponente der 4C4FirstResponder-Systemarchitektur ist der Kommunikationsmanager (KomMan). Dieser agiert als Broker zwischen Anforderungen der Applikation und den verfügbaren Ressourcen. Er wählt anhand der QoS-Anforderungen der Applikationen, der Charakteristika der zu übertragenden Daten und der aktuellen Eigenschaften der verfügbaren Kommunikationskanäle die passenden Netzwerkschnittstellen aus. Darüber hinaus werden die zu versendenden Daten an die verfügbaren Netzwerkressourcen angepasst und gruppen- und rollenbasiert verteilt. Der KomMan unterstützt auch eine Priorisierung von Kommunikationsaufgaben. Dies ist insbesondere in Situationen notwendig, in denen die Netzwerkressourcen nicht ausreichen, um alle Kommunikationsanforderungen zu erfüllen. Die Priorität der Daten wird dabei anhand von Applikations- bzw. Benutzervorgaben festgelegt.

Die Unterstützung von TETRA, welches unter den Einsatzkräften großes Vertrauen genießt, ist eine grundlegende Anforderung an den KomMan. Eine wichtige Aufgabe des KomMan ist es, TETRA mit Breitbandtechnologien zu vereinen, um zusätzliche Dienste wie Multimediakommunikation zu ermöglichen. Der KomMan ist als JAVA-Modul implementiert und auf Standard Plattformen wie Android-Smartphones oder Linux-basierten Routern einsetzbar.



Integrationskonzept des Kommunikationsmanager-Moduls

Projektleitung
JOANNEUM RESEARCH Forschungsges.mbH
DIGITAL, Institut für Informations- und Kommunikationstechnologien

Projektpartner
- Bundesministerium für Inneres
- Karl-Franzens-Universität Graz – Institut für Soziologie
- Lakeside Labs GmbH
- Ing. Richard Feischl, IFR
- Eurofunk Kappacher GmbH
- Dräger Safety Austria GmbH
- Freiwillige Feuerwehr Gumpoldskirchen

Kontakt
DI Alexander Almer
JOANNEUM RESEARCH
Forschungsges.mbH DIGITAL,
Institut für Informations- und
Kommunikationstechnologien
Steyrergasse 17, 8010 Graz
Tel.: +43 316 876-1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at

AMBOS

Abwehr von unbemannten Flugobjekten für Behörden und Organisationen mit Sicherheitsaufgaben

Unbemannte Luftfahrzeuge können in unterschiedlichsten Preis- und Gewichtsklassen mit Basisfunktionen bspw. Wegpunktnavigation oder programmierbaren digitalen Ausgängen kommerziell erworben werden. Dadurch sind potentiellen Angreifern sämtliche für einen Angriff notwendige Funktionalitäten verfügbar, wodurch diese Geräte eine potentielle Störgröße darstellen. Aus sicherheitspolitischer Sicht ist zur Aufrechterhaltung der Versorgungssicherheit mit lebenswichtigen Gütern und Dienstleistungen in und für Österreich eine Adaptierung an sich verändernde Bedrohungsszenarien von entscheidender Bedeutung. Der Schutz der kritischen Infrastruktur ist zum derzeitigen Zeitpunkt je nach individuellem Bedrohungspotential unterschiedlich ausgerichtet. Vor allem im zivilen Bereich ist diese Problemstellung bisher von Forschung und Industrie nur unzureichend adressiert worden, wodurch unzureichend Forschungsergebnisse vorhanden sind.

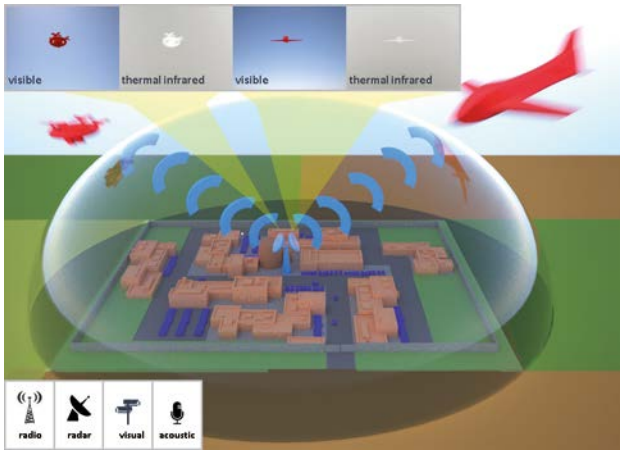
Basierend auf den grenzübergreifenden Erkenntnissen vom deutschen G7-Gipfeltreffen 2015 und dem österreichischen Bilderbergtreffen 2015, wurden technologische, rechtliche und ethische Herausforderungen festgestellt, die in diesem Projekt zielgerichtet adressiert werden. Bei diesen Treffen konnten das deutsche Bundeskriminalamt Wiesbaden und das österreichische Bundesministerium für Inneres bereits sehr eng und effizient zusammenarbeiten, um die Sicherheit ihrer Gäste zu gewährleisten. Dieses bilaterale Forschungsprojekt knüpft an die grenzübergreifenden Erkenntnisse an und geht die entscheidenden nächsten Schritte.

Das übergeordnete Ziel des Projekts ist die Entwicklung und Evaluierung von Technologiekomponenten zur Erkennung und Abwehr potentieller Bedrohungen durch verhältnismäßige Mittel der Intervention sowie zur Lagebilderstellung und Entscheidungsunterstützung. Die entwickelten Technologiekomponenten werden anhand ausgewählter behördlich-relevanter Szenarien demonstriert. Dabei werden unterschiedliche Sensormodalitäten, die beim G7-Gipfeltreffen in Elmau 2015 und dem Bilderbergtreffen in Telfs/Tirol 2015 nur autark eingesetzt wurden, miteinander fusioniert, um in der Gesamtheit eine robuste Sensorik zu ermöglichen.

Der besondere Innovationsgehalt des Projekts umfasst sowohl technologische Bereiche, die eine wesentliche Verbesserung der Technologien zum aktuellen Stand der Technik im Kontext des Projekts erlauben, als auch sozialwissenschaftliche Innovationen, die die im Rahmen des Projekts entwickelte zivile Lösung der Entscheidungsunterstützung zur Luftabwehr unter ethischen und rechtlichen Aspekten erst ermöglichen. Insbesondere trägt dieses Projekt wesentlich zur Fusion der unterschiedlichen Sensortechnologien bei, die bisher noch nicht verfügbar ist und aus aktuellen behördlichen Erfahrungen einen wesentlichen Mehrwert darstellt. Zusätzlich werden Benutzerprozesse und -regelungen zur allgemeinen Technologienutzung sowie zur Entscheidungsunterstützung erarbeitet.

Methodisch wird dabei ein dreistufiger Prozess verfolgt, bestehend aus Detektion, Verifikation und Intervention:

- Die Detektionsphase beinhaltet die individuelle Erkennung mittels unterschiedlicher Sensormodalitäten, die Datenfusion und Nachverfolgung dieser Hypothesen. Die untersuchten Sensormodalitäten sind monokulare und stereoskopische elektrooptische Verfahren, thermisches Infrarot-Verfahren, Akustik und Radar, wobei diese jeweils stationär oder teilweise mobil eingesetzt werden können.
- In der Verifikationsphase wird eine Kamera nachgeführt, um durch dieses vergrößerte Bild automatisch eine verbesserte Klassifikation durchführen zu können. Zusätzlich wird in der Lagebilddarstellung in einem Human-In-The-Loop-Ansatz eine manuelle Verifikation ermöglicht.
- In der Interventionsphase soll das verifizierte Objekt beeinflusst werden.



Visualisierung eines Szenarios zum Schutz kritischer Infrastrukturen

Ein besonderer Fokus liegt dabei auf der Schaffung eines technologischen Mehrwerts der eingesetzten Technologien in Bezug zum Stand der Technik sowie eines Betriebsleitfadens zur behördlichen Anwendung der Technologie. Die Ergebnisse werden in Form eines funktionalen Technologieträgers, anhand der behördlich-relevanten Szenarien, gezeigt.

Die Abbildung illustriert ein mögliches Szenario zum Schutz einer kritischen Infrastruktur. Ein regional abgegrenzter Bereich wird durch multimodale Sensorik u.a. visueller, akustischer und Radarsensorik hinsichtlich eindringender Bedrohungen aus dem Luftraum überwacht. Die fusionierte Sensorinformation wird in einer Lagebilddarstellung dem Operator visualisiert, der verhältnismäßige Maßnahmen zur Intervention einleiten kann.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Autonomous Systems Center for Vision, Automation & Control

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Bundesministerium für Verkehr
- Donau Universität Krems, Zentrum für Integrierte Sensorsysteme
- CNS-Solutions & Support GmbH
- INRAS GmbH
- Austro Control Österreichische Gesellschaft für Zivilluftfahrt mbH
- Joanneum Research Forschungsgesellschaft mbH
- Frequentis AG

Kontakt
Christoph Sulzbachner
AIT – Austrian Institute of Technology GmbH
Autonomous Systems Center for Vision, Automation & Control
Donau-City-Straße 1, 1220 Wien
Tel.: +43 50550-4177
christoph.sulzbachner@ait.ac.at
www.ait.ac.at

BITCRIME

Verfolgung und Prävention organisierter Finanzkriminalität mit virtuellen Währungen

Das bilaterale Forschungsprojekt BITCRIME erforschte innovative Lösungen zur Identifikation, Prävention und Reduktion der organisierten Finanzkriminalität am Beispiel der Geldwäsche und mit besonderer Hinsicht auf virtuelle Kryptowährungen. Das Projekt entwickelte (Ermittlungs-)technische, wissenschaftliche und rechtliche Ansätze und zielte darauf ab, die Sicherheit beim Umgang mit virtuellen Kryptowährungen zu erhöhen sowie legale Nutzer vor Bedrohungen durch virtuelle Währungen zu schützen.

Das österreichische Teilprojekt hat zwei an den wichtigsten Herausforderungen der Bedarfsträger ausgerichtete Hauptergebnisse produziert. Zum einen wurde eine Reihe von Berichten erstellt, die PolitikerInnen, JuristInnen und Behörden Grundlagen für die wirtschaftliche Einordnung von virtuellen Währungen zur Verfügung stellen. Zum anderen wurden Methoden und Algorithmen entwickelt, die

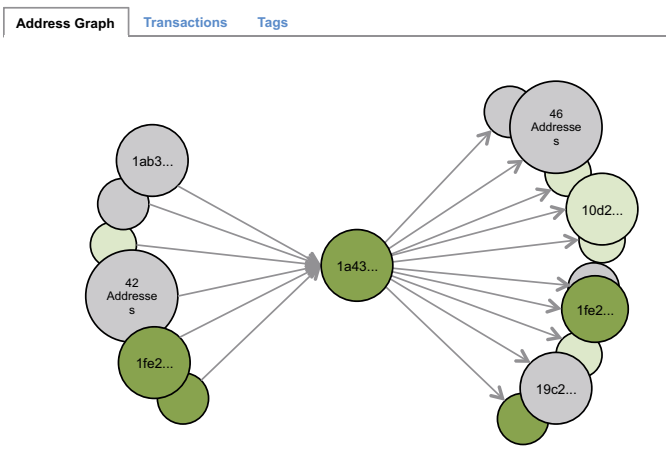
- Transaktionen mit der virtuellen Währung Bitcoin aggregieren, um spezifische Entitäten zu identifizieren,
- diese Transaktionen beobachten, um potentielle kriminelle Aktivitäten auszumachen, und
- diese Transaktionen zu Aktivitäten in versteckten sozialen Netzwerken in Verbindung bringen, um die De-Anonymisierung von AkteurInnen zu unterstützen.

Die im Rahmen des Projekts entwickelte, diese Methoden umsetzende Software wurde bei den Bedarfsträgern installiert, getestet und evaluiert.

Es wurden forensische Methoden zur Inspektion und Verfolgung von Bitcoin-Transaktionen sowie ein Crawler für Darknet-Marktplätze entwickelt, die testweise bereits in realen Fällen zum Einsatz kamen. Die in BITCRIME entwickelten Transaktionsanalysemethoden werden im Rahmen des Projektes GraphSense (bmvit/IKT der Zukunft) weiterentwickelt und somit in weiteren Folgeprojekten zum Einsatz kommen. Das resultierende prototypische Tool kann Transaktionsflüsse zwischen Bitcoin-Adressen inspizieren, Bitcoin-Adressen zu Clustern zusammenfassen und durch Integration externer, kontextuell relevanter Information (z. B. tags) einen Bezug zwischen Bitcoin-Adressen und realweltlichen Akteuren herstellen. Die Basisdaten für die Analyse liefert der Darknet-Crawler, der die Durchsuchung und Archivierung sowie Caching und Versionierung von Darknet-Inhalten ermöglicht. Darüber hinaus ermöglicht er eine gezielte Suche nach Wallet-IDs zur Identifikation illegaler Transaktionen und Crawling von passwortgeschützten

Summary	
No. Transactions	1887 { 1782 | 105 }
First Usage	2013-09-05 21:10:26
Last Usage	2016-10-18 21:29:56
Total Received	130.42245965BTC
Final Balance	31.634123445BTC

Address Cluster	
No. Addresses	4
No. Transactions	2754 { 2639 | 115 }
First Usage	2011-12-07 22:58:12
Last Usage	2016-10-18 21:29:56
Total Received	1080.72654572BTC
Final Balance	32.1571249BTC



Das in BITCRIME entwickelte Bitcoin-Transaktionsanalysetool.

Darknet-Foren. Das Bitcoin-Transaktionsanalysetool wurde von österreichischen und deutschen Behörden in realen Ermittlungen in den Bereichen Drogenhandel, Kinderpornographie und Terrorismus-Finanzierung eingesetzt.

Die im Rahmen von BITCRIME erstellten Berichte zur wirtschaftlichen und rechtlichen Einordnung von virtuellen Währungen leisten einen wichtigen Beitrag zur Klärung von Sicherheits- und Rechtsfragen im Kontext von virtuellen Kryptowährungen in Österreich, Deutschland und im europäischen Raum. Zum einen wurden Globale Treiber und Akteure (bzw. Akteursgruppen) identifiziert, zum anderen Prozesse und Regulatoren unter Einbeziehung der Globalen Treiber den Akteuren zugeordnet. Verhaltensmuster klassischer Geldwäsche wurden analysiert und auf den Bereich der Kryptowährungen übertragen. Rechtliche Rahmenbedingungen zur Erfassung illegaler Transaktionen mittels Bitcoins wurden analysiert und ausgewertet. Der Stand der Forschung zu organisierter Kriminalität bzw. illegalen Märkten mit Verbindung zu virtuellen Währungen wurde durch Einbeziehung österreichischer Stakeholder qualitativ und quantitativ erhoben.

Das Konsortium sieht BITCRIMEs Potenzial hauptsächlich in Law Enforcement- sowie Finanzmärkten. Im Projektzeitraum konnte durch zwei zeitlich verschobene Datenbankabfragen ein merklicher Anstieg von Unternehmen, welche sich mit Kryptowährungen (Bitcoins, litecoins, peercoins etc.) beschäftigen, festgestellt werden. Hauptsächlich handelt es sich dabei um Start-Ups, welche vor allem in den USA angesiedelt sind. Zusätzlich sind vermehrt Medienberichte identifizierbar, welche vor allem Bitcoins als zukünftiges Zahlungsmittel anpreisen. Des Weiteren ist das Potential der Block-Chain-Technologie noch nicht ausgeschöpft und weiterer Forschungsbedarf gegeben.

Im Rahmen der Verwertungsplanung wurde, basierend auf den Ergebnissen der bei den Bedarfsträgern BM.I und BMF durchgeführten Bedarfserhebungen, ein Produktkonzept erstellt. Die resultierenden Virtual Currency Analytics wurden als TRL-5 Level Web Applikation Prototyp implementiert. Während der Projektlaufzeit konnte das BITCRIME-Konsortium erfolgreich erste Schritte zur Etablierung der Ergebnisse bei den österreichischen Bedarfsträgern einleiten. Eine User Mailingliste, die jetzt aus ca. 130 LEA (Law Enforcement Agency) aus Deutschland, Österreich und weiteren Ländern besteht, wurde aufgesetzt.

Die Erkenntnisse der österreichischen Bedarfsträger wurden herangezogen, um die Ergebnisse nach Abschluss des Projekts auf Produktreife weiterzuentwickeln. AIT leitet derzeit die nächsten Schritte zur Weiterentwicklung der Software ein, um diese produktreif zu machen, und investiert Eigenmittel, um diese auf einer SAAS-Plattform für internationale Kunden anbieten zu können. In einem weiteren Schritt soll ein Businessmodell für dieses Service ausgearbeitet werden. Darüber hinaus erweitern Kernpartner des österreichisch-deutschen BITCRIME-Konsortiums im H2020-Folgeprojekt TITANIUM die Forschungen auf europäische Ebene. Dieses Projekt hat ein Volumen von 5 Millionen Euro mit 15 Partnern aus 7 europäischen Ländern. Das Projekt befasst sich mit der Weiterentwicklung der BITCRIME-Forschungsergebnisse und startet im Mai 2017.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Finanzen
- Xylem – Science and Technology Management GmbH
- IRKS Research GmbH
- SBA Research gemeinnützige GmbH
- M2D MasterMind Development GmbH

Kontakt
Dr. Ross King
AIT – Austrian Institute of Technology GmbH
Donau-City-Strasse 1, 1220 Wien
Tel.: +43 50550-4271
E-Mail: ross.king@ait.ac.at
www.ait.ac.at

CERBERUS

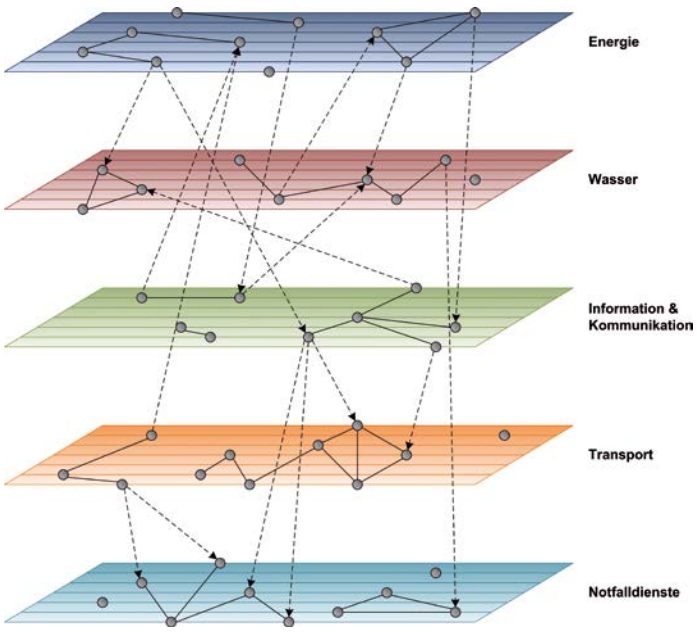
Cross Sectoral Risk Management for Object Protection of Critical Infrastructures

Kritische Infrastrukturen bilden einen zentralen Eckpfeiler der Gesellschaft. Insbesondere aufgrund der starken Abhängigkeiten zwischen diesen Infrastrukturen bleiben Zwischenfälle meist nicht auf eine Organisation beschränkt, sondern haben teilweise weitreichende Kaskadeneffekte. Daher bedarf es eines umfassenden Risikomanagements, um potentielle Bedrohungen früh identifizieren und deren Auswirkungen bewerten zu können. In CERBERUS wird ein derartiger Risikomanagementansatz konzipiert und in Form eines Demonstrators exemplarisch umgesetzt.

Im Allgemeinen werden als kritische Infrastrukturen jene Anlagen, Systeme oder Teile davon bezeichnet, die für die Aufrechterhaltung wesentlicher gesellschaftlicher Funktionen verantwortlich sind und deren Störung oder Ausfall erhebliche Auswirkungen auf das wirtschaftliche und soziale Wohlergehen der Bevölkerung haben. Kritische Infrastrukturen sind daher von signifikanter Bedeutung für die Aufrechterhaltung zentraler gesellschaftlicher Abläufe, wie etwa der Versorgung mit lebensnotwendigen Gütern und Dienstleistungen. Diese kritischen Infrastrukturen sind in unterschiedlichen Bereichen zu finden und umfassen sowohl die grundlegenden Versorgungsnetzwerke (Strom, Gas, Wasser) als auch Informations- und Kommunikationsnetzwerke und reichen bis hin zu Systemen mit komplexen Verflechtungen, etwa medizinische Versorgung oder Transportnetzwerke. Durch die stetig wachsenden und immer komplexeren Verbindungen zwischen den einzelnen kritischen Infrastrukturen nehmen auch die Interdependenzen untereinander zu, woraus sich ein höchst sensibles Netzwerk von Netzwerken ergibt.

Aufgrund dieser stark verflochtenen Zusammenhänge und Abhängigkeiten ist deutlich, dass eine Beeinträchtigung oder gar der Ausfall einer kritischen Infrastruktur nicht nur diese Infrastruktur alleine betrifft, sondern potentiell auch Auswirkungen auf eine Reihe anderer kritischer Infrastrukturen sowie auf das wirtschaftliche und soziale Wohlergehen der Bevölkerung haben kann. Allein für den Bereich der Energiewirtschaft und Elektrizitätsversorgung zeigten dies die beiden Studien BlackÖ.1 und BlackÖ.2, welche aus den gleichnamigen KIRAS-Projekten hervorgingen, sowie das tatsächliche zwölfstündige Blackout in Italien im Jahr 2003, aus dem ein finanzieller Schaden von ca. 1,182 Milliarden Euro resultierte.

Ein zentraler Ansatzpunkt, um solch einer Beeinträchtigung oder einem Ausfall entgegenzuwirken, ist der Einsatz einer entsprechenden Sicherheitsarchitektur sowie eines Risikomanagementsystems. Einen speziellen Platz nimmt in diesem Zusammenhang der physische Schutz (Objektschutz) der Infrastrukturen ein, welcher vor allem den Umgang mit natürlichen oder durch Menschen verur-



Schematische Darstellung der Abhängigkeiten zwischen kritischen Infrastrukturen

sachten Bedrohungen betrachtet. Im Projekt CERBERUS werden Informationen zum Objektschutz kritischer Infrastrukturen strukturiert aufbereitet und in einem neuartigen Risikomodell zusammengefasst.

Einen zentralen Aspekt in CERBERUS stellen die Interdependenzen zwischen kritischen Infrastrukturen dar. Mit den aktuell zur Verfügung stehenden Risikomanagementansätzen ist es kaum möglich, Verbindungen und Abhängigkeiten zwischen den einzelnen kritischen Infrastrukturen explizit zu identifizieren und darzustellen. Um jedoch einen Gesamtüberblick über die aktuelle Situation der kritischen Infrastrukturen eines bestimmten Gebietes, eines oder mehrerer Sektoren sowie auf nationaler Ebene zu erhalten, sind diese Abhängigkeiten von zentraler Bedeutung. Fehlt eine Beschreibung dieser Interdependenzen, können weitläufige und wesentliche indirekte Folgen (Kaskadeneffekte) eines Ereignisses bei einer kritischen Infrastruktur unbemerkt bleiben. Daher wird im Projekt CERBERUS eine strukturierte Darstellung dieser Abhängigkeiten sowie ein mathematisches Modell für die Beschreibung der Kaskadeneffekte entwickelt.

Darüber hinaus ist es ebenfalls schwierig, konkrete Aussagen über die Resilienz einzelner kritischer Infrastrukturen zu treffen. So sind zwar die Informationen aus den derzeit erhobenen Daten der Infrastrukturen für eine Risikobewertung verfügbar, die Auswirkungen des Ausfalls einer einzelnen Infrastruktur auf das gesamte Netzwerk in Österreich können aber daraus nur schwer abgeleitet werden. Eine Verbesserung wird hier durch die Definition von Resilienzmetriken im Zuge des Projekts erreicht.

Ein Großteil der Bewertung von Risiken basiert auf Einschätzungen der Betreiber kritischer Infrastrukturen oder der entsprechenden ExpertInnen in diesen Organisationen. Hierbei können Probleme auftreten, wenn Einschätzungen von Personen mit unterschiedlicher Risikoeinstellung verglichen oder aggregiert werden müssen. Eine zu hohe Einstufung von Bedrohungen (z. B. durch eine eher vorsichtige Person) ist ebenso nachteilig wie eine zu niedrige Einstufung. Um dem entgegenzuwirken, werden im Zuge von CERBERUS mathematische Methoden eingesetzt, um eine Harmonisierung der Einschätzungen zu erreichen.

Ein zusätzliches Problem für die Risikobewertung ist, dass es aktuell keine einheitliche Referenz oder Guideline im Bereich Objektschutz für die österreichischen kritischen Infrastrukturen gibt. Zwar werden bei den einzelnen Infrastrukturen internationale Standards und Richtlinien für das Risikomanagement (wie etwa die ISO 31000, die ISO 27005 oder die Special Publications der NIST) herangezogen, die Vielfalt und unterschiedliche Ausprägung dieser Standards erschwert jedoch einen Vergleich oder eine Aggregation verschiedener Bewertungen. Im Zuge des Projekts wird hier durch die Erarbeitung einer nationalen Referenz-Guideline Abhilfe geschaffen.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Universität Wien
- Alpen-Adria-Universität Klagenfurt
- avedos business solutions GmbH
- Institut für empirische Sozialforschung GmbH (IFES)

Kontakt
DI Dr. Stefan Schauer
Austrian Institute of Technology GmbH
Lakeside B10a, 9020 Klagenfurt
Tel.: +43 50 550 4055
E-Mail: stefan.schauer@ait.ac.at
www.ait.ac.at

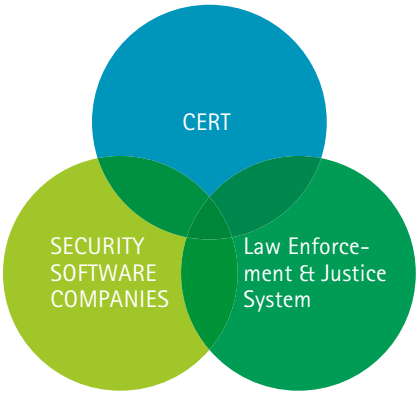
CERT-Komm II

Computer Emergency Response Teams (CERT) Kommunikationsmodell II

Im Cyberraum nehmen die Bedrohungen rasant zu, insbesondere sind auch immer stärker kritische Infrastrukturen betroffen. Daher vermehren sich auch die Aufgaben der „Feuerwehren im Internet" – der CERTs. Dies erfordert eine Verstärkung der Kommunikation und des Austausches mit den anderen IKT-Sicherheits-Stakeholdern im Cyberraum. Das Projekt CERT-Komm II baut auf der Studie CERT-Komm I auf und geht der Frage nach, welche gemeinsamen Ziele die Stakeholder verfolgen und wie ihre Anstrengungen bei der Bekämpfung von aktuell gravierenden Bedrohungen, wie Botnetzen und gezielten Angriffen APTs (Advanced Persistent Threats), gebündelt werden können. Das Ergebnis des Projekts ist ein Demonstrator einer Software, die die Aufgabe hat, den Stakeholdern im Cyberraum Hilfestellung bei jenen rechtlichen Fragestellungen zu bieten, die bei ihrer Kommunikation zu berücksichtigen sind. Um den Demonstrator mit allen notwendigen Inhalten zu füllen, erarbeitet ein multidisziplinäres Projektteam technische, soziologische und kriminologische sowie juristische Rahmenbedingungen.

Technische Rahmenbedingungen für die Bekämpfung von APTs und Botnetzen

In einem ersten Schritt wurden im Projekt CERT-Komm II die IT-Sicherheitsziele der im Cyberraum aktiven Stakeholder analysiert. Der Wunsch, einen gemeinsamen, geschützten und funktionstüchtigen Cyberspace zu erhalten, gilt für alle diese Stakeholder. Allerdings hat sich gezeigt, dass beispielsweise bei CERTs oder Sicherheitsanbietern trotz gemeinsamer genereller Ausrichtung jeder der Akteure einen unterschiedlichen Schwerpunkt hinsichtlich der Sicherheitsziele hat, der über die Schnittmenge der gemeinsamen Sicherheitsziele hinausgeht. Klarerweise sind Kommunikation und Kooperation nur dann möglich, wenn es sich um die Realisierung gemeinsamer Ziele handelt.



Schnittmenge gemeinsamer Sicherheitsziele der beteiligten Stakeholder

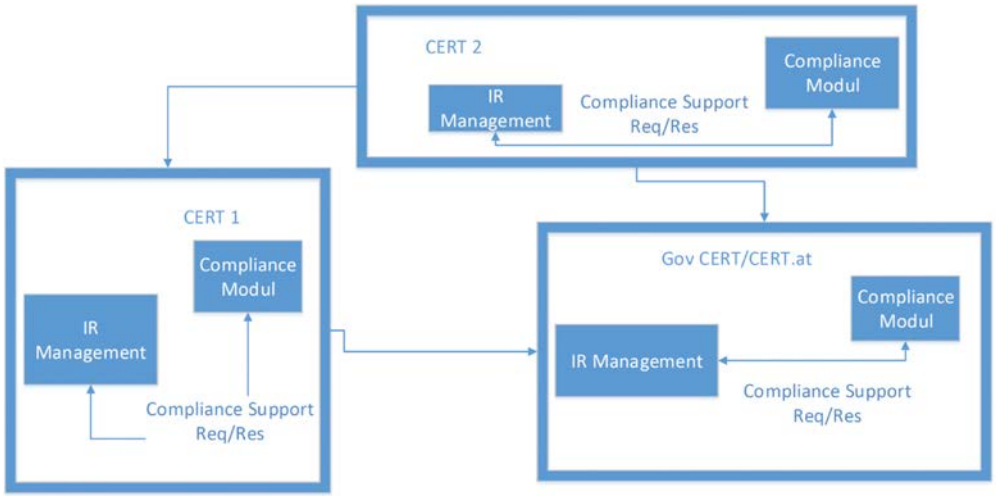
Soziologische und kriminologische Rahmenbedingungen für CERTs

Wissensaustausch unter den internationalen CERTs sowie Kompetenzaufbau stehen im Vordergrund der grenzüberschreitenden Kooperation. Dazu wird eine internationale Befragung unter den CERTs durchgeführt. Die Ergebnisse der empirischen Befragung stellen den Bedarf der CERTs dar und dienen als Grundlage der rechtlichen, technischen und organisatorischen Entwicklung des Demonstrators. Darüber hinaus werden gerichtlich bekannte Cybercrime-Vorfälle der letzten zehn Jahre analysiert, um den typischen Modus Operandi der Täter besser verstehen zu können.

Rechtsrahmen für CERTs

Im Rahmen des Projekts erfolgt außerdem die Erfassung der Rechtslage für CERTs mit besonderem Augenmerk auf die kürzlich von der EU verabschiedete NIS-Richtlinie (Network and Information Security Directive). Diese wird in Österreich mit dem geplanten Cybersicherheitsgesetz umgesetzt und betrifft Betreiber wesentlicher Dienste (kritische Infrastrukturen) und bestimmte Anbieter digitaler Dienste (Suchmaschinen etc.). Entscheidende Themen dieser Richtlinie sind die Meldepflicht von Sicherheitsvorfällen mit erheblichen Auswirkungen auf die Verfügbarkeit der bereitgestellten Dienste sowie die freiwillige Meldung von Vorfällen, die auch im Hinblick auf den Datenschutz zu betrachten sind. In weiterer Folge werden Lösungsansätze für die rechtliche Umsetzung in Österreich im Hinblick auf die Kommunikation von CERTs formuliert, um insbesondere den Vertrauensaufbau zu den CERTs zu fördern. Bei der IRIS 2017-Konferenz in Salzburg wurde zu diesem Thema ein Vortrag gehalten und ein Beitrag im Tagungsband publiziert.

Publizierter Tagungsband bei der IRIS 2017-Konferenz in Salzburg



Compliance Modul für CERTs

Demonstrator

Zur Realisierung des Demonstrators müssen dessen Inhalte im Detail festgelegt und seine technische Ausprägung spezifiziert werden. Letzter Schritt im Projekt ist daher die Realisierung des Demonstrators für das Compliance Modul.

Die gezeigte Grafik erläutert die Funktionalität des Compliance Moduls. Dieses soll das CERT unterstützen, indem insbesondere die Kommunikation mit anderen CERTs und Kommunikationspartnern im Einklang (compliant) mit den rechtlichen und allfälligen sonstigen Anforderungen ist (Datenschutzgesetz, NIS-RL, Behandlung von freiwilligen und verpflichtenden Meldungen von IT-Sicherheits-Zwischenfällen lt. NIS-RL, Cybersicherheitsgesetz, Arbeitsrecht, z. B. Betriebsvereinbarung, Betriebsrat, interne Regeln). Die im Projektverlauf erhobenen und behandelten Fragestellungen werden in das System eingepflegt und dieses wird auch erweiterbar gestaltet.

Mit Hilfe des Compliance Moduls kann die Kommunikation zwischen CERTs erheblich erleichtert werden, weil die relevanten rechtlichen Fragen jeweils abgesichert und nicht im Einzelfall zu klären sind.

Projektleitung
SBA Research gGmbH

Projektpartner
- Bundeskanzleramt
- Universität Wien, Forschungsgruppe Multimedia Information Systems
- Donau-Universität Krems, Zentrum für Infrastrukturelle Sicherheit
- Research Institute AG & Co KG
- IKARUS Security Software GmbH

Kontakt
SBA Research GmbH
Dr. Edgar Weippl, Dr. Otto Hellwig
Favoritenstraße 16, 1040 Wien
Tel.: +43 1 505 36 88
E-Mail: eweippl@sba-research.org,
ohellwig@sba-research.org
www.sba-research.org

CISA – Cyber Incitent Situation Awareness

Lagebewusstsein für Cyberbedrohungen

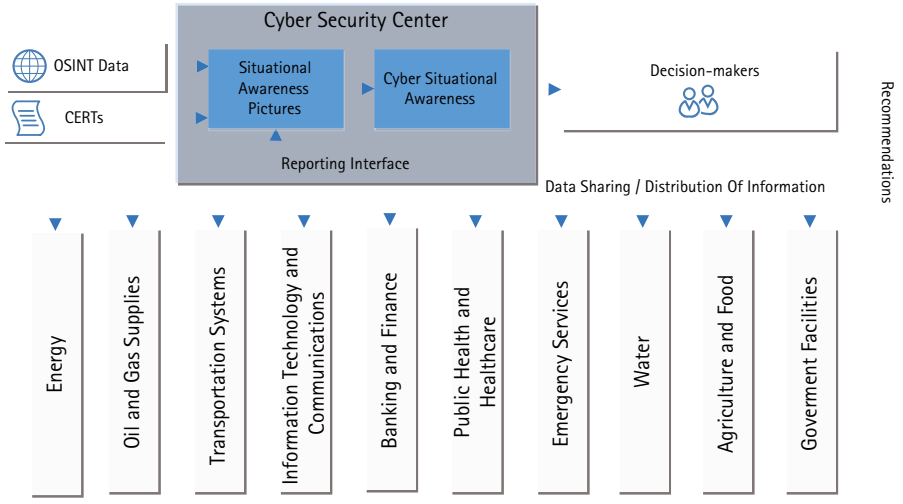
Die finale Version der NIS Richtlinie (Network and Information Security Directive) schreibt fest, dass Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste unter bestimmten Umständen Cybersicherheitsvorfälle (z. B. Angriffe, welche in Ausfällen resultieren) behördlich melden müssen. Es ist dann die Aufgabe der Behörde(n), diese Meldungen aufzunehmen und zu verarbeiten, um die Cybersicherheit aller Organisationen zu erhöhen. Mögliche Maßnahmen reichen beispielsweise von Frühwarnungen an weitere potentiell betroffene Organisationen, über Assistenz bei der Behebung einer Störung bis zu Verteilung von Empfehlungen innerhalb eines Wirtschaftssektors. Jedoch ist es essentiell, ein Cyberlageverständnis und -bewusstsein (cyber situational awareness) zu etablieren, um Entscheidungen bezüglich effektiver Maßnahmen zu fällen. Die Erstellung angemessener Lagebilder ist eine höchst komplexe, nicht-triviale Aufgabe.

Kritische Dienstleistungen wie Energieversorgung, Transportwesen und Bankenwesen werden weitgehend von privaten Betreibern angeboten. Da diese Dienstleistungen für die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit unerlässlich sind, ist es Aufgabe des Staates – und im besten Interesse des Staates – , die Sicherheit der damit verbundenen Infrastrukturen zu gewährleisten. Es muss daher eine formale Vereinbarung zwischen dem öffentlichen und dem privaten Sektor geschaffen werden, in der die Kooperation geregelt ist. Idealerweise würde der Staat direkt Infrastrukturanbieter beim sicheren Betrieb unterstützen, indem er ihnen wichtige Sicherheitsinformationen zur Verfügung stellt. Die Infrastrukturanbieter würden wiederum dem Staat sicherheitsrelevante Informationen wie den Status ihrer Dienstleistungen oder erkannte Angriffe (bzw. -versuche) in ihren Netzen melden. Diese Daten aus jeder einzelnen Organisation sind von wesentlicher Bedeutung, um ein klares Lagebild und in Folge Cyberlagebewusstsein für das betriebliche Umfeld zu schaffen und so die Grundlage für eine gerechtfertigte und effektive Entscheidungsfindung der Behörden auf nationaler Ebene zu etablieren.

In den vergangenen Jahren wurden technische Lösungen zur Erfassung von Netzwerkdaten und deren Verarbeitung innerhalb von Organisationen entwickelt und allgemeine Sicherheitsstrategien im nationalen Geltungsbereich formuliert. Allerdings ist die Frage, wie technische Informationen aus dem Cyberspace in einem solchen Cyberlagebild verarbeitet und präsentiert werden können – ein herausforderndes Problem, für das es noch keine adäquate Lösung gibt. Ziel des Projekts CISA ist es, diese Lücke zu schließen und eine Verbindung zwischen den technischen Daten und den strategischen Entscheidungen zu schaffen, die zur Minderung von Cyberbedrohungen auf nationaler Ebene erforderlich sind. Cyberlagebewusstsein ist eine erforderliche Fähigkeit der nationalen Bedarfsträger, ihre Operationen, die sich auf das aktuelle Wissen über den technischen Status kritischer Infrastrukturen stützen, effektiv auszuführen. Dieses Lagebewusstsein erfordert eine ausgefeilte Methodik, um die aktuelle Lage zu ermitteln, Trends zu identifizieren, visuell darzustellen und zukünftige Entwicklungen abzuschätzen.

Die CISA-Designprinzipien

CISA sieht sowohl die Involvierung privater als auch staatlicher Stakeholder vor, um Informationen mit einem Cybersicherheitszentrum zu teilen. Die Struktur deckt dabei alle Management- und Entscheidungsebenen ab, von der technischen, über die organisatorische Managementebene bis hin zur strategisch-politischen Ebene, um eine gemeinsame Sicht auf die Cybersicherheitslage zu etablieren. Hier ist es wichtig, ein Verständnis der zahlreichen Kategorien relevanter Informationen zu erlangen, die jeweils spezifisch behandelt werden müssen. Zum Beispiel müssen technische Informationen, wie IP-Adressen von Command-und Control-Servern oder Beschreibungen von technischen Schwachstellen, anders modelliert und geteilt werden als etwa abstraktere Geschäftsinformationen, wie z. B. die potenziellen wirtschaftlichen Auswirkungen aufgrund von Ausfällen bestimmter Dienste. CISA zielt darauf ab, bestehende Organisationsstrukturen und Kommunikationskanäle (z. B. Links zu CSIRTs, Computer Security Incident Response Teams) zu verwenden, um unnötige Kosten zu vermeiden und die Barrieren, CISA zu nutzen, für alle Stakeholder zu senken. Weiters legt CISA Wert auf die angemessene Balance zwischen manuellen, menschlich kontrollierten Aktivitäten (wie z. B. Vorfallsklassifizierung oder Vorbereitung von Empfehlungen) und automatisch ablaufenden Prozessen (wie Datenanalyse zwecks Intrusion Detection).



Ansatz zur Etablierung eines nationalen Cyberlagebewusstseins für Entscheidungsträger

Das Modell sieht vor, dass in einem (oder mehreren) Cybersicherheitszentrum/-en zahlreiche Cyberlagebilder entstehen – je nach Art des betroffenen Entscheidungsträgers (zivil, militärisch) und der Ebene, auf der die Entscheidungen getroffen werden müssen (operativ, taktisch, strategisch). Diese Lagebilder können mit externen öffentlichen Informationen (OSINT: Open Source Intelligence) von CSIRTs sowie mit nicht-öffentlichen (nationalen, europäischen) Quellen weiter angereichert werden. Schließlich werden Empfehlungen für sorgfältig ausgewählte Empfängerkreise ausgegeben, um die Auswirkungen von aktuellen Vorfällen abzuschwächen und die Vorbereitung auf zukünftige zu erhöhen (z. B. durch Verteilung von Frühwarnungen).

Neben der Entwicklung wissenschaftlicher Methoden ist die ordnungsgemäße Demonstration der Anwendbarkeit der Ergebnisse von CISA in einem realen Umfeld von großer Bedeutung, um das geplante System zu testen und zu bewerten. Daher sind mit den zuständigen Behörden Übungen mit externen Stakeholdern auf nationaler Ebene geplant.

Projektleitung
AIT – Austrian Institute of Technology GmbH, Center for Digital Safety and Security

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Bundeskanzleramt
- Thales Austria
- Secure Business Austria
- REPUCO Unternehmensberatung GmbH
- Infraprotect GmbH
- Wiener Zentrum für Rechtsinformatik
- T-System Austria

Kontakt
Dr. Dr. Florian Skopik
AIT – Austrian Institute of Technology, Center for Digital Safety and Security
Donau-City-Straße 1, 1220 Wien
Telefon: +43 664 8251495
E-Mail: florian.skopik@ait.ac.at
www.ait.ac.at

Couragierte Gemeinde

Produktentwicklung zur zivilgesellschaftlichen Handlungsfähigkeit bei gewaltbereitem Verhalten von Jugendlichen

Couragierte Gemeinde entwickelt ein Modell, mit dem Gemeinden Gewalt, Vandalismus und Kriminalität von Jugendlichen entgegentreten können. Nach dem Konzept der Neuen Autorität werden Netzwerke gebildet, die auf gewaltlosem Widerstand, Präsenz und wachsamer Sorge der Erwachsenen beruhen. Wissenschafts-, Wirtschaftspartner und Bedarfsträger entwickeln das Modell, das in der Stadtgemeinde Ansfelden/Oberösterreich getestet wird. Ein Tool-Kit (Leitsystem, IT-Lösung) soll künftig in allen Gemeinden Österreichs eingesetzt werden können.

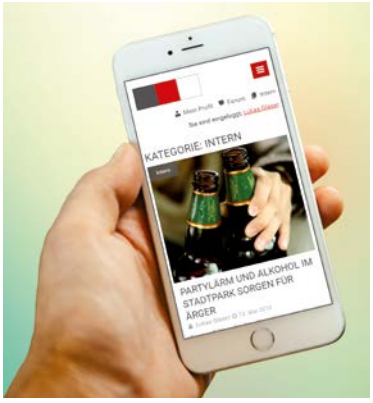
Das Tool-Kit umfasst hilfreiches Trainingsmaterial zur Haltung der Neuen Autorität und für die Umsetzung auf Gemeindeebene. Aus Holz wurde ein Prototyp hergestellt, der äußerlich einem Rathaus gleicht: mit sieben Säulen (den sieben Prinzipien der Neuen Autorität entsprechend), einer Basis und einem Dach. In der Basisschublade befinden sich vier Körbe, die der Klärung der Ressourcen für ein friedliches Miteinander dienen. Mit Hilfe eines Ampelsystems werden jene Verhaltensweisen identifiziert, gegen die ein kommunales Netzwerk für Zivilcourage Widerstand leistet. Die sieben hochformatigen Säulen enthalten Erklärungskarten zu Methoden (inkl. IT-Lösung) und Beispielen der Neuen Autorität. Unter dem Dach finden sich Informationen zu Zivilcourage und zu Rechten und Pflichten der BürgerInnen. Durch eine Bedarfsanalyse auf der Basis von Interviews und Exkursionen an „Orten des Geschehens" wurde die Prototypentwicklung wissenschaftlich begleitet.

Ein Informationsabend am 9. Mai 2016 im Stadtsaal Haid in Ansfelden war gut besucht. Über 40 Interessierte holten sich Infos aus erster Hand. Mitglieder des Projektteams stellten das Projekt Couragierte Gemeinde vor und luden die Anwesenden dazu ein, Teil des „Netzwerk Zivilcourage" zu werden. Am 3. Juni fand der erste Basis-Workshop statt. Weitere folgten am 21. Juni und 6. Juli. Dabei beschäftigten sich die Teilnehmenden mit den Themen Zivilcourage und Neue Autorität. Neben Theorie gab es die Möglichkeit praxisnaher Übungen. An diesen rund dreistündigen Workshops nahmen insgesamt 23 Interessierte teil. Am 25. Oktober 2016 wurde das „Netzwerk Zivilcourage" gegründet. Am 17. Jänner 2017 fand der Info-Abend „Mutig sein – sich einmischen – Verantwortung übernehmen" statt. Dabei erläuterte Chefinspektor Thomas Schmolz (Bezirkspolizeikommando Linz-Land) wesentliche rechtliche Grundlagen: Mutiges Einschreiten – Was darf ich tun? Wann soll ich/wann muss ich die Polizei rufen? Notwehr/Nothilfe.

Gegenwärtig treffen sich im Rahmen der Couragierten Gemeinde Akteure rund um den Schulhof (Verein, Schule, Stadt), um gemeinsam Nutzungsregeln für diesen städtischen (Frei)Raum zu erarbeiten.

Kommunikation spielt im Projekt Couragierte Gemeinde eine entscheidende Rolle. Während bei der Durchführung der Methode der Neuen Autorität in Schulen noch auf die persönliche Kommunikation der Mitglieder des Koordinationsteams gesetzt werden konnte, ist dies im Kontext einer ganzen Stadt nicht

„Toolbox" Couragierte Gemeinde mit den sieben Säulen: Präsenz & Wachsame Sorge, Selbstkontrolle & Deeskalation, Unterstützungsnetzwerk & Bündnisse, Protest & Gewaltloser Widerstand, Gesten der Wertschätzung & Versöhnung, Transparenz & Partielle Öffentlichkeit, Wiedergutmachungsprozesse



Die Kommunikations-App der Couragierten Gemeinde

Projektteam Couragierte Gemeinde: W. Baaske, E. Kumpl-Frommel, B. Appelt, G. Kobleder, St. Ofner, B. Lancaster, G. Schmiedl, G. Kienböck, E. Jochim, D. Haider (v.l.n.r.)

mehr möglich. Stattdessen wird auf eine speziell für das Projekt entwickelte Softwarelösung gesetzt, die auf mobilen Geräten und Desktops genutzt werden kann. Soziale Netzwerke wie Facebook werden zwar zur rascheren Verbreitung von Nachrichten eingebunden, sensitive Informationen werden aus Sicherheitsgründen aber nur in der projekt-internen Datenbank gespeichert. Mit Hilfe des Systems werden die Mitglieder über Vorkommnisse informiert, können Nachrichten austauschen, Diskussionen führen und Termine vereinbaren. Mit Hilfe eines Abstimmungsmoduls können Entscheidungen rasch und demokratisch getroffen werden.

Mit Couragierte Gemeinde sollen sich Vandalismus-Schäden nachhaltig halbieren lassen und das subjektive Sicherheitsempfinden soll steigen. Davon profitieren insbesondere Frauen, ältere Menschen, Jugendliche/Kinder und die Gemeinde als sicherer Lebens- und Wirtschaftsraum. Durch Kooperation und Netzwerkbildung mit der Zivilgesellschaft erhöht sich die Wirksamkeit der polizeilichen Arbeit. Eine österreichweite Fachtagung fand am 1. Juni 2017 statt.

Projektleitung
STUDIA Schlierbach, Studienzentrum für Internationale Analysen

Projektpartner
- Bundesministerium für Inneres
- Fachhochschule St. Pölten Forschungs GmbH
- Institut für Neue Autorität Steinkellner & Ofner OG
- SPES GmbH
- Stadtgemeinde Ansfelden – Jugendbüro

Kontakt
Mag.a Bettina Lancaster,
Dipl.-Math. Wolfgang Baaske
Panoramaweg 1, 4553 Schlierbach,
Tel: +43 7582 81981-96
baaske@studia-austria.com
www.studia-austria.com

CPS-Security

Verhaltensbasierte Anomalie-Erkennung in Cyber-Physischen Systemen

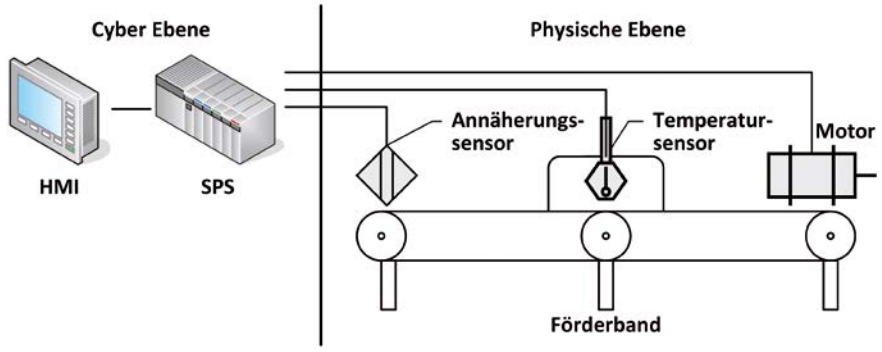
Die Industrie war lange Zeit durch proprietäre Systeme und Protokolle sowie durch physische Abschottung gekennzeichnet. In den letzten Jahren wurden diese Systeme durch den zunehmenden Einzug von Informations- und Kommunikationstechnologien zu offenen, vernetzten Systemen, die eine Verbindung von digitalen Netzen und physischen Prozessen ermöglichen.

Diese sogenannten cyber-physischen Systeme (CPS) eröffnen einerseits weitreichende innovative Möglichkeiten für die Produktion, andererseits führt die fortwährende Integration von Standard-Kommunikationstechnologien in derartigen Betriebsumgebungen zu neuen Schwachstellen und größeren Angriffsflächen und erhöht damit das Risiko von Cyberangriffen.

Erfolgreiche Angriffe auf cyber-physische Systeme können schwerwiegende Schäden nach sich ziehen, folglich müssen diese Systeme ausreichend vor Cyberangriffen geschützt werden. Aufgrund der speziellen Charakteristika cyber-physischer Systeme sind Abwehrmaßnahmen der konventionellen IT-Landschaft oft nicht anwendbar und spezifische Lösungen für industrielle Betriebsumgebungen derzeit noch wenig vorhanden.

Im Projekt CPS-Security werden neue Möglichkeiten zur laufenden Überwachung cyber-physischer Systeme und zur Erkennung von Angriffen erforscht. Das Ziel ist, Abweichungen im Systemverhalten einer industriellen Anlage festzustellen und dadurch mögliche Cyberangriffe auf das System zu erkennen. Dazu wird verhaltensbasierte Anomalie-Erkennung eingesetzt.

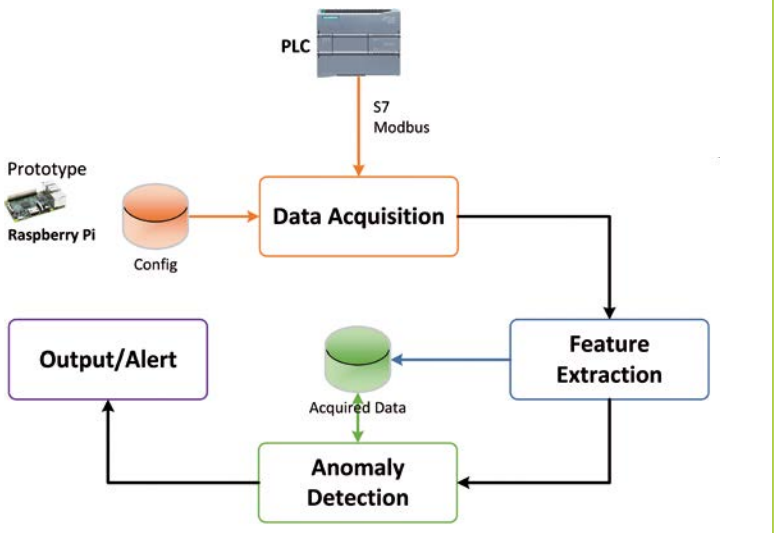
Ein wichtiger Bestandteil dieses Projekts ist die Verwendung zuverlässiger und realitätsnaher Echtdaten, welche aus den Prozessen eines echten Industriesystems stammen. Dazu wurde eine Testanlage – ein einfaches Förderband mit einer Heizkammer – als Modell gebaut. Die Steuerung des Modells erfolgt durch eine handelsübliche speicherprogrammierbare Steuerung (SPS), wie sie in der Praxis häufig vorkommt. Das Förderband, wie in der nachfolgenden Abbildung dargestellt, besteht aus einer Cyber-Ebene, die Industriesteuergeräte enthält, sowie einer physischen Ebene, die über Sensoren Messwerte liefert und durch Aktoren (z. B. Motor) physische Vorgänge auslöst. Durch den Einsatz von Industriehardware können realitätsnahe Daten gewonnen werden.



Schematische Darstellung der Testanlage

Diese Anlage kann einerseits im normalen Betriebsmodus ablaufen, es können aber auch gezielte Angriffe auf die Anlage durchgeführt werden. Um diese Angriffe zu erkennen, wird Anomalie-Erkennung eingesetzt. Dazu wird ein Modell des Normalverhaltens der Anlage anhand von aufgezeichneten Daten des Normalbetriebs definiert. Die Erfassung der Daten erfolgt alle 50 ms, um alle Systemänderungen aufzuzeichnen. Dadurch entstehen große Datenmengen, in denen Anomalien schwer zu erkennen sind. Deshalb wurde Feature Extraction eingesetzt, um die Dimensionalität der Daten zu verringern, ohne dabei ihre Aussagekraft zu beeinträchtigen. Als Features wurden statistische Kennzahlen wie Standardabweichung, Varianz und Durchschnitt verwendet. Das Modell wird mit Hilfe von Verfahren des maschinellen Lernens erstellt: Für die Features wird mittels eines Klassifikationsalgorithmus ein Outlier-Threshold (Schwellenwert) ermittelt. Dann werden verschiedene Cyber-Angriffe auf das System durchgeführt und gleichzeitig die Daten der Anlage aufgezeichnet. Das aktuelle Systemverhalten wird mit dem Modell des Normalverhaltens verglichen, um Abweichungen – Anomalien – festzustellen.

Die Forschungsergebnisse zeigen, dass durch diesen Projektansatz vor allem aktive Angriffe, welche Systemwerte modifizieren, deutlich erkannt werden. Rein passive Man-in-the-Middle-Angriffe, bei denen Daten nur abgehört, aber nicht verändert werden, konnten ebenfalls – aufgrund der zeitlichen Varianz der Netzwerkpakete – als Anomalien erkannt werden.



CPS-Security Prototyp

Basierend auf diesem Lösungsansatz wird ein Prototyp entworfen, der als Proof-of-Concept die praktische Anwendbarkeit des Verfahrens nachweist. Der Prototyp führt die Anomalie-Erkennung weitgehend automatisiert durch. Wichtige Bestandteile für die Datenerfassung sind die Unterstützung der gängigsten Industrieprotokolle, sowie eine echtzeitnahe Abfrage von Daten. Danach werden die Features berechnet, die zuvor definiert wurden. Der Prototyp implementiert eine laufende Überwachung der aufgezeichneten Daten durch Vergleich mit dem Modell des Normalverhaltens. Bei Erkennung einer Anomalie wird ein Alarm ausgelöst. Zusätzlich wird versucht, die Anomalie einem bereits bekannten Angriff zuzuordnen.

Projektleitung
FH St. Pölten, Institut für IT Sicherheitsforschung
Projektpartner
- Bundesministerium für Inneres
- SEC Consult Unternehmensberatung GmbH

Kontakt
DI Dr. Paul Tavolato, Univ.-Doz. DI Dr. Ernst Piller
Fachhochschule St. Pölten,
Institut für IT Sicherheitsforschung
Matthias Corvinus-Strasse 15, 3100 St. Pölten
Tel.: +43 2742 313 228 634
E-Mail: paul.tavolato@fhstp.ac.at
www.isf.fhstp.ac.at

CSISmartScan3D

3D-Tatortaufnahme und -dokumentation mit kostengünstigen 3D-Sensoren sowie Tablets/Smartphones

3D-Modelle erlauben eine dauerhafte und vollständige „Konservierung" der räumlichen Situation an Tat- und Unfallorten. Sie sind eine geeignete Basis für die computerunterstützte Analyse, Dokumentation und verständliche visuelle Aufbereitung im Rahmen von Gerichtsverfahren, die zu mehr Transparenz, Reproduzierbarkeit und letztlich Rechtssicherheit führen.

Derzeitige 3D-Aufnahmetechnologien können nicht alle Anforderungen im Rahmen der Tatortdokumentation gleichzeitig erfüllen. Punkte wie Aufnahmequalität, Zeit, Verfügbarkeit, Störung der Ermittlungen, Ergonomie sowie hohe Kosten führen dazu, dass 3D-Scanner nur für Spezialfragestellungen abseits der routinemäßigen Gesamtdokumentation des Tatorts zum Einsatz kommen. Darüber hinaus sind gegenwärtige 3D-Scanner reine Aufnahmegeräte ohne unmittelbaren Nutzen am Tatort. Potentielle Vorteile dieser Geräte ergeben sich erst im Zuge der Nachbearbeitung und Analyse der aufgenommenen Daten.

Das Ziel von CSISmartScan3D ist die Erforschung der praktischen Umsetzbarkeit einer neuen Art von 3D-Tatortdokumentationssystem, das nicht nur die Erstellung eines 3D-Modells unter Berücksichtigung der Anforderungen am Tatort erlaubt, sondern auch dessen unmittelbare Nutzung als Referenzmodell im Rahmen der Tatortarbeit. Durch Fusion der Daten von kostengünstigen 3D-Sensoren und der direkten Darstellung am Aufnahmegerät sollen ein hohes Maß an Robustheit des Aufnahmeverfahrens, Vollständigkeit und Qualität des 3D-Modells sowie ein Aufnahmeprozess ohne Verzögerung der Ermittlungen erreicht werden. Die Möglichkeit zur Nutzung des Modells als 3D-Referenzmodell und der Annotation (z. B. Markierung von Spuren) soll darüber hinaus der Effizienz dienen.

In CSISmartScan3D werden die Möglichkeiten und Grenzen der verwendeten Sensortechnologien, Datenverarbeitungsgeräte, Interaktionstechniken und nicht zuletzt Algorithmen analysiert und aufgezeigt werden. Im Vordergrund stehen dabei deren Anpassung und Verbesserung entsprechend der Anforderungen am Tatort und die Überprüfung, inwieweit mit derartigen Technologien die zeitnahe Aufnahme adäquater vollständiger 3D-Modelle und deren Dokumentation möglich ist.

In der bisherigen Projektlaufzeit konnte ein erster Prototyp entwickelt werden. Dieser wurde auf Basis einer sehr preisgünstigen RGD-D-Kamera als Sensor und eines Tablets mit einem leistungsfähigen Grafikprozessor als Verarbeitungsgerät sowie einer Akkulampe, deren Akku der Stromversorgung von Tablet und Sensor dient, als Plattform umgesetzt (siehe Abbildung unten). Sensor und Recheneinheit wurden aufgrund der geringen Kosten bei hoher Rechenleistung bzw. Qualität der Sensordaten ausgewählt. Der Prototyp ermöglicht 3D-Aufnahmen unter Zuhilfenahme von 3D-Registrierungs- und Echtzeitfusionsalgorithmen auf Basis der Daten eines Sensors. Das entstehende 3D-Modell wird sofort am Bildschirm dargestellt und kann hinsichtlich Qualität und Vollständigkeit unmittelbar während der Aufnahme begutachtet werden.

CSISmartScan3D-Prototyp bestehend aus NVidia Tablet, Orbbec RGB-D Sensor und dem Griff einer Akku-Taschenlampe

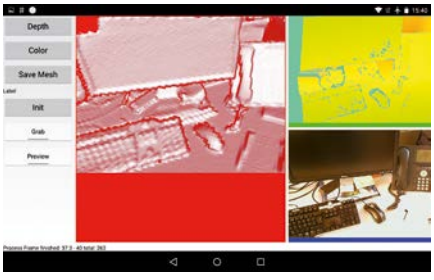
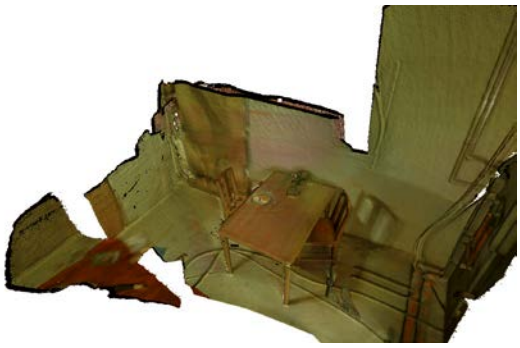


Foto eines im Rahmen von CSISmartScan3D aufgebauten künstlichen Tatorts. Ergebnis der 3D-Rekonstruktion unter Verwendung kantenbasierter visueller Odometrie



Der Prototyp wurde ausgiebig, u.a. an einem simulierten Tatort, und unter Verwendung vieler bekannter Echtzeitregistrierungs- und Fusionsverfahren getestet. Der Tatort selbst wurde mit Unterstützung von zwei forensisch geschulten Mitarbeitern des Ludwig Boltzmann Institutes für Klinisch Forensische Bildgebung aufgebaut und beinhaltete eine Reihe von praxisrelevanten Spuren wie z. B. ein eingeschlagenes Kellerfenster, Fußspuren, stumpfe Gewalt gegen den Kopf, Blutspritzer, einen blutverschmierten Hammer neben dem Kopf als mögliches Tatwerkzeug.

Im Zuge der Tests unter realitätsnahen Bedingungen wurden gängige Verfahren zur Schätzung des Kamerapfades (visuelle Odometrie) als eine wesentliche Schwachstelle auf dem Weg zu qualitativ hochwertigen 3D-Modellen identifiziert. Ungenauigkeiten der visuellen Odometrie führen bei komplexen Szenarien zu erheblichen Modellfehlern. Bekannte alternative Methoden zur Schätzung der Kameraposition auf Basis von „Features" erwiesen sich wegen der aufwändigen Berechnung als ungeeignet für CSISmartScan3D. Deshalb wurde an der TU Graz ein neuartiges kantenbasiertes Verfahren entwickelt, welches die Vorteile beider Welten bei gleichzeitig niedrigem Rechenaufwand vereinigt und zu qualitativ hochwertigen Ergebnissen führt.

Neben den Arbeiten am Prototyp wurde intensiv an Verfahren und möglichen Arbeitsflüssen zur Nachverarbeitung der Daten gearbeitet. So wurden vom Firmenpartner Holistic Imaging Möglichkeiten der Cloud-basierten Rekonstruktion evaluiert sowie neue Verfahren zur Berechnung von Dreiecksrepräsentationen und Texturen aus den aufgenommenen Punktwolken entwickelt.

Zusätzlich wurden die rechtlichen Rahmenbedingungen für 3D-Bildgebung bzgl. Tatortarbeit und anderer Tätigkeiten des Bedarfsträgers untersucht sowie historische Aspekte des Einsatzes von 3D-Methoden in der Kriminalistik – unter anderem durch Hans Gross, Grazer Pionier der Kriminalistik an der Karl-Franzens Universität Graz. Zu diesem Thema ist eine Ausstellung in Vorbereitung.

Projektleitung
Ludwig Boltzmann Institut für Klinisch-Forensische Bildgebung

Projektpartner
- Bundesministerium für Inneres
- TU Graz, Institut für Maschinelles Sehen und Darstellen
- Karl-Franzens-Universität Graz, Institut für Geschichte
- Fa. Holistic Imaging Meixner & Rüther OG

Kontakt
Dr. Alexander Bornik
Ludwig Boltzmann Institut für Klinisch-Forensische Bildgebung
Universitätsplatz 4, 8010 Graz
Tel.: +43 316 380-4331
E-Mail: alexander.bornik@cfi.lbg.ac.at
www.cfi.lbg.ac.at/de/forscher-profile/csismartscan3d

Darknet Analysis

Analyse von Untergrundnetzwerken zum Austausch illegaler Waren und Dienstleistungen

Im Vordergrund des Projekts Darknet Analysis steht die Privacy-sensible Analyse von Untergrund-Plattformen in Hinblick auf Trends, Funktionsweisen und Angriffspunkte, ohne jedoch direkt Einzelfälle zu analysieren.

Unter dem Begriff „Darknet" werden im weiteren Sinn sog. Overlay-Netzwerke verstanden, die typischerweise nur einem begrenzten und (mehr oder weniger) ausgewählten Personenkreis zugänglich sind. Diese Netzwerke wurden vor allem in der jüngeren Vergangenheit einem weiten Publikum in Zusammenhang mit illegalen Aktivitäten ein Begriff. Speziell in Zusammenhang mit kriminellen und terroristischen Aktivitäten stellte sich daher die Frage einer effizienten Untersuchung von Darknets und anderen, ähnlich aufgebauten, Kommunikationssystemen. Ein Fokus unserer Projektarbeit liegt dabei in der Untersuchung der Verbreitung von politischer Propaganda und Anwerbung (bspw. durch Organisationen wie den „Islamischen Staat"), aber auch der Kommunikation mit Gleichgesinnten mit Hilfe von Untergrundforen.

Als weiteres Fokusfeld unserer Forschungen ist vor allem der Austausch und Handel von illegalen Waren und Dienstleistungen hervorzuheben, die über sog. „underground marketplaces" stattfinden, wobei das Hauptaugenmerk unserer Untersuchungen speziell auf staatsschutzrelevanten Delikten liegt. Beispielsweise werden in solchen Foren auch Dienste durch Botnetze verkauft, um DDOS-Attacken („Distributed Denial of Services"), wie sie bspw. gegen das ukrainische Stromnetz lanciert wurden, ohne eigene technische Kenntnisse durchführen zu können. Eine effiziente Aufklärung ist daher auch vor dem Hintergrund der Terrorprävention wesentlich.

Im Rahmen dieses Projekts sollen Techniken entwickelt werden, um Trends in von politischen und ideologischen Gruppierungen kriminell genutzten Darknets besser verstehen zu können, wobei der Fokus hauptsächlich auf drei Forschungsaspekte gelegt wird:

1. **Fundierte Quellenanalyse und Erschließung:**
   Dabei ist sowohl die inhaltliche Untersuchung in Hinblick auf Propaganda und verbotene Inhalte/Angebote als auch die Analyse der Quellen selbst in Hinblick auf ihre Relevanz ein wichtiger Projektteil, der der Optimierung der Aufklärungsarbeit dient und eine wesentliche Steigerung der Performance im Rahmen dieser Tätigkeiten verspricht.

2. **Privacy-sensible Auswertung und Analyse der Information**, wozu Methoden und Techniken des „Privacy-Preserving Machine-Learnings" entwickelt werden. Speziell durch die Forderungen der „General Data Protection Regulation" (GDPR) der EU müssen datenverarbeitende Applikationen hohen datenschutzrechtlichen Anforderungen genügen. Dazu gehören auch Techniken der Zugriffskontrolle durch die Endnutzer des Systems, Techniken gegen Datenmanipulationen am Backend sowie der Schutz der internen Datenbanken.

3. **Analyse der Funktionsweise von Underground Marketplaces**, besonders der Mechanismen zur Kontaktaufnahme, Preisbildung, Bezahlung und Übergabe von Waren, speziell wenn es sich um Waren in physischer Form handelt, bei denen ein Kontakt in der „Offline-Welt" unausweichlich ist und entsprechend ermittlungstechnisch genutzt werden kann.

Zusätzlich zu den technischen Fragestellungen bringt die Analyse von Netzwerken auch grundlegende rechtliche Fragestellungen mit sich, die im Laufe des Projektvorhabens geklärt werden. Dabei sind vor allem die neuen Regelungen, die durch die GDPR (General Data Protection Regulation) sowie die DSGVO (Datenschutzgrundverordnung) in Kraft treten, wesentlicher Inhalt der Forschungsarbeiten, da sich hierbei wesentliche Änderungen für datenverarbeitende Anwendungen im Allgemeinen ergeben, sowohl was die Sicherstellung von Transparenz bei der Verarbeitung persönlicher Informationen betrifft als auch das Thema des Löschens von Daten aus der datenverarbeitenden Anwendung sowie der Sicherstellung der Nachvollziehbarkeit der Verarbeitung.

Im Rahmen der Auswertung bezüglich verbotener Angebote wird dabei auf die Entwicklung von Techniken Wert gelegt, die höchstmögliche Automatisierung gewährleisten, dennoch den menschlichen Ermittler als wichtige Komponente in der Erkennung von Tatbeständen, aber auch zur Validierung, integrieren. Dabei ist es von Vorteil, dass die entwickelten Methoden den Fokus auf die Erkennung von Trends legen und nicht auf die Ermittlung im Rahmen von Einzelfällen abgestellt sind. Die auf den Erkenntnissen basierende Analyse der sog. Underground Marketplaces besitzt ebenfalls den Fokus der Trendanalyse, so sollen bspw., auch basierend auf den Ergebnissen des im 7. europäischen Forschungsrahmenprogramms geförderten Projekts CyberRoad, speziell die Marktmechanismen solcher Märkte untersucht werden, um zu verstehen, wie diese in Zukunft bekämpft werden könnten. Auch hierbei geht es nicht um Einzelfallanalysen, sondern vor allem um die Erkennung von Trends und grundlegenden Eigenschaften.

Wesentlicher Aspekt des Projektvorhabens ist der Schutz der Anonymität und der Privatsphäre Unbeteiligter. Der Fokus liegt daher auf der Entwicklung von Techniken, die eine effiziente Analyse mit möglichst weitreichendem Schutz kombinieren. Dabei gehen wir von einem strengen „Data Minimization"-Prinzip aus, wie es auch in der GDPR gefordert wird: Statt wahllos möglichst alle erreichbaren Daten zu sammeln und diese für „immer" zu speichern, wird schon die Datenerfassung möglichst selektiv vorgenommen, womit sowohl eine bessere Performance in Hinblick auf die Erfassung selbst erreicht werden kann als auch ein grundlegender Aspekt der Datensparsamkeit befolgt wird. Dies betrifft vor allem auch etwaige Metainformationen, die für die Auswertung im Rahmen von Trendanalysen wenig informativen Wert besitzen, gleichzeitig aber hochsensible Informationen enthalten können.

Ein wesentlicher Aspekt der im Rahmen dieses Ziels betriebenen Forschung liegt in der Analyse des Einflusses von Mechanismen des Datenschutzes auf Performance und Ergebnis „klassischer" Algorithmen des Machine Learnings: Techniken, die zum Schutz sensibler Informationen in Daten angewandt werden, wie bspw. die Anonymisierung mit Hilfe von k-Anonymity, aber auch das Löschen von Datensätzen im Rahmen des „Rechts auf Vergessenwerden" verzerren die ihnen unterworfenen Daten nachhaltig. Diese Effekte wurden bisher noch nicht ausreichend analysiert und quantifiziert, obwohl dies einen wichtigen Aspekt bei der Wahl der geeigneten Schutzmechanismen darstellt.

Im Rahmen dieses Forschungsprojekts wird nicht nur der Effekt diverser Mechanismen auf die Analysequalität eruiert, es werden auch Methoden entwickelt, diese Effekte zu mitigieren oder zumindest besser abschätzbar und damit beherrschbarer zu machen.

Die entwickelten Techniken zum Schutz der Privatsphäre werden den Bedarfsträgern auch für andere Vorhaben zur Verfügung gestellt, um im Rahmen dieses Projekts einen wesentlichen Beitrag zum Datenschutz im Zuge von Ermittlungsarbeiten zu leisten.

Projektleitung
SBA Research gGmbH
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- TU Graz, Institut für Maschinelles Sehen und Darstellen
- Universität Wien, Arbeitsgruppe Rechtsinformatik
- Bravestone GmbH

Kontakt
DI Peter Kieseberg
SBA Research gGmbH
Favoritenstrasse 16, 1040 Wien
Tel.: +43 1 5053688
pkieseberg@sba-research.org
www.sba-research.org

DHS-AS

Detektion humaner Signaturen zur Aufdeckung von Schlepperei

Im Projekt DHS-AS wird ein tragbarer Prototyp zur Detektion menschlicher Spurengase, die über Atem, Haut oder andere Ausscheidungsorgane freigesetzt werden, weiterentwickelt und optimiert. Zudem kann das Gerät mit Hilfe einer Infrarotkamera die personengenerierte Wärme auch bei Dunkelheit visualisieren. Das Ziel des Projekts ist es, mit dem tragbaren Gerät ein typisches Signalmuster der detektierten flüchtigen Verbindungen zu erkennen, ähnlich einem Hund, der mit seiner Nase z. B. den Geruch verschütteter Menschen aufspüren kann.

Nach neuesten Forschungsergebnissen werden Verbindungen, die zu der Gruppe der Aldehyde gehören, wie z. B. Hexanal, Octanal, Nonanal oder Dekanal, von der menschlichen Haut freigesetzt, sind aber auch in Urin detektierbar und tragen zum individuellen menschlichen Geruch bei. Im Projekt DHS-AS ist die gezielte Detektion dieser Substanzgruppen zusätzlich zu den bisherigen Gasmessungen vorgesehen. Dabei sollen flüchtige Substanzen, die von anderen Quellen stammen, wie etwa Duftstoffe, Hintergrundmatrix etc., herausgefiltert werden. Da das Gerät modular konzipiert wurde, ist die Integration zusätzlicher Sensoren und Kommunikationsmodule jederzeit möglich. Im geplanten Projekt wird nun die Kapazität der Gasmessungen durch die Kombination mit einem Aldehydsensor ausgedehnt.

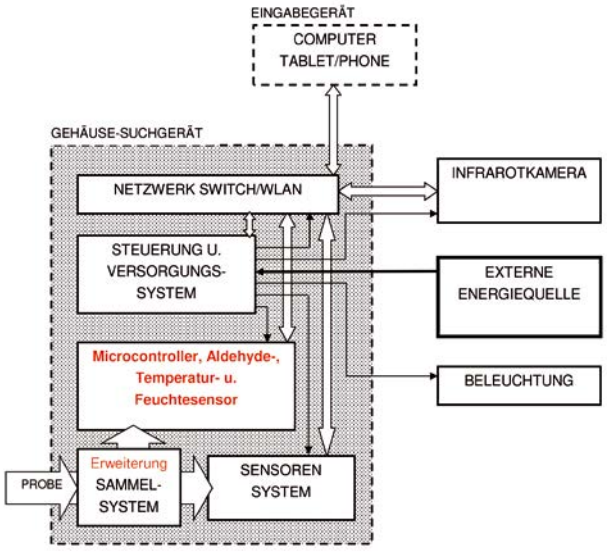
Die Entwicklung von Gassensoren, die eine gute Selektivität für bestimmte Stoffgruppen und zugleich eine Detektierbarkeit der Substanzen im Spurenbereich (ppb, parts per billion, 1 Teilchen unter 1 Milliarde) erreichen, stellt eine große Herausforderung dar. Deshalb soll in diesem Projekt der von der Partnerfirma Ionicon Analytik GmbH zur Verfügung gestellte Aldehydsensor charakterisiert und für bestimmte biologische Proben getestet werden. Um die Selektivität und Sensitivität des mit dem Aldehydsensor erweiterten Prototyps zu testen, werden unterschiedliche Testgasgemische der Aldehyde hergestellt und gemessen. Anschließend wird das Antwortsignal des Prototyps zu bestimmten biologischen Proben und Matrices (cross-sensitivity check) getestet und in seiner Wirksamkeit überprüft.

Mit Hilfe von Messungen humaner Proben (Urin, Schweiß) und Testversuchen mit ProbandInnen (Messung an der Hautoberfläche, Analyse von Hautemissionen in einer speziellen Kammer, Atemgas) wird das System trainiert. Daneben werden typische Hintergrundmatrizen mit Hilfe der Bedarfsträger vermessen. Vergleichsmessungen werden zusätzlich mit anderen gasanalytischen Verfahren wie Proton-Transfer-Reaktion Massenspektrometrie oder Gaschromatographie mit Massenspektrometrie durchgeführt.

leicht tragbarer Prototyp

Tragetasche

Lanze



Schematische Darstellung des Prototyps nach dem Einbau des Aldehydsensors und dazu gehörige Komponenten

Der entwickelte Prototyp wird in Feldversuchen gemeinsam mit den Partnern validiert und für die spätere Anschlussfähigkeit an bestehende Systeme optimiert. Daneben ist eine Algorithmus- und Softwareentwicklung vorgesehen, um den Zugriff auf alle Sensorendaten, Wärmebilder und Geräteparameter sowie eine Vernetzung der Daten zu ermöglichen. Weiters wird die Umsetzung der externen Steuerung auf einem Tablet/Smartphone durchgeführt.

Die Einbindung des BM.I und BMLVS erfolgt durch die anwendungsorientierte Anbindung des Konzepts an die derzeitige Praxis bei Routinekontrollen. Die beteiligten Organisationseinheiten sind insbesondere zuständig für die Anforderungen an die technische Spezifikation sowie deren Umsetzung. Dadurch wird gewährleistet, dass das entwickelte System an die aktuelle Praxis und Einsatztechnik des Bedarfsträgers anschlussfähig ist und die gesammelten Daten in die Systeme der Einsatzzentrale zukünftig integriert werden können.

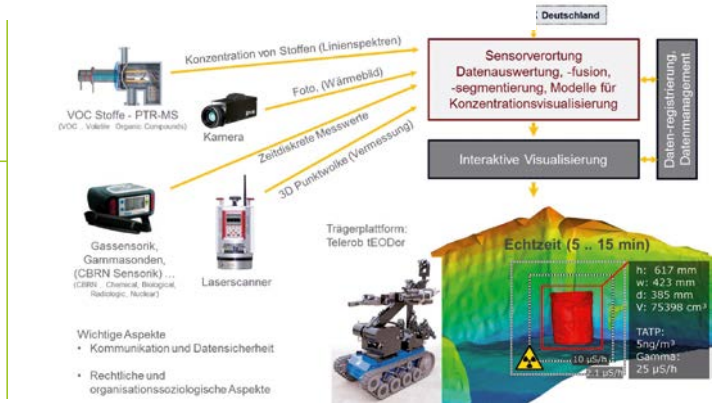
Für die Zukunft zielt DHS-AS darauf ab, den tragbaren Prototyp soweit zu entwickeln, dass er die Effektivität der Sucheinsätze durch Erkennung von humanen Spuren mit Hilfe des hochmodernen Detektorsystems stärkt, damit Menschen, die von Schleppern versteckt und transportiert werden, früher und leichter gefunden und aus ihrer menschenunwürdigen Lage befreit werden können.

Projektleitung
Universität Innsbruck, Institut für Atemgasanalytik
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Jens Herbig, Ionicon Analytik Gesellschaft mbH
- Georg Aumayr, Johanniter-Unfall-Hilfe in Österreich
- Universität Innsbruck, Institut für Mechatronik

Kontakt
Dr. Ing. Veronika Ruzsanyi
Universität Innsbruck, Institut für Atemgasanalytik
Innrain 66, 6020 Innsbruck
Tel: + 43 512 24632
E-Mail: Veronika.Ruzsanyi@uibk.ac.at
www.uibk.ac.at/breath-research/index.html.de

Durchblick

Detektion unterschiedlicher unkonventioneller Spreng- und Brandvorrichtungen mittels intelligenter analytischer Sensorik



Übersicht über die geplanten Technologien

Das Projekt DURCHBLICK beschäftigt sich mit der Untersuchung und Kombination von verschiedenen Sensortechnologien zur robotergestützten Analyse verdächtiger Objekte (z. B. Gepäckstücke, Mülleimer etc.) im öffentlichen Raum.

Die Anschläge von Paris sowie die Terrorwarnungen von Hannover und München in den letzten Jahren sind nur einige Beispiele dafür, wie konkret die Bedrohung durch Bombenanschläge aktuell ist. Insbesondere durch die zunehmende Verbreitung von Anleitungen zur Herstellung von improvisierten bzw. unkonventionellen Spreng- und Brandvorrichtungen (sogenannte USBVs) ergibt sich eine ernstzunehmende Gefährdung der öffentlichen Sicherheit. Daher müssen die Sicherheitskräfte in der Lage sein, verdächtige Objekte wie herrenlose Gepäckstücke, manipulierte Mülleimer, Gasflaschen, umfunktionierte Pyrotechnik und ähnliche verdächtige Gegenstände schnell, zuverlässig und mit möglichst geringem Eigenrisiko zu untersuchen. Aktuell setzen die zuständigen Einsatzkräfte für diese Zwecke einen fernlenkbaren Roboter ein, um das verdächtige Objekt mittels unterschiedlicher Sensorik wie Transmissions-Röntgen und optischen Kameras zu untersuchen und die Gefahrenlage einzuschätzen. Doch diese Technologie stößt nur allzu oft an ihre Grenzen. Einer der Gründe dafür ist, dass an einer Wand stehende oder angebrachte Objekte nur von einer Seite aus zugänglich sind. In diesem Fall ist ihr Inhalt mit der verfügbaren Technologie nicht berührungslos zu untersuchen. Solche Situationen bedeuten ein enormes Risiko sowohl für die Einsatzkräfte vor Ort als auch die Bevölkerung in der unmittelbaren Umgebung. Alle Informationen, die über den aktuellen Stand der Technik hinaus gewonnen werden können, tragen dazu bei, das Leben der zuständigen Einsatzkräfte und die öffentliche Sicherheit zu schützen.

Aus dieser aktuellen Bedarfslage heraus wurde das Projekt DURCHBLICK initiiert und vorangetrieben. Ziel ist es, den Einsatzkräften ein leistungsstarkes Sensorik-System zur Verfügung zu stellen, welches den aktuellen Stand der Technik übertrifft. Es soll robotergestützt an die potenzielle Gefahrenquelle herangesteuert werden können, um schnell detaillierte Informationen über das Objekt zu sammeln, die mit derzeitig verfügbaren Systemen so nicht zugänglich sind.

Basierend auf einer detaillierten Bedarfsdefinition durch die Sicherheitsorganisationen werden für diesen Anwendungszweck potenzielle Sensortechnologien evaluiert und verglichen. Durch die Kombination mit anderen Sensoren wie Infrarot-Kamera, optische Sensoren (Laserscanner, Fotokamera) für die Vermessung und Sensorik zur Detektion und Identifikation von Radioaktivität, Gasen und flüchtigen Gefahrstoffen (Proton Transfer Reaction – Mass Spectrometry PTR-MS) können umfangreiche Daten zur Gefahreneinschätzung und Beweismittelsicherung gesammelt werden. Mittels Datenfusion der verschiedenartigen Sensordaten und einer eigens für die Einsatzkräfte in Stresssituation zu entwickelnden, effizienten Benutzerschnittstelle werden die Daten für die Einsatzkräfte schnell erfassbar. Damit wird eine zuverlässige Lageeinschätzung aus sicherer Distanz möglich. Durch Tests und Demonstrationen unter realitätsnahen Bedingungen unter Einbeziehung der Endanwender, bereits während der Projektlaufzeit, wird die Entwicklung eines leistungsstarken, nutzbaren Systems gewährleistet, welches einen deutlichen Vorteil im praktischen Einsatz gegenüber der aktuell verfügbaren technologischen Unterstützung bietet. Die Einbindung ethischer, soziologischer sowie juristischer Experten bei der Auswahl, Optimierung und schließlich dem Einsatz der verwendeten Technologien stellt sicher, dass im Rahmen der Entwicklung des intendierten Systems gesellschaftliche und rechtliche Aspekte entsprechend berücksichtigt werden.

Projektleitung
AIT – Austrian Institute of Technology GmbH

Projektpartner
- Bundesministerium für Landesverteidigung und Sport (BMLVS)
- Johannes Kepler Universität Linz, Institute of Networks and Security
- Vienna Centre for Societal Security – VICESSE
- CBRN Protection GmbH
- Ionicon Analytik Gesellschaft mbH
- IQSOFT Gesellschaft für Informationstechnologie mbH
- DI Dr. Heinz Stanek, IStancon

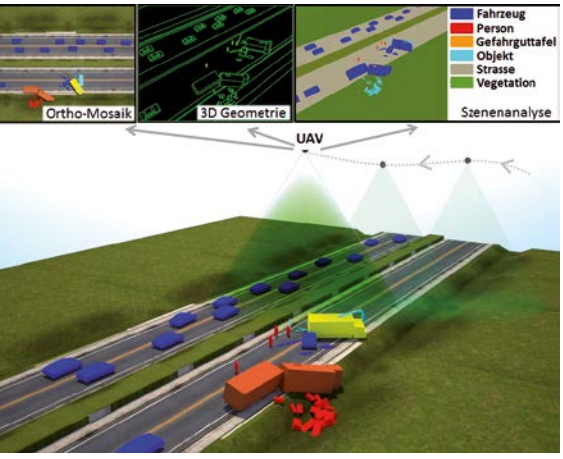
Kontakt
DI Michael Hofstätter
AIT – Austrian Institute of Technology GmbH
Center for Digital Safety & Security
Donau-City-Straße 1, 1220 Wien
Tel.: +43 0 50550 4202
E-Mail: michael.hofstaetter@ait.ac.at
www.ait.ac.at

LEAL

Luftgestützte Erfassung und kontextabhängige Analyse von dynamischen Lagebildern in Krisenszenarien

In Krisensituationen ist es besonders wichtig, sehr rasch einen ersten Überblick der Lage zu erhalten. Je genauer dieser Überblick ist, desto sicherer und schneller können die wichtigsten, ersten Sofortmaßnahmen eingeleitet werden.

Fokus dieses Projekts ist der zielgerichtete Einsatz von unbemannten Luftfahrzeugen (UAV) zur Adhoc-Erstellung des Lagebildes im Falle eines kritischen Ereignisses. Zu den möglichen Szenarien zählen Verkehrsunfälle wie Massenkarambolage im Hochleistungsstraßennetz, allgemeine Gefahrensituationen wie Großbrände, Industrieunfälle, Evakuierungsfälle, aber auch Tatorte. Bei letzterem Szenario steht die Dokumentation im Vordergrund. Die Lagebilder werden mittels optischer Sensoren im visuellen und infraroten Spektralbereich, die im UAV integriert sind, ermittelt. Zusätzlich zur Sensorik aus der Luft werden im Projekt Laserscanner verwendet, um das Lagebild um Details, die aus der Luft nicht sichtbar oder nicht genau genug messbar sind, zu erweitern. Die UAVs werden bereits aus größerer Entfernung gestartet, können über die direkte Luftlinie schneller am Ort des Geschehens sein und bereits am Weg dorthin Beobachtungsdaten übermitteln (Lagebild wird in Echtzeit aufgebaut).



Konzept der Lagebilderfassung und kontextbasierten Szenenanalyse

Die Interpretation der Sensordaten beinhaltet eine kontextabhängige Analyse der Szene, z.B. die Erkennung und Auswertung von Gefahrgutsymbolen, Ermittlung des Zerstörungsgrads der beteiligten Fahrzeuge, Detektion von inner- und außerhalb von Fahrzeugen befindlichen Personen, Ermittlung des schnellsten Weges zum Unfallort bei z. B. blockierter Rettungsgasse. Somit kann eine unmittelbare Entscheidungshilfe für Auswahl und Art der notwendigen Rettungs- oder Evakuierungsmaßnahmen bereitgestellt werden. Im Falle der Dokumentation von Unfällen oder Tatorten liefert das Lagebild eine zentimetergenaue Darstellung der Szenerie. Dadurch können beliebige Vermessungen der Szene auch im Nachhinein hochpräzise durchgeführt werden. Ein besonderes Merkmal der Benutzerfreundlichkeit stellt die semiautonome Fluglageregelung dar, die dem Bediener in Krisen- und Stresssituationen die besonders wichtige Freiheit geben soll, sich auf den eigentlichen Einsatzzweck konzentrieren zu können und nicht auf das Pilotieren des UAVs.

Grundlage der Verkehrsanalysenforschung ist die Datenerfassung nach Unfällen und die damit verbundene elektronische Datenverarbeitung. Die Eingabe der Daten ist sehr aufwändig und soll deshalb in diesem Projekt, mithilfe der Lagebilder, automatisiert werden. Informationen aus den Lagebildern sollen außerdem in bestehende Trainings- und Schulungstools integriert werden, um eine noch realistischere Simulation und Planung eines Einsatzes zu ermöglichen. Zusammen mit den Industriepartnern und den Bedarfsträgern werden die Ergebnisse anhand typischer Anwendungsszenarien evaluiert. Neben dem Potential der innovativen Anwendungen erwarten wir für das Sensor- und Analysesystem eine hohe wirtschaftliche Rentabilität bei vergleichsweise geringen Kosten mit Vermarktungspotential in Verkehr, Sicherheit aber auch Industrie.

Die übergeordnete Methode in LEAL ist die luftgestützte, unbemannte Aufklärung unter Einsatz unterschiedlicher Sensoren, wobei verschiedene Analysemethoden und gezielte Filterung die Geschwindigkeit der Auswertungen so maximieren sollen, dass in Echtzeit fusionierte Bild- und Analysedaten bereitgestellt werden können, um den Einsatzorganisationen Entscheidungsgrundlagen für die zeit- und ressourcen-effiziente Hilfeleistung zu bieten. Die Abbildung illustriert ein mögliches Szenario anhand eines Verkehrsunfalls. Nachdem der Unfall passiert ist und die Einsatzkräfte informiert sind, werden UAVs eingesetzt, um möglichst schnell ein Echtzeit-Lagebild der Situation zu erstellen, welches aus der 3D-Geometrie des kompletten Unfallortes und den dazugehörigen Bildinformationen besteht. Das Lagebild wird gleichzeitig analysiert, um wichtige Informationen wie Anzahl der beteiligten Fahrzeuge, Personen etc. zu ermitteln. Diese Informationen sollen dem Einsatz vor Ort zur Verfügung stehen. Wenn die Gefahrensituation beherrscht ist, wird zusätzlich zur Fotodokumentation ein Laserscanner eingesetzt, um den kompletten Unfallort hochpräzise zu erfassen. Die beiden Lagebilder und jegliches weitere Fotomaterial werden dann offline miteinander verbunden und stehen zur Dokumentation und Postanalyse zur Verfügung.

Projektleitung
AIT – Austrian Institute of Technology GmbH

Projektpartner
- Bundesministerium für Inneres
- RIEGL Research Forschungsgesellschaft mbH
- FH Joanneum Gesellschaft mbH
- EYE.AERO GmbH
- LKR Leichtmetallkompetenzzentrum Ranshofen GmbH
- Schild & Partner GmbH

Kontakt
Christoph Sulzbachner
AIT – Austrian Institute of Technology GmbH
Autonomous Systems Center for Vision, Automation & Control
Donau-City-Straße 1, 1220 Wien
Tel.: +43 50550 4177
E-Mail: christoph.sulzbachner@ait.ac.at
www.ait.ac.at

E.V.A. – Electronic Visual Analysis

Computerunterstützte visuelle Analyse und Auswertung von Bild- und Video-Messdaten

Synopsis

Ziel dieses Projekts ist die Entwicklung eines Systems für computerunterstützte visuelle Analyse und Auswertung von Bild- und Video-Massendaten mit Methoden des Maschinenlernens und der Künstlichen Intelligenz. Die Leistungsfähigkeit sowohl des KI-Systems als auch der zugrundeliegenden, im Projekt entwickelten polizeilichen Methodik wird am Fallbeispiel des Deliktsfeldes Kinderpornographie getestet und evaluiert.

Projektbeschreibung

Durch die rasante Verbreitung von digitalen Kameras, Tablets und Smartphones entstehen täglich enorme Mengen an Bild- und Videodaten. Alleine auf Youtube und Instagram werden jede Minute mehr als 400 Stunden Videomaterial sowie rund 55.000 neue Fotos veröffentlicht. Tatsächlich wird aber der Großteil der ständig aufgenommenen digitalen Fotos und Videos gar nicht veröffentlicht, weshalb die tatsächliche Zahl der täglich neu erzeugten Dateien um ein Vielfaches höher ist. Aufgrund dieser stetig wachsenden Menge an digitalen Bild- und Videodaten ergeben sich für Polizeibehörden neue Herausforderungen und neue Ermittlungsansätze.

Kriminalpolizeiliche Ermittler im Deliktsumfeld Kinderpornographie werden folglich ebenfalls mit einer immer stärker wachsenden Menge an strafrechtlich relevantem Material wie Fotos oder Videos konfrontiert. So liegt die Anzahl der in Österreich jährlich zu bearbeitenden Dateien mittlerweile im zweistelligen Millionenbereich (aktuell über 30 Mio.). Fälle mit mehreren hunderttausend Bildern und Videos pro Sicherstellung sind keine Seltenheit mehr. Diese enorme Menge an Dateien muss von Polizeibeamten aber nicht nur forensisch behandelt und klassifiziert, sondern auch fallübergreifend ausgewertet werden, um Serientatbestände zu erkennen und eine funktionierende Täter-Opfer-Erkennung zu gewährleisten.

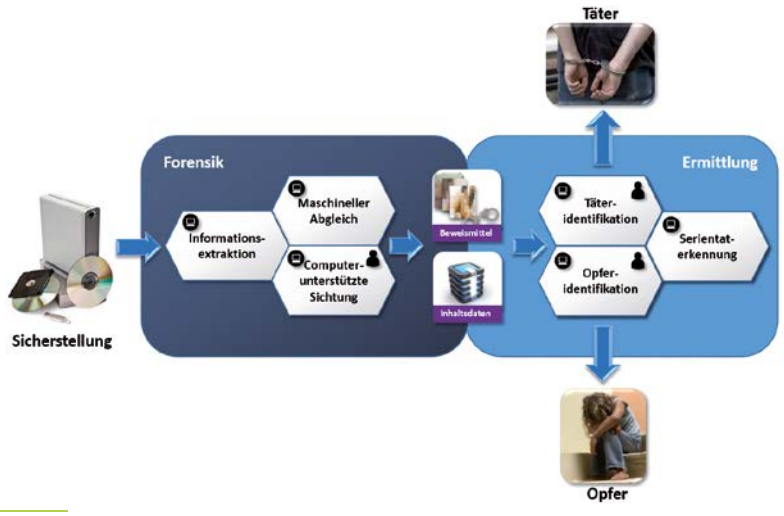
Das Projekt E.V.A. zielt darauf ab, eine Methodik zu entwickeln und bereitzustellen, in der die Arbeit der ermittelnden Beamten durch ein Computersystem massiv unterstützt und vereinfacht wird.

Neue Hightech-Werkzeuge sollen den benötigten Zeitaufwand für die forensische Sichtung und Klassifikation von Mediendateien sowie die psychische Belastung für die ermittelnden BeamtInnen deutlich reduzieren. Außerdem sollen diese Werkzeuge komplexe investigative und sogar fallübergreifende Fragestellungen zulassen und dadurch eine effektive Erkennung von Tatserien auch im internationalen Kontext der organisierten Kriminalität ermöglichen.

E.V.A.-Prozess

Als erster Schritt wird, basierend auf der Untersuchung bestehender polizeilicher Prozesse in Fachbereichen, die mit großen Datenmengen befasst sind, ein Prozess für die computerunterstützte polizeiliche Ermittlungsarbeit bei digitalen Bild- und Videomassendaten entwickelt.

Überblick des polizeilichen E.V.A.-Prozesses



Dieser gliedert sich in drei Phasen:

1. **Datenerfassung:** Alle fallrelevanten Daten werden erfasst: Bild- und Videoinformation (Inhalte), inhaltsbezogene Metadaten, forensische Metadaten und fallbezogene nicht technische Daten.
2. **Informationsgewinnung:** In dieser Phase werden automatisiert neue Information aus den zuvor erfassten Daten extrahiert, oder es werden die erfassten Daten um neue Fakten erweitert. Dies beinhaltet u.a. die Klassifizierung von Bildinhalten, die Bestimmung von Inhaltsmerkmalen, die inhaltsbezogene Beschlagwortung von Bild- und Videoinhalten oder die Erkennung und Markierung von Personen.
3. **Ermittlung:** In der Ermittlungsphase werden alle Informationen mittels einer intelligenten Abfrageschnittstelle interaktiv verknüpft und ausgewertet. Sie dient der Gewinnung von weiteren nicht inhärenten Erkenntnissen durch Verknüpfung von Fakten und Erkennung von Mustern.

Die ersten beiden Phasen sind so konzipiert, dass Methoden des Maschinenlernens und der Künstlichen Intelligenz hauptsächlich automatisiert Information gewinnen. Im Unterschied dazu wird intelligente Leistung in der dritten Phase vom Menschen, den ErmittlerInnen, erbracht, während das Computersystem durch Bereitstellung von Information und Abfrageschnittstelle nur mehr unterstützend tätig ist.

Technische Realisierung

Im zweiten Schritt werden technische Systemkomponenten entwickelt, die in der Lage sind, Bildinhalte zu „verstehen" und diese Information automatisiert zu extrahieren. Schon in der Planungsphase zum Projekt E.V.A. wurde deutlich, mit welchen Datenmengen allein bei der Erfassung und fallübergreifenden Verarbeitung von Bild- und Videodaten zu rechnen ist. Für eine effiziente aber auch leistungsstarke visuelle Suche in diesen Datenbeständen werden pro Bild mehrere Tausend durch Analyseverfahren erzeugte Merkmale bestimmt, die gespeichert und zwischen allen Bildern und Videos des gesamten Datenbestandes abgeglichen werden müssen. Daher müssen alle zum Einsatz kommenden Verfahren in der Lage sein, effizient mit großen Mengen an Bild- und Videodaten umzugehen. Im Projekt wird deshalb besonderes Augenmerk auf den Zukunftsbereich der Neuroinformatik, im Speziellen auf die Methodik des Deep-Learnings, gelegt. Hierfür wird im Projekt nicht nur Software, sondern auch hochspezialisierte Hardware entwickelt, die komplexe Berechnungen mit Massendaten im späteren operativen Echtbetrieb in Polizeibehörden energie- und kosteneffizient realisiert.

Testumfeld Kinderpornografie

Im dritten und letzten Schritt wird der zuvor entwickelte computerunterstützte polizeiliche Prozess mit den im zweiten Schritt entwickelten technischen Systemkomponenten realisiert. Dabei werden spezifische Fragestellungen des polizeilichen Prozesses umgesetzt:

- **Erkennung von ähnlichen Inhalten:** Derivate eines Bildes wie auch inhaltsähnliche Bilder werden automatisch erkannt, zugeordnet und gruppiert. Weitere Aktionen können gleichzeitig auf die gesamte Gruppe zusammengehöriger Inhalte angewendet werden.
- **Erkennung von Menschen:** Bilder, die Menschen enthalten, werden automatisch annotiert, eine Klassifikation nach Alter (Kind/Erwachsener) wird durchgeführt.
- **Gesichtserkennung:** Gesichter werden gefunden und, wo biometrisch verwertbar, markiert.
- **Auffinden von Objekten in der Spurendatenbank:** Objekte aus einem Ausgangsbild oder der Objektdatenbank werden in der Bildspurendatenbank gesucht. Neben der Zusammenfassung von Dateien innerhalb eines Falles wird dadurch die Verknüpfung von verschiedenen Fällen über markante Bildinhalte möglich.
- **Interaktives Abfrage-Interface:** Mittels eines Abfrage-Editors können vom Ermittler/Ermittlerin eigene Fragestellungen und Verknüpfungen entworfen und ausgeführt werden.

Projektleitung
Asgard Technology GmbH
Projektpartner
- Bundesministerium für Inneres, Bundeskriminalamt
- Technische Universität Wien
- Johannes Kepler Universität Linz
- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Kontakt
Dr. Dietmar Schreiner
Asgard Technology GmbH
Gumpendorferstrasse 91, 1060 Wien
E-Mail: dietmar.schreiner@asgard-technology.com

ePartizipation

Authentifizierung bei demokratischer Online-Beteiligung

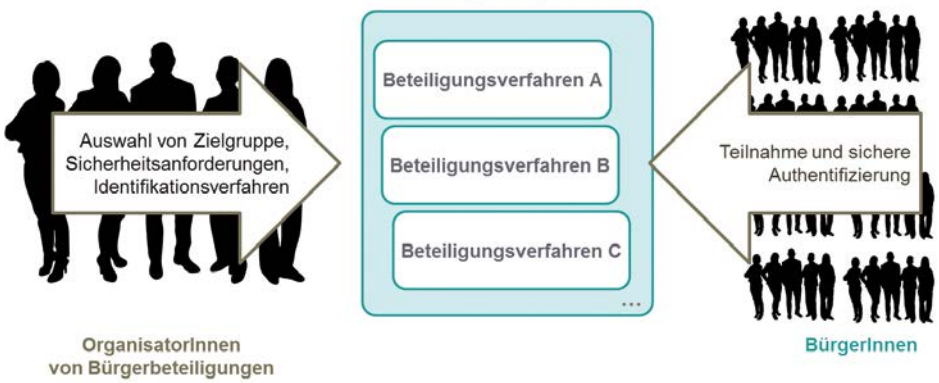
Gesellschaftliche Beteiligung und Teilnahme an demokratischen Entscheidungsprozessen im digitalen Zeitalter stellen Organisationen aus allen Bereichen vor große Herausforderungen. Es stehen nicht nur die erhöhte Partizipationsbereitschaft, sondern auch die möglichen Einsparungspotentiale in Verwaltungsverfahren im Fokus von IKT-gestützter Beteiligung der Gesellschaft. Das Projekt ePartizipation – Authentifizierung bei demokratischer Online-Beteiligung hat sich zwei Jahre detailliert mit den wichtigsten Kernaspekten dieses Themenkomplexes auseinandergesetzt und wurde im Jahr 2016 erfolgreich abgeschlossen.

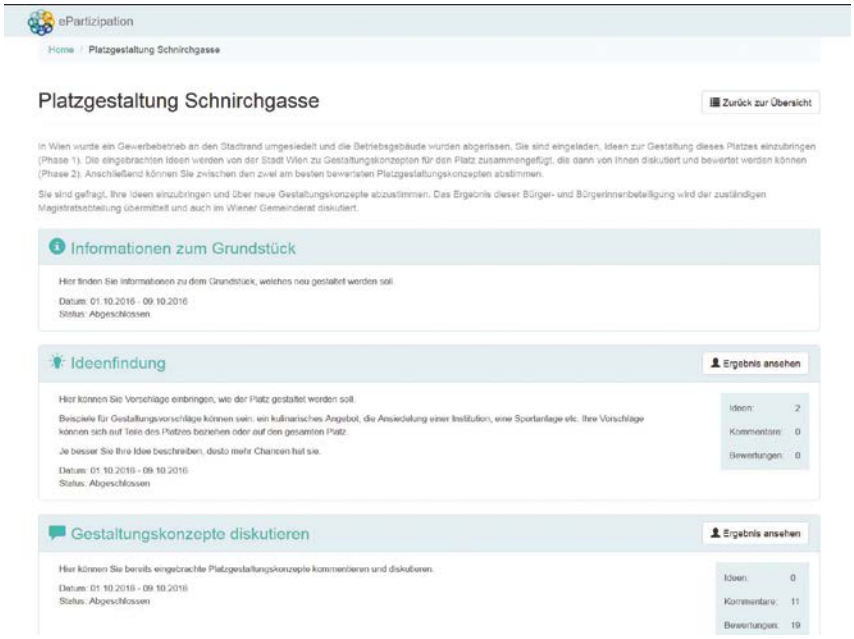
Die komplexe Ausgangslage im Bereich der E-Partizipation bildete den Grundstein dieses Projekts zur Förderung der direkten Demokratie, gestützt durch die aktuellen Möglichkeiten im Bereich der Informations- und Kommunikationstechnologien. So gilt es bei einer Auseinandersetzung mit E-Partizipation eine Vielzahl von Anwendungsszenarien zu beachten, denen unterschiedliche rechtliche und technische Rahmenbedingungen zu Grunde liegen. Im Projekt wurden eine Reihe von konkreten Anwendungsszenarien, wie beispielsweise die Einrichtung einer Fußgängerzone oder die Planung eines öffentlichen Platzes, entwickelt und auf organisatorische und rechtliche Aspekte untersucht. Sie dienten in weiterer Folge als Basis der zu entwickelnden Architektur und Implementierung.

Das Projekt ePartizipation wurde mit dem Ziel der Vereinfachung der Bürgerbeteiligung in politischen Entscheidungsprozessen mittels einer attraktiven, ganzheitlichen und benutzerfreundlichen E-Partizipationsplattform, insbesondere für OrganisatorInnen, gestartet. Das Projekt ermöglicht erstmals in Österreich eine direkt anwendbare, skalierbare und sichere Gesamtarchitektur eines E-Partizipations-Ökosystems, das für verschiedene Stakeholder auf nationaler Ebene zur Verfügung steht. Dabei berücksichtigt die Architektur grundlegende Aspekte der Sicherheit und Privatsphäre sowie des Datenschutzes und kann mit bereits bestehenden elektronischen Identitäten genutzt werden. Die sichere Authentifizierung war ein wichtiger Aspekt im Projekt, um das Vertrauen der NutzerInnen in Online-Beteiligungen zu stärken. Eine weitere Herausforderung des Projekts war es, offene und interoperable Schnittstellen zu verschiedenen neuen Medien einzubinden, die unerlässlich für eine erfolgreiche Implementierung sind, jedoch hohe Expertise im Bereich der Sicherheits- und Datenschutzstandards verlangen.

Die im Rahmen des Projekts ePartizipation durchgeführte Analyse der rechtlichen und sozialwissenschaftlichen Umwelt floss unmittelbar in die Entwicklung der Beteiligungsplattform (Prototyp) ein. Die Unterstützung der Architektur von verschiedenen Beteiligungsformen der Partizipation – die Bandbreite beginnt

Überblick eines E-Partizipations-Ökosystems





Beispiel eines fiktiven Bürgerbeteiligungsverfahrens

Projektleitung
AIT – Austrian Institute of Technology
Projektpartner
- Bundesministerium für Inneres
- Universität Wien, Arbeitsgruppe Rechtsinformatik
- Donau-Universität Krems, Zentrum für E-Governance
- Österreichische Staatsdruckerei GmbH
- rubicon IT GmbH

Kontakt
Dr. Maria Leitner
AIT – Austrian Institute of Technology GmbH
Center for Digital Safety & Security
Donau-City-Straße 1, 1220 Wien
Tel.: +43 50550 2839
E-Mail: maria.leitner@ait.ac.at
www.ait.ac.at

beim passiven Erhalten von Informationen und reicht bis zum Mitentscheiden – sowie die Unterstützung von unterschiedlichen elektronischen Identitäten spiegeln die Nutzer- und Serviceorientierung des Projekts wider. Im Rahmen der Implementierung des Demonstrators wurden, wie im Architekturkonzept vorgeschlagen, zwei voneinander unabhängige Komponenten entwickelt, die nur über eine definierte Schnittstelle miteinander kommunizieren. Sie wurden darauf ausgelegt, vollständig getrennt voneinander betrieben werden zu können, idealerweise von zwei verschiedenen Organisationen. Die erste Komponente – die E-Partizipationsplattform – umfasst alle Funktionalitäten, die eine aktive Bürgerbeteiligung ermöglichen können, und unterstützt die Beteiligungsformen Information, Konsultation und Mitentscheidung. Die zweite Komponente – der Authentication Hub – ermöglicht die Authentifizierung von TeilnehmerInnen durch die Nutzung von verschiedenen elektronischen Identitäten (z. B. Bürgerkarte, Twitter, Google).

Die Evaluierung ergab, dass eine sehr hohe Attraktivität der genutzten Anwendungsfälle vorliegt, eine hohe Relevanz und ein Mehrwert der E-Partizipationsplattform erkannt wurde, sowie eine Stärkung der Attraktivität der Bürgerkarte (insbesondere mittels Handy-Signatur) durch die Plattform erfolgen könne. Das im Projekt entworfene E-Partizipations-Ökosystem kann beispielsweise dazu beitragen, Verwaltungsabläufe und Beteiligungsprozesse langfristig einfacher, transparenter und offener zu gestalten und wechselseitige Interaktionen zwischen BürgerInnen und Behörden noch vielfältiger auszuformen.

Florida

Flexibles, teilautomatisiertes Analysesystem zur Auswertung von Videomassendaten nach Terroranschlägen

Mithilfe des bilateralen deutsch-österreichischen Projekts FLORIDA soll ein flexibles, teilautomatisiertes System geschaffen werden, welches die für die öffentliche Sicherheitsverwaltung zuständigen Behörden bei der Ermittlung, Beweisführung und Aufklärung von terroristischen Anschlägen unterstützt. Die bereitgestellten Hilfsmittel zur Analyse und Suche in großen Mengen von Videodaten sollen es den ermittelnden Beamten ermöglichen, effizienter zu arbeiten. Im Speziellen sollen das Bundesministerium für Inneres und das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung bei der Untersuchung, dem Sammeln und Sichern von Beweisen sowie bei der Aufklärung von Terroranschlägen durch ein teilautomatisiertes System unterstützt werden. Durch den Einsatz modernster Technologien soll das System die Arbeitsqualität und die Arbeitsbedingungen der in diesem Umfeld beschäftigten Personen spürbar erleichtern, indem eine teilautomatisierte Recherche, Aufbereitung und Analyse von extrem umfangreichen und heterogenen Beständen an Audio- und Videodaten unterstützt wird.

Die wichtigsten Entwicklungsziele im Projekt sind: Die Schaffung einer skalierbaren Plattform für forensische Video-Analysen in großem Umfang; die Definition entsprechender Schnittstellen; die Entwicklung neuer Analysealgorithmen sowie die Evaluierung des gesamten Projekts, hinsichtlich der Anforderungen der Projektpartner einerseits und der im Rahmen des Projekts erforschten rechtlichen und ethischen Rahmenbedingungen andererseits.

FLORIDA geht dabei von einem Extremfall in einer Größenordnung ähnlich dem Bombenanschlag auf den Boston Marathon 2013 aus, zu dem sechstausend Stunden Videomaterial entstanden sind. Das verwendete Datenmaterial soll sowohl aus Überwachungsgeräten (Kameras, Mikrofone) als auch von freiwillig zur Verfügung gestellten Aufnahmen (mobile Geräte, Smartphones) stammen können. Eine schnelle Ermittlung in solch einem Szenario bedarf deshalb Entscheidungsunterstützungssysteme zur Komplexitätsreduktion, welche das zu sichtende Material vorselektieren und nutzerfreundlich präsentieren.

Das System soll die Ermittler in zweierlei Hinsicht unterstützen. Durch die Indizierung des Video-Materials anhand von audio-visueller Analyse wird eine automatisierte Vorselektion ermöglicht, welche die einzelnen Videos anhand ihres Inhalts sortiert und priorisiert. In weiterer Folge werden Möglichkeiten zur inhaltlichen Suche im Video-Material bereitgestellt werden. Diese beziehen sich sowohl auf konkrete visuelle Objekte (z. B. Auto, Straße, Fenster etc.) als auch auf akustische Ereignisse (z. B. Explosion, Schuss, Schrei etc.). Speziell die Ergänzung um die akustische Suche stellt eine innovative Erleichterung dar, da sie eine schnelle Fokussierung auf relevante Ereignisse erlaubt.

Prototypische Darstellung des User-Interfaces. Zwei Videos können synchron abgespielt werden. Akustische Ereignisse sind farblich markiert (Schüsse: orange; Sprache: rosa; Einsatzfahrzeug: türkis)

Eine entscheidende technische Herausforderung, welche im Projektvorhaben FLORIDA umgesetzt werden soll, ist die skalierbare Analyse großer Medienbestände. Die FLORIDA-Plattform wird durch eine skalierbare, cloud-basierte Architektur in der Lage sein, sehr große Datenmengen aus verschiedenen Quellen (Uploads von Zeugen, Material aus Videoüberwachung sowie Videos von Dritten) automatisiert zu verarbeiten. Das System kann dynamisch instanziiert werden, um auch große Datenbestände (z. B. tausende Stunden an Videomaterial nach einem Terroranschlag) durch den zeitgleichen Einsatz vieler (ggf. cloud-basierter) Rechenknoten effizient und zeitsparend verarbeiten zu können. FLORIDA wird außerdem erforschen, ob und wie bereits existierende Algorithmen zur Videoanalyse im Rahmen des Projekts parallelisiert und auf der skalierbaren Plattform eingesetzt werden können. Darüber hinaus werden neue Algorithmen entwickelt werden, die auf Audioanalyse (Charakterisierung, Ereignisdetektion, Synchronisation mehrerer Videos) und Objektverfolgung abzielen.

Durch den im Projekt verfolgten Ansatz zur Interoperabilität werden Ermittler über graphische Anwendungen in der Lage sein, Ergebnisse, die durch die Vorverarbeitung der Video-Massendaten auf der Plattform generiert werden, zu nutzen und in die Ermittlungen einzubeziehen. Dies wird durch eine grafische Anwendung, basierend auf der PKE AVASYS-Plattform, gezeigt und evaluiert werden. Gänzlich neu ist hier die Einbindung von spezifischen Metadaten wie Audio-Signalen und Annotationen durch die Benutzer. Neu ist auch die Einbindung von Offline-Quellen, das heißt Datenquellen, welche nicht im Live-System vorhanden sind, sondern als file-basierte Inhalte zur Verfügung stehen. Solche Daten werden On-Demand importiert, was durch die vorherige Generierung von Metadaten möglich wird.

FLORIDA wird darüber hinaus rechtliche und ethische Anforderungen erarbeiten, die – in Bezug auf EU- und österreichisches Recht – für die Entwicklung einer solchen Plattform zur forensischen Videoanalyse und Nutzung von Daten von Augenzeugen zu beachten sind. Damit verbunden sind etwa Fragen nach der Versicherheitlichung von privatem Videomaterial, dem Diskriminierungspotential der eingesetzten Technologie oder der Legitimation staatlich-repressiven Handelns. Besonderer Bedacht wird auch auf eine enge Verzahnung mit der technologischen Entwicklung von FLORIDA genommen, um sicherzustellen, dass das System sowohl rechtlichen als auch ethischen Rahmenbedingungen entspricht, von datenschutzrechtlichen über verfassungsrechtliche und menschenrechtliche bis hin zu moralphilosophischen Grundlagen. Die Beachtung dieser ethischen und rechtlichen Rahmenbedingungen wird durch eine interne Evaluation überprüft, die sich sowohl auf die entwickelten Technologien als auch auf die Implementierung erstreckt.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Projektpartner
- Bundesministerium für Inneres
- PKE Electronics AG
- LIquA – Linzer Institut für qualitative Analyse
- Research Institute AG & Co KG

Kontakt
Dr. Ross King
AIT – Austrian Institute of Technology GmbH,
Center for Digital Safety & Security
Donau-City-Straße 1, 1220 Wien
Tel: +43 50550 4271
E-Mail: ross.king@ait.ac.at
www.ait.ac.at

Foresight-Cockpit

Softwarelösung zur strategischen, kollaborativen sowie ressortübergreifenden Entscheidungsunterstützung

Das Projekt Foresight-Cockpit befasst sich mit der Konzeption und Umsetzung eines modernen Systems zur strategischen Entscheidungsunterstützung in sicherheitspolitischen Themengebieten. Erfahrene Top-Manager aus Militär, Sicherheitsrat, Polizei, Sicherheitsdienste, Risikovorstände von DAX-Unternehmen, Sicherheitssprecher in den Parlamenten können damit entweder intern oder übergreifend gesamtstaatliche, regionale oder globale Prognose-Szenarien entwerfen, deklinieren und bewerten. Das ressortübergreifend angelegte und auf Kooperation ausgerichtete System stellt eine softwaregestützte strategische Plattform dar, die ein umfassendes Zukunftslagebild als Entscheidungshilfe für die relevanten Entscheidungsträger erstellt und visualisiert. Damit wird es möglich, frühzeitig auf unerwartete Trendbewegungen und Zukunftsszenarien aufmerksam zu werden, entsprechende qualifizierte Reaktionen zu setzen und so dauerhaft die Qualität des Risiko- und Krisenmanagements zu steigern.

Auswirkungen eines starken Wirtschafts-Isolationismus der USA, jahrzehntelanger Sanktionen gegen Russland, einer Mittelstands-Revolte in China, eines Bürgerkrieges in Syrien, globaler Ernteausfälle, eines breiten Bankenzusammenbruches in Italien oder dem Fall des Königshauses in Saudi-Arabien lassen sich mit dem Werkzeugkasten des Foresight-Cockpit jenseits des abstrakten Bedrohungsszenarios differenziert strukturieren, deklinieren, visualisieren, diskutieren, abgrenzen, so dass rechtzeitig Einsatz- und Fallback-Pläne etabliert werden können.

Die Foresight-Plattform ist darauf ausgelegt, alle relevanten öffentlichen und privaten Akteure und verbundene Informationsquellen zusammenzuführen und dadurch die ressort- und organisationsübergreifende Zusammenarbeit zu ermöglichen. Im Rahmen des Projekts wurde eine browserbasierte, strategische Entscheidungsplattform, das Foresight-Cockpit, umgesetzt. Dieser Demonstrator wurde im Rahmen von ressortübergreifenden, gemeinsamen Erprobungsverfahren hinsichtlich der operativen Leistungsfähigkeit evaluiert und in Bezug auf Usability geprüft. Der Erfolg des Projekts liegt dabei nicht zuletzt in der engen Kooperation von F&E-Partnern mit Bedarfsträgern begründet.

Foresight-Cockpit adressiert zahlreiche strategische Ziele der österreichischen und europäischen Sicherheitsforschung, u.a. auch folgende **KIRAS-Ziele:**

Ziel 1: Erhöhung der Sicherheit und des Sicherheitsbewusstseins der BürgerInnen
Das prototypisch umgesetzte System deckt einige praktische Projekte, gerade auch im Feld der Cybersicherheit, ab. So konnte z. B. die „Cyber-Risikomatrix 2016" des Kuratoriums Sicheres Österreich auf dem Demonstrator durchgeführt werden und dabei erstmals auch einer Gruppe von sicherheitsbewussten BürgerInnen direktes Feedback zum System möglich machen. Das aktuelle risikobasierte Lagebild erlaubt darüber hinaus der Öffentlichkeit eine Reflektion zu sicherheitsrelevanten Fragestellungen.

Ziel 2: Generierung sicherheitspolitisch erforderlichen Wissens
Foresight-Cockpit wurde in seiner praktischen Testphase im ressortübergreifenden, kooperativen Ansatz u.a. zur Analyse der Sicherheitslage mit Blick auf die nach Europa ausgerichtete Migration genutzt. Tagesaktuelle Ist-Lageanalysen zur Migrationslage außerhalb Europas belegen, dass die Generierung von Wissen und operative Betreibung eines gesamtstaatlichen Lagebildes möglich ist.

Ziel 5: Auf- und Ausbau von Exzellenz im Bereich der Sicherheitsforschung

Foresight-Cockpit bestätigt durch seine praktische Nutzbarkeit, dass der vernetzte Ansatz in der Forschung und die bewährte 1+1+1+1-Formel für die Zusammensetzung von Konsortien der KIRAS-Ausschreibungen Garanten für ein integriertes Entwicklungsmanagement sein können. Nur durch den engen und konstruktiven Austausch zwischen allen Projektbeteiligten war es möglich, alle Projektziele zu erreichen, einen Demonstrator zu schaffen und somit Expertise in Österreich zu halten und auszubauen.

Zusammengefasst liefert das Projekt ein System zur Entscheidungsunterstützung als onlinebasierte Softwarelösung, das bereits erfolgreich Zukunftslagebilder als Entscheidungsgrundlagen für die relevanten öffentlichen und privaten Entscheidungsträger liefert.

Der Demonstrator bindet 170 Indikatoren aus mehr als 30 Quellen in eine harmonisierte Datenbank ein und dient bereits heute der strategischen Ist-Lageanalyse und der darüber hinausgehenden strategischen Vorausschau im aktiven Dienst (Trends, Risiken, Ideen, Faktoren, Schlüsselfaktoren und deren Projektionen u.v.m.). Szenarien-Analysen alternativer und explorativer Art unterstützen komplexe Fragen zur sicherheitspolitischen Zukunft des Landes gesamtstaatlich und ressortintern gleichermaßen.

Visualisierung eines strategischen Trends mit dem Foresight Cockpit

Projektleitung
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Bundeskanzleramt
- TU Wien, Fachbereich Rechtswissenschaften
- Universität Salzburg, Fachbereich Politikwissenschaften und Soziologie
- Repuco Unternehmensberatung GmbH

Kontakt
Dr. Markus Gruber
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F, 2320 Schwechat
Tel.: +43 664 60 8444 1149
E-Mail: markus.gruber@rise-world.com
www.rise-world.com

FORMS – FORensic Marks Search

Verfahren zum semiautomatischen Suchen und Auffinden von Form- und Werkzeugspuren

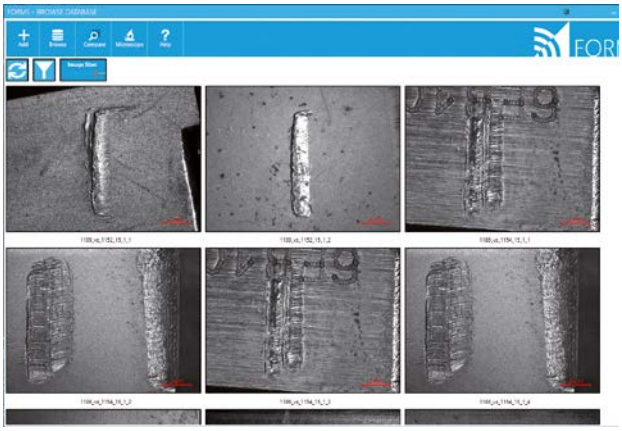
Einbruchsdiebstähle, insbesondere in Eigenheimen und Firmen, sind eine häufig auftretende Straftat in Österreich mit großem Verunsicherungspotenzial für die Bevölkerung und hohem Ressourceneinsatz für die Aufklärung seitens der Polizei. Wenn Täter auf frischer Tat ertappt werden, kann vielfach nur die zuletzt begangene Tat vor Gericht bewiesen werden. Viele Täter sind jedoch Serientäter. Um die Beteiligung an früher begangenen Straftaten zu beweisen, werden je nach Tathergang u.a. DNA, Fingerabdrücke, Schuhspuren, Materialspuren – und besonders Werkzeugspuren herangezogen. Gerade letztere können bei Einbruchsdiebstählen häufig gesichert werden. Allerdings ist der Vergleich von Werkzeugspuren von verschiedenen Tatorten sehr komplex, zeit- und personalintensiv. Derzeit werden alle ansatzweise ähnlich aussehende Spuren einzeln und händisch in einem Vergleichsmikroskop mühsam gegenübergestellt und auf Gemeinsamkeiten abgesucht. Dies erfordert hohen Aufwand, und der Vergleich einer gesicherten Werkzeugspur mit sehr vielen verfügbaren Spuren von ungeklärten Straftaten in einer umfangreichen Spurensammlung ist schlicht unmöglich. Dadurch kann das hohe Potential von Werkzeugspuren zur Aufdeckung von Seriendelikten derzeit nur unzureichend genutzt werden.

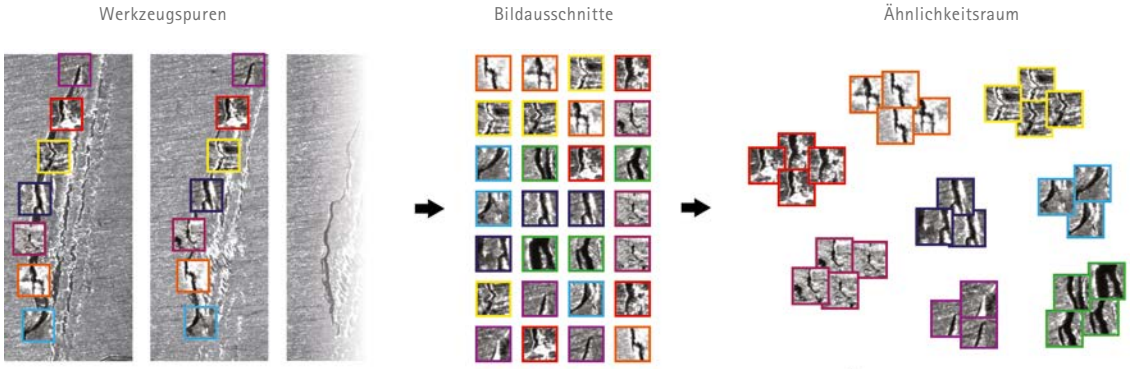
Das interdisziplinäre Forschungsprojekt FORMS hat es sich zum Ziel gesetzt, mit innovativen Computermethoden ein schnelles Verfahren zum semiautomatischen Suchen und Auffinden ähnlicher Form- und Werkzeugspuren in umfangreichen Werkzeugspurendatenbanken zu schaffen. Durch die Vorselektion ähnlicher Werkzeugspuren aus tausenden von Spuren durch die FORMS-Software kann sich die aufwändige kriminaltechnische Untersuchung im Vergleichsmikroskop auf einige wenige, möglichst ähnliche Spuren beschränken. Das reduziert einerseits den Personaleinsatz für die Vorselektion ähnlicher Spuren, stellt die freigewordenen Personalressourcen für den eigentlichen Werkzeugspurenvergleich zur Verfügung und schöpft andererseits das bislang kaum ausgenutzte Potential der Werkzeugspuren für die Aufklärung von Serienstraftaten aus.

Der Arbeitsprozess wird zukünftig folgendermaßen ablaufen: Fotos der gesicherten Spuren werden in das FORMS-System eingepflegt und von einem Werkzeugspurenspezialisten die charakteristischen Spurenmerkmale am Bildschirm markiert, um einen effektiven Abgleich zu gewährleisten. Die Suche erfolgt zentral auf einem Server, auf dem ein speziell für FORMS entwickeltes Verfahren zum Bildvergleich Ähnlichkeiten zwischen den Spuren berechnet. Der Werkzeugspurenspezialist kann in der Programmoberfläche in den von FORMS selektierten „ähnlichsten" Spuren nun mögliche Übereinstimmungen im Detail vergleichen.

Da Spuren desselben Werkzeugs durch verschiedene Faktoren wie Abnutzung, Art der Verwendung/Handhabung (z. B. Ansatzwinkel), Art des Materials, auf dem die Spur entstanden ist, u.v.m. komplexe Unterschiede aufweisen können, werden in FORMS neue informatische Methoden zum Bildervergleich herangezogen. Hier hat sich in den letzten Jahren gezeigt, dass Verfahren, die auf maschinellem Lernen basieren, in derartigen Anwendungsgebieten konventionellen Verfahren weit überlegen sind. Mit sog. „Deep Learning" ist es heute möglich, sehr große Mengen an Daten miteinzubeziehen. Ein prominentes Beispiel dafür ist die Google Bildersuche, bei der für hochgeladene Bilder mittels Inhalts-

Die Benutzeroberfläche ermöglicht das Hinzufügen, Durchsuchen und den semi-automatischen Vergleich von Werkzeugspuren





Deep-Learning-Verfahren: Werkzeugspuren werden in zahlreiche Bildausschnitte unterteilt und im Ähnlichkeitsraum gruppiert

analyse thematisch verwandte Bilder unter vielen Millionen anderer Bilder gefunden werden. Aber auch Gesichts- und Spracherkennungssoftware, die heute in Smartphones angeboten wird, basiert meist auf „Deep Learning". Der größte Vorteil dieser Verfahren zeigt sich in ihrer Zuverlässigkeit und Anpassungsfähigkeit, wie das z. B. bei moderner Spracherkennung trotz Aussprache-unterschieden oder Hintergrundgeräuschen erstaunlich gut funktioniert. Bei FORMS werden dazu zu Beginn die vom Werkzeugspurenspezialisten markierten Bereiche vom Computer in zahlreiche Bildausschnitte zerlegt. Danach werden die verschiedenen Bildausschnitte von Tat und Vergleich einander gegenübergestellt und ihre Ähnlichkeiten mittels eines eigens für FORMS entwickelten Deep Learning-Verfahrens berechnet. Dabei wird anhand von vielen Lernbeispielen mit bekannten Übereinstimmungen und Nichtübereinstimmungen das Verfahren darauf trainiert, ähnliche Strukturen zu erkennen. Da die aufwändige Berechnung nur beim Abspeichern in der Datenbank erfolgt, können Ähnlichkeitsabfragen mit neuen Spuren sehr rasch erfolgen. So ist es möglich, sehr große Mengen an Daten in die Suche miteinzubeziehen, ohne lange auf ein Ergebnis warten zu müssen oder sehr leistungsfähige Datenleitungen zu besitzen.

Erste Tests mit dem speziell für FORMS entwickelten Deep-Learning-Verfahren zeigen vielversprechende Ergebnisse, und neue Tests mit weiteren 3.500 Bilder, die unter verschiedenen Beleuchtungsbedingungen aufgenommen wurden, bringen weitere Feinregulierungen und Verbesserungen. Spätestens bis zum Projektende im September 2017 wird die erste Testversion des FORMS-Systems im Probebetrieb sein und bei der Aufklärung von Einbruchsdiebstählen einen wertvollen Beitrag leisten. Bei Bewährung soll über ein EU-finanziertes Projekt das Rollout in die Bundesländer zum flächendeckenden Einsatz erfolgen.

Projektleitung
TU Wien, Computer Vision Lab
Projektpartner
- Bundeskriminalamt
- CogVis GmbH
- Vienna Centre for Social Security (VICESSE)

Kontakt
Univ. Prof. DI Dr. Robert Sablatnig
TU Wien, Computer Vision Lab
Tel.: +43 1 58801 18351
sab@caa.tuwien.ac.at
www.caa.tuwien.ac.at/cvl/project/forms/

ForStrat-Cockpit

Kollaborative, softwarebasierte, teilautomatisierte Entscheidungsunterstützung für Echtzeit-Medien-gesteuertes Zukunftslagebild

ForStrat-Cockpit ist ein derzeit noch laufendes Forschungsprojekt, das zum Ziel hat, die Erstellung von Lagebildern zur Entscheidungsunterstützung in diversen Bereichen auszubauen und zu verbessern. Aufbauend auf den Ergebnissen von vorangegangenen KIRAS-Projekten wie Foresight-Cockpit werden bestehende Ansätze und Artefakte analysiert und gezielten Anpassungen und Erweiterungen unterzogen. ForStrat-Cockpit integriert u.a. neue Features wie Echtzeit-Online-Medienanalyse, erweitert das webbasierte Softwaretool um eine harmonisierte Indikatorenlandschaft und stellt den Entscheidungsträgern neueste Foresight-Methoden zur Verfügung. Die bereits erprobten Kernaspekte dieses Werkzeugs für Entscheidungsträger, wie die Möglichkeit zur gleichzeitigen und unabhängigen Bearbeitung vielfältiger Themenfelder, bleiben dabei uneingeschränkt vorhanden.

Zentrale Projektziele von ForStrat-Cockpit sind die weitere Steigerung der Analysefähigkeit für NutzerInnen und die Entwicklung eines erstmals echtzeitorientierten gesamtstaatlichen Lagebildes inklusive der Aufbereitung von Strategie- und Handlungsoptionen für die Zielgruppe.

Weiters zielt das Projekt vertieft darauf ab, neben dynamischen Daten auch für einzelne Partner jeweils vertrauliche Daten zu einem Gesamtbild zu aggregieren (Zonenkonzepte), so dass in späterer Zukunft dynamische, kollaborative Aggregationen und Auswertungen für Anlassfälle möglich werden, ohne dass Partner vertraulichste Einzeldaten (datenschutz-)rechtlich unzulässig weitergeben.

Ausgangslage

In früheren KIRAS-Projekten wurde deutlich erkannt, dass ein Beitrag zur Interoperabilitätssteigerung zwischen öffentlichen und privaten Ressorts (z. B. zwischen Behörden und Unternehmen) durch die Anpassung von Prozessen und Analysen an Hand eines gemeinsamen, systemisch geprägten Vorgehens für neue Formen von Projekten und Zusammenarbeitsmodellen unumgänglich ist (bspw. das operative Management aller Migrationsthemen).

Das kollaborative Bearbeiten von generischen Themen und somit letztendlich die Möglichkeit des schnellen Reagierens (Quick Response) auf ein wechselndes Lagebild wurde durch die bisherigen Tools und Systeme nicht zufriedenstellend unterstützt, weil ihre Auslegung vor allem auf langfristige Trendanalyse für das Top-Management priorisiert war.

Die Notwendigkeit einer Erweiterung der Ausgangsbasis konnte in vorangegangenen ressortübergreifend durchgeführten Projekten mit den Bedarfsträgern BM.I, BMLVS und BKA bereits aufgezeigt werden. Die dort vorhandenen relevanten systemischen Lücken, die beim Erstellen und Bearbeiten des gemeinsamen Lagebildes im Sinne von Weiterentwicklungs- und Innovationspotentialen auftraten und systematisch identifiziert werden konnten, werden im Projekt ForStrat-Cockpit geschlossen.

ForStrat-Cockpit Konzept

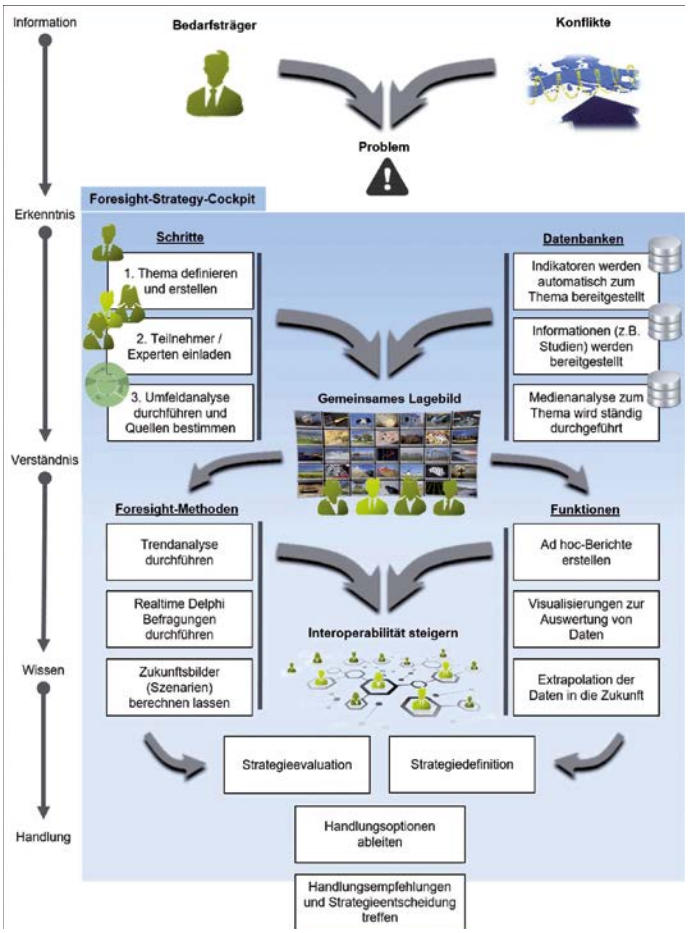
ForStrat-Cockpit schließt die Lücke hin zu einem ressortübergreifenden, echtzeitgestützten Lagebildmonitor und folglich zu einem gemeinsamen Strategie- und Foresight-System, das den sicherheitsrelevanten Akteuren in Österreich als wesentliches Medium zum Austausch und zur vertieften Kooperation dienen soll. Das Projekt hilft dabei, die vorhandenen Herausforderungen in der Kommunikations- und Führungsfähigkeit zwischen zivilen, militärischen und behördlichen Akteuren zu bewältigen, und trägt zu einem umfassenden Ansatz in der Sicherheitspolitik und einem verbesserten wechselseitigen Verständnis füreinander bei.

Das ForStrat-Cockpit Konzept umfasst im Wesentlichen:

- die vorgelagerte, intelligente und
- automatisierte Datenauswertung
- die flexible Anbindung unterschiedlicher Quellen
- die technische Fähigkeit zur Echtzeit-Analyse von sozialen Medien
- die Möglichkeit zur Bewertung strategischer Optionen

Durch diese F&E-Tätigkeiten, deren Erprobung und Integration in ein IT-System/Produkt wird erstmalig z. B. ein ganzheitlicher, gemeinsamer Strategie- und Foresight-Prozess ressortübergreifend, flexibel und schnell durchgeführt werden können. Der inkludierende Ansatz schafft die Möglichkeit, ausgehend von einer gemeinsamen Lageanalyse die zahlreichen entscheidenden Faktoren und Entscheidungsparameter festzustellen. Mit Hilfe dieser identifizierten Faktoren, und unterstützt durch das Tool, können in Folge Zukunftsszenarien oder auch strategische Handlungsfelder entworfen werden.

Somit wird es in einem kooperativen und ganzheitlich-systemisch gedachten Prozess möglich, die notwendigen und im Sinne der Arbeitsteilung zu besetzenden Handlungsoptionen aufzuteilen und deren Wirkung mit Hilfe von Pre-Testmöglichkeiten vorab abzuschätzen.



ForStrat-Cockpit Flow

Dadurch wird zum einen die Interoperabilität der Sicherheit generierenden und Stabilität gewährenden Institutionen und Organisationen verbessert. Zum anderen kann dadurch die Formulierung und Umsetzungsmöglichkeit von gemeinsamen Handlungsoptionen erneuert und in Teilen neu gedacht werden.

Ein Fallbeispiel: Akute Stimmungsbilder in sozialen Medien eines destabilisierten Landes verbunden mit demoskopischen Werten und wirtschaftlichen Erwartungswerten können unterschiedliche Institutionen so frühzeitig von den Effekten informieren, dass operativ und kommunikativ rechtzeitig gegengesteuert oder gefördert werden kann, je nach politischem Willen: aktiv statt reaktiv. Ebenso wird so erstmals denkbar, z. B. Ausbildung, Schulung und Arbeitserlaubnisse in unterschiedlichen Regionen Europas nach Bedarf, Einkommen und sozialer Integrierbarkeit „vernünftig" zu bemessen.

Projektleitung
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Universität Salzburg, Fachbereich Politikwissenschaft und Soziologie
- Modul University Vienna GmbH
- Repuco Unternehmensberatung GmbH

Kontakt
Dr. Markus Gruber
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F, 2320 Schwechat
Tel.: +43 664 60 8444 1149
E-Mail: markus.gruber@rise-world.com
www.rise-world.com

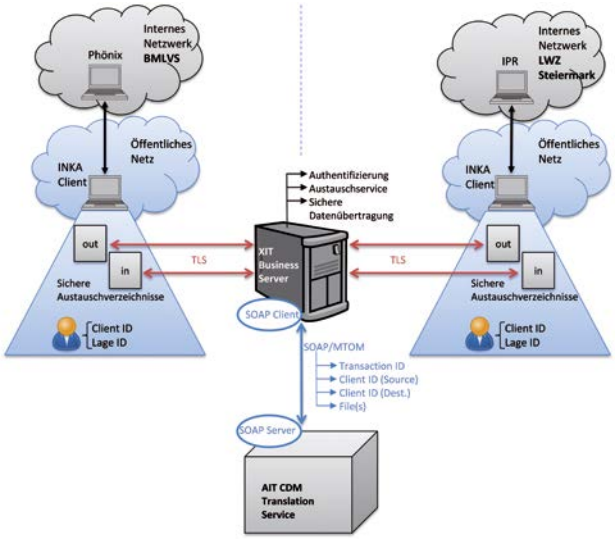
INKA

Interoperabilität zwischen zivilen und militärischen Organisationen im Katastrophenmanagement

Im vergangenen Jahrzehnt kam es in Österreich vermehrt zu Katastrophen größeren Ausmaßes wie beispielsweise Hochwasser, Muren und Lawinenabgängen.

Neben den physischen Herausforderungen bei der Bewältigung solcher Großschadenslagen und Katastrophen ist die notwendige Zusammenarbeit und die dadurch bedingte Koordination der unterschiedlichen teilnehmenden Organisationen und Partner auf allen Ebenen (operativ/taktisch/strategisch) ein zentraler Erfolgsfaktor für eine effektive und effiziente Hilfeleistung. Neben den Blaulichtorganisationen und den Fachabteilungen der Landes- und Bundesverwaltungen (z. B. Katastrophenschutzabteilungen, Wildbach- und Lawinenverbauung, ZAMG) nimmt auch das österreichische Bundesheer als wichtiger Partner in den Phasen der Katastrophenbewältigung und Wiederherstellung der Infrastruktur eine tragende, unverzichtbare Rolle ein. Für Behörden und Organisationen, deren Strukturen, Abläufe und im Besonderen auch Informations- und Kommunikationssysteme primär auf die Agenden im Kontext der öffentlichen Sicherheit – national, aber auch international – ausgerichtet sind (z. B. Österreichisches Bundesheer), stellt die Zusammenarbeit und Koordination mit nicht-militärischen und vermehrt auch nicht-staatlichen Organisationen im Zuge von Assistenzleistungen eine besondere Herausforderung dar.

Ziel des Projekts INKA war es, durch die Schaffung einer Interoperabilitäts-Schnittstelle für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im zivilen Katastrophenmanagement das Angebot im Bereich der standardisierten, IT-gestützten Informationskanäle zu verbessern. Im Speziellen adressierte das Projekt die Einbindung des BMLVS in das Informationsmanagement-Netzwerk der einzelnen Einsatzorganisationen, um dadurch den organisationsübergreifenden Informationsaustausch zu verbessern. Dies wurde durch die prototypische Umsetzung eines Datenknotenpunkts erreicht, der einen bidirektionalen Datenaustausch zwischen dem BMLVS und nicht-militärischen Einsatzorganisationen und Behörden über offengelegte Schnittstellen ermöglicht. Hierbei stellten die besonderen Bedürfnisse des österreichischen Bundesheeres (wie bspw. Schutz von militärischen Informationen) wie auch die Organisation mit öffentlichen



INKA Interoperabilitätsschnittstelle

Sicherheitsaufgaben eine besondere Herausforderung dar, welche es stellvertretend und mit dem Hintergrund der Übertragbarkeit auf andere Behörden im Kontext der öffentlichen Sicherheit zu bearbeiten galt.

Mit Hilfe eines speziellen, an der TU Graz entwickelten und an das Projekt angepassten Vorgehensmodells wurden die Akteure, deren Kommunikationswege und die Prozesse im Rahmen des organisationsübergreifenden Informationsaustausches bei der Bewältigung von Katastrophen untersucht und dabei potentielle Umsetzungspunkte für die Interoperabilitäts-Schnittstelle identifiziert. Im Rahmen dieser Untersuchung wurden folgende Themenkomplexe analysiert:

- Organisation und Strukturen
- Prozesse
  - Einsatz- und Anforderungsprofile
  - Nutzenhebel
- Kommunikation und Information
  - Terminologie
  - Semantik
  - Technologie
- Datensicherheit, Datenschutz undallgemeine Rechtssicherheit (z. B. Haftungsfragen wegen Kommunikationsproblemen)

In einem ergebnisoffenen Ansatz wurden auf der Basis dieses Vorgehensmodells im Zuge der Anforderungsanalyse zwei Verbesserungspotenziale für den Informationsaustausch zwischen den zivilen und militärischen Organisationen bei der Katastrophenbewältigung prototypisch implementiert und im Rahmen einer zivil-militärischen Katastrophenschutzübung im Herbst 2016 im Bezirk Voitsberg evaluiert:

1. **INKA Interoperabilitätsschnittstelle**
Die INKA Interoperabilitätsschnittstelle ermöglicht einen sicheren, weitgehend medienbruchfreien Datenaustausch zwischen den Führungsinformationssystemen des österreichischen Bundesheeres (FüIS Phönix) und der Landeswarnzentrale Steiermark (FüIS Intergraph Planning & Response). Dabei geht es nicht um den Austausch von geographischen Daten, die im Lagebild als separater Layer angezeigt werden können, sondern um eine transparente Umsetzung der zivilen und militärischen Datenformate mit dem Ziel eines vollständig integrierten Lagebildes auf beiden Seiten.

2. **INKA Virtuelle Amtstafel**
Aus dem Wunsch der Bedarfsträger nach einem elektronischen Austausch von lagerelevanten Dokumenten bei kleinräumigen Katastrophenereignissen entstand der zweite INKA-Prototyp. Dieser ist als Web-Applikation implementiert und kann somit einfach über den Web-Browser aufgerufen werden. Die Kernfunktionalität besteht in der Anlage von Dokumentenmappen mit geografischer Verortung auf der Landkarte. Damit können z. B. zu einer Schadstelle alle relevanten Dokumente wie Verordnungen, Ankündigungen, Informationen oder Erlässe gesammelt abgelegt werden. Über ein definiertes Rollen- und Rechtesystem können die Dokumente für verschiedene Benutzergruppen bzw. Organisationen oder Behörden zugreifbar gemacht werden. Außerdem besteht die Möglichkeit, Dokumente für die Öffentlichkeit sichtbar zu machen, wodurch sich ein nicht angemeldeter Benutzer der Web-Applikation über allfällige Verordnungen oder Erlässe informieren kann.

Bei beiden Prototypen wurde besonderes Augenmerk auf die Sicherheit bei der Datenübertragung, die Datenintegrität und -authentizität gelegt. Außerdem bildete die Bewertung der rechtlichen Fragen hinsichtlich der gesetzlichen Grundlagen des Katastrophenschutzes, des Datenschutzgesetztes und des Telekommunikationsrechts einen wesentlichen Bestandteil des Projekts.

Projektleitung
AIT – Austrian Institute of Technology,
Center Digital Safety & Security

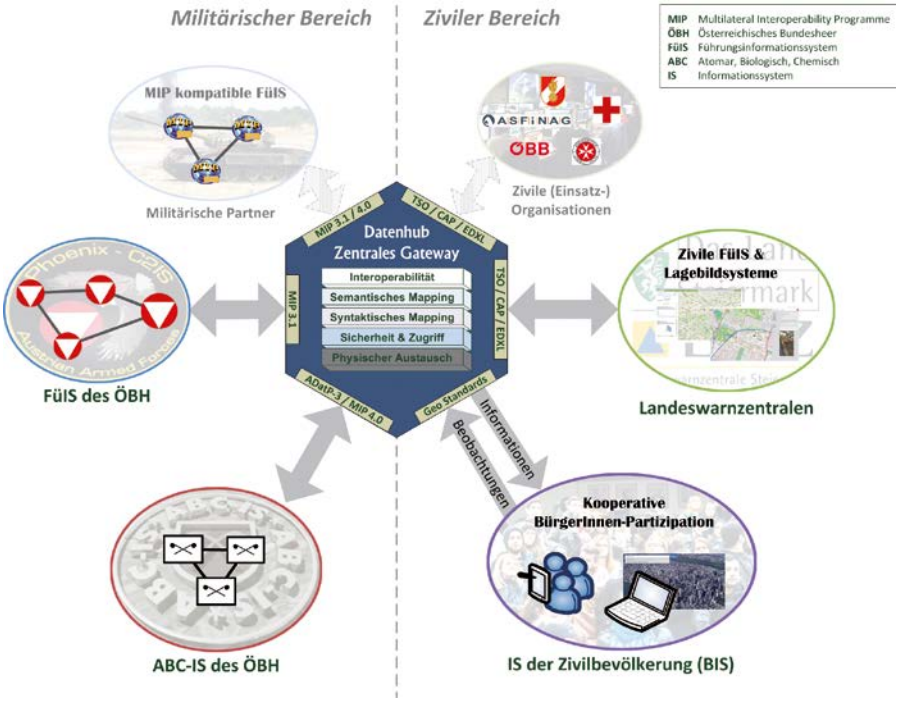
Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- TU Graz, Institut für Maschinenbau- und Betriebsinformatik
- XiTrust Secure Technologies GmbH,
- EOC Quality Management gemeinnützige GmbH

Kontakt
Dr. Ivan Gojmerac
AIT – Austrian Institute of Technology GmbH,
Center for Digital Safety & Security
Donau-City-Str. 1, 1220 Wien
Tel.: +43 50550 2826
E-Mail: ivan.gojmerac@ait.ac.at
www.ait.ac.at

INTERPRETER

Interoperabilität im Katastrophenmanagement der nächsten Generation

Die Hilfeleistung bei Elementarereignissen und Unglücksfällen außergewöhnlichen Umfanges stellt neben der Landesverteidigung eine der wichtigsten verfassungsmäßigen Aufgaben des Österreichischen Bundesheeres dar. Im Zuge solcher Einsätze wirkt das Bundesheer gemeinsam mit den zivilen Strukturen auf allen föderalen Ebenen an der Bewältigung der vorliegenden Situation mit, wobei die informationstechnische Interoperabilität der zivilen und militärischen Einsatzkräfte von besonderer Bedeutung ist, insbesondere auf der Ebene von Landeswarnzentralen und den Militärkommanden der einzelnen Bundesländer. In Anknüpfung an den aktuellen Stand der Forschung wird im Projekt INTERPRETER mittels modernster Softwaredesignmethoden ein vollständig automatisierter Datenaustausch zwischen den zivilen und militärischen (Führungs-)Informationssystemen mit besonderem Fokus auf die semantische Integrität der ausgetauschten Informationen entwickelt. Durch den modularen Aufbau von INTEPRETER wird des Weiteren eine generische Erweiterbarkeit des Systems geschaffen, die als Grundvoraussetzung für seine nachhaltige Verwendbarkeit gilt. Darüber hinaus wird das Projekt ein erweitertes Konzept der IT-gestützten Einbindung der betroffenen Bevölkerung in den Prozess des Krisen- und Katastrophenmanagements entwickeln und evaluieren, wodurch den



INTERPRETER Architekturkonzept

aktuellen Trends nach mehr Bürgerbeteiligung Rechnung getragen wird und gemeinsam mit den GSK-Partnern das Potential zur Steigerung der Gesamteffizienz des Krisenmanagements in Österreich beleuchtet wird.

Zu diesem Zweck wird das vorliegende Projekt sowohl die Präferenzen der Bevölkerung als auch der Bedarfsträger erheben, um technische und organisatorische Anforderungen definieren zu können, die in der Architektur des neuen Systems zur zivil-militärischen Interoperabilität berücksichtigt werden müssen. Da die Beteiligung der Bevölkerung am Prozess des Krisen- und Katastrophenmanagements in allen ihren Phasen viele Bereiche der Gesetzgebung berührt, wird INTERPRETER eine ausführliche Analyse der aktuellen gesetzlichen Rahmenbedingungen durchführen und gegebenenfalls Novellierungen vorschlagen, die die aktuell vorhandenen Einschränkungen unter Einhaltung striktester Privatsphärenschutzmechanismen aufheben bzw. ablösen könnten. Die resultierende INTERPRETER-Architektur wird im Rahmen des Projekts in Form eines Proof-of-Concept implementiert, das in der Evaluierungsphase sowohl mit den Bedarfsträgern als auch mit der Bevölkerung bezüglich seiner Akzeptanz und Effizienz evaluiert wird. Die praktische Relevanz von INTERPRETER ist nicht nur durch die innovativen Kernideen des Projekts gegeben, sondern sie erschließt sich vielmehr durch das bedacht ausbalancierte, interdisziplinäre Konsortium, das bestrebt ist, die angedachten neuen Funktionalitäten mittelfristig auch operationell umzusetzen.

Aus diesem Grund wird INTERPRETER einen wichtigen Meilenstein in der Entwicklung der zivil-militärischen Interoperabilität darstellen und in den nächsten Jahren einen unersetzlichen Beitrag zum Krisen- und Katastrophenmanagement in Österreich leisten.

Zentrales Element ist der INTERPRETER-Datenhub, der ausschließlich über standardisierte Schnittstellen mit den bestehenden zivilen und militärischen Informationssystemen kommuniziert und an ein spezifisches Web-Portal angebunden ist, das dem Informationsaustausch mit der Zivilbevölkerung dient.

Folgende Komponenten werden in INTERPRETER als Proof of Concept entwickelt und evaluiert:

- **INTERPRETER Mapping Engine.** Sie stellt das Kernelement des Datenhubs dar, zuständig für die Übersetzung der Begrifflichkeiten, basierend entweder auf Ontologien oder auf Taxonomien der beteiligten Systeme.
- **INTERPRETER Interoperabilitätsschnittstellen inkl. Plugin-Konzept.** Der Datenhub implementiert die zivilen und militärischen Interoperabilitätsprotokolle, die für die Kommunikation zwischen den Systemen notwendig sind. Die Implementierungen basieren auf einem innovativen Plugin-Konzept, das eine einfache Erweiterung des Datenhubs und somit die Zukunftssicherheit des Systems gewährleistet.
- **INTERPRETER Kooperatives Bevölkerungsinformationssystem (BIS).** Diese Komponente ermöglicht den Informationsaustausch zwischen der Zivilbevölkerung und den Einsatzkräften. Die Benutzerschnittstelle des BIS basiert auf mobilen und web-basierten Anwendungen, während das Back-End für Proof of Concept-Zwecke rudimentäre Informationssystemelemente beinhalten wird, die die Erfassung, Darstellung und den Austausch von Informationen aus und mit der Bevölkerung ermöglichen.

Projektleitung
AIT – Austrian Institute of Technology, Center Digital Safety & Security

Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- Amt der Steiermärkischen Landesregierung, Fachabteilung Katastrophenschutz und Landesverteidigung, Referat Landeswarnzentrale
- Frequentis AG
- Syncpoint GmbH
- Universität Wien, Rechtswissenschaftliche Fakultät, Abteilung für Völkerrecht und Internationale Beziehungen des Instituts für Europarecht, Internationales Recht und Rechtsvergleichung
- IFES Institut für empirische Sozialforschung GmbH
- IFES Feld GmbH
- JOANNEUM RESEARCH Forschungsgesellschaft mbH

Kontakt
Dr. Ivan Gojmerac
AIT – Austrian Institute of Technology GmbH, Center for Digital Safety & Security
Donau-City-Str. 1, 1220 Wien
Tel.: +43 50550 2826
E-Mail: ivan.gojmerac@ait.ac.at
www.ait.ac.at

IsoCSI

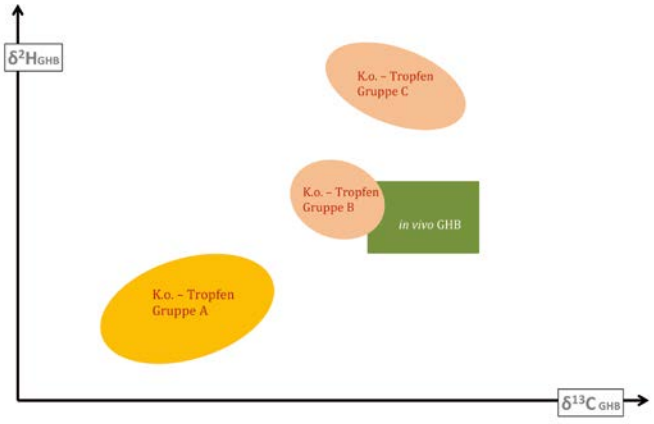
Anwendung der Isotopenanalytik in der Forensik

Im Rahmen des Projektes IsoCSI wurde anhand zweier Pilotprojekte der Nutzen des Einsatzes von stabilen Isotopen in der Beweissicherung und Verbrechensbekämpfung erprobt.

Pilotprojekt 1

Der Missbrauch von 4-Hydroxybutansäure (GHB) bzw. -Butyrolacton (GBL) als K.o.-Tropfen stellt eine enorme Schwierigkeit in der Strafverfolgung dar, da nur wenige Opfer die Straftat bei den Behörden melden oder sich gesundheitlich untersuchen lassen. Selbst bei polizeilicher Meldung ist es aufgrund des Gedächtnisverlustes der Opfer und fehlender analytischer Nachweismethoden schwierig, den Nachweis einer Straftat zu führen. Der Stand der Technik ermöglicht einen gesicherten Nachweis nur 6-12 Stunden nach Gabe der K.o.-Tropfen. In diesem Zeitraum befinden sich die meisten Opfer noch in tiefer Bewusstlosigkeit.

Im Rahmen des Projekts IsoCSI wurden neue Wege in der Analytik gegangen: Anstatt die Konzentration von GHB in Urin zu ermitteln, wurden die Isotopenverhältnisse von GHB analysiert. Die Signatur stabiler Kohlenstoff- und Wasserstoffisotope lässt nämlich einen Schluss zu, ob das GHB aus körpereigener Produktion (in vivo) oder durch Gabe eines künstlichen Stoffes (exogen) entstanden ist. Damit kann das Nachweisfenster für exogene Anreicherung von GHB/GBL signifikant erhöht werden.



Isotopenwerte GHB/GHL

Die Abteilung für Forensische Toxikologie der Medizinischen Universität Wien hat mehrere innovative Methoden untersucht, jedoch musste – aufgrund der starken individuellen Schwankungen zwischen den biologischen Proben und der tw. sehr niedrigen Konzentrationen – schlussendlich auf die in der Literatur beschriebene, mehrstufige Probenvorbereitung zurückgegriffen werden. Zweistufig vorgereinigte Urinproben von mehr als 130 Probanden wurden mittels Hochleistungsflüssigkeitschromatograph (HPLC) weiter aufgereinigt. Die Fraktion mit GHB wurde für die gaschromatographische (GC) Analyse vorbereitet, in GBL umgewandelt und extrahiert. Injektionskühlung und Lösungsmittel-Abdampfung mit einem speziellen Temperatur-Druck-Profil ermöglichten die Etablierung einer optimalen gaschromatographischen Analyse.

Hierauf wurden die aufgetrennten chemischen Komponenten in einem Verbrennungsofen zu Kohlendioxid oxidiert und im Isotopenverhältnismassenspektrometer (IRMS) hinsichtlich ihrer Isotopenkomposition untersucht.

Anhand der gesammeltem Urinproben konnte eine Datenbank für den endogenen Bereich der Kohlenstoff-Isotopensignatur von GHB im Urin erstellt werden, des Weiteren wurde erstmalig auch die Wasserstoff-Isotopensignatur von in vivo-GHB ermittelt. Darüber hinaus wurden vom Bundeskriminalamt beschlagnahmte GHB- und GBL-Proben analysiert. GBL musste in die Studie einbezogen werden, da es im menschlichen Blut durch die 1,4-Lactonase zu GHB hydrolysiert wird und genauso wirkt wie GHB.

Die GBL/GHB-Substanzen konnten anhand der Isotopenverhältnisse in drei unterschiedliche Gruppen klassifiziert werden:

- **Gruppe A:** Hier unterschieden sich sowohl Kohlenstoff- als auch Wasserstoffisotopenverhältnisse deutlich vom in vivo-Bereich. Die meisten Proben gehören zu dieser Gruppe.
- **Gruppe B** weist sowohl in Wasserstoff- als auch Kohlenstoff-Isotopenwerten eher eine geringfügige Abweichung zum in vivo-Bereich auf. Eine eindeutigere Identifikation von extern zugeführten GHB/GBL in niedrigeren Konzentrationen blieb weiterhin schwierig.
- **Gruppe C** ist in der Kohlenstoff-Isotopensignatur fast identisch mit dem in vivo GHB-Bereich, aber sehr gut über die Wasserstoff-Isotopenwerte differenzierbar.

Die Resultate zeigen, dass in den meisten Fällen die Möglichkeit der Unterscheidung von endogenem und exogenem GHB besteht, auch wenn die Konzentration von GHB im Urin im natürlichen Bereich liegt. Dies zeigt deutlich, dass das Verfahren als Untersuchungsmethode etabliert werden kann und Potential zur Weiterentwicklung hat, zumal eine Erweiterung der Analyse auf die Isotopenverhältnisse von Sauerstoff dazu beitragen könnte, auch die Gruppe B vom in vivo-Bereich abzugrenzen.

Zudem wurde im Rahmen des Projekts der Status Quo der rechtlichen und ethischen Situation für Gesundheitsbehörden und Opfer bei der Probensicherung und Strafverfolgung ermittelt. Durch das Institut für Ethik und Recht in der Medizin (Medizinische Universität Wien) wurde ein theoretischer (rechtlicher) Teil erarbeitet, und es wurden empirische Daten erhoben. Der empirische Teil umfasst ExpertInnen-Interviews mit MitarbeiterInnen von Opferschutzeinrichtungen, mit Opfern von K.o.-Mittel-Delikten, Onlinefragebögen für die potenzielle Opfergruppe und für MitarbeiterInnen von Krankenanstalten sowie die Erhebung zweier Strafakten. Es wurden somit qualitative wie quantitative Forschungsmethoden angewandt, mit dem Ziel, Daten und Zahlen zu Straftaten im Zusammenhang mit K.o.-Mitteln für die Jahre 2014 bis 2016 zu erhalten. Daneben lag der Schwerpunkt auf der Schulungs- und Aufklärungsarbeit zum Thema K.o.-Mittel-Delikte, z. B. durch Vorträge auf einer Opferschutztagung, Vorträge und Schulungen für medizinisches Personal in Spitälern sowie die Präsentation der Forschungsergebnisse auf der Abschlusstagung „K.o.-Mittel-Delikte: Herausforderungen, Strafverfolgung und Opferschutz". Dort fand auch ein interdisziplinärer Austausch jener Berufsgruppen statt, die mit Opfern von K.o.-Mittel-Delikten zu tun haben.

Pilotprojekt 2

Ein weiterer Bestandteil des Projekts war die Entwicklung eines analytischen Verfahrens zur Messung der Isotopensignaturen von Baumwollfasern von Tatortsicherungen. Hierbei sollte versucht werden, Proben mit einem Gewicht < 9 ng zu analysieren. Durch die Optimierung der Analytik konnte die minimalbenötigte Menge auf 20 ng Kohlenstoff minimiert werden, was jedoch nicht ausreichend für die Fragestellung war. Weiterhin wurde die Variabilität der Kohlenstoff-, Wasserstoff- und Sauerstoff-Isotopensignaturen für unverarbeitete Baumwolle ermittelt und eine Datenbank für Produktionszentren weltweit erstellt. Die im Projekt entwickelte und optimierte Methode zur Analyse von Baumwollfäden konnte somit als Analytik für den Abgleich der Herkunft von Baumwollfasern etabliert werden.

Projektleitung
Imprint Analytics GmbH
Projektpartner
- Bundeskriminalamt
- Medizinische Universität Wien, Abteilung für Forensische Toxikologie, Institut für Ethik und Recht in der Medizin

Kontakt
Dr. Balázs Horváth, Dr. Bernd Bodiselitsch
Imprint Analytics GmbH
Werner von Siemens Straße, 7343 Neutal
Tel.: +43 59010 8900
E-Mail: horvath@imprint-analytics.at,
bodiselitsch@imprint-analytics.at
www.imprint-analytics.at

ITsec.at

Abhärtung der österreichischen IT-Landschaft gegen Bedrohungen aus dem Cyberraum

Angriffe aus dem Cyberraum gehören heute zu den größten Gefahren für Unternehmen und den öffentlichen Sektor. Ohne funktionierende IT steht das öffentliche Leben still, viele Unternehmen sind in ihrer Existenz gefährdet. Die heutige IT ist leicht verwundbar, die Angriffe nehmen stetig zu. Besonders gefährlich sind Angriffe, welche die Widerstandsfähigkeit gezielt schon im Produktdesign bzw. während der Produktentwicklung reduzieren, indem sich die Schwachpunkte von Anfang an im Produkt befinden. Da fast die gesamte IKT-Infrastruktur Österreichs aus dem Ausland stammt, ist die Abhängigkeit von meist „unkontrollierbaren" Herstellern (Produzenten) besonders hoch. Wer Produkte kauft, die in irgendeiner Form Software enthalten, kauft das Problem mitunter schon mit: Unsichere Komponenten in Produkten können sich für Organisationen (Behörden, Unternehmen, Verbände etc.) als Problem herausstellen. Trotz bzw. gerade wegen der relativ geringen Bedeutung Österreichs – aber auch der EU – im globalen IKT-Herstellermarkt, kann dieser scheinbar ausweglosen Abhängigkeit entgegengewirkt werden - durch die IT-sichere Beschaffung der Produkte.

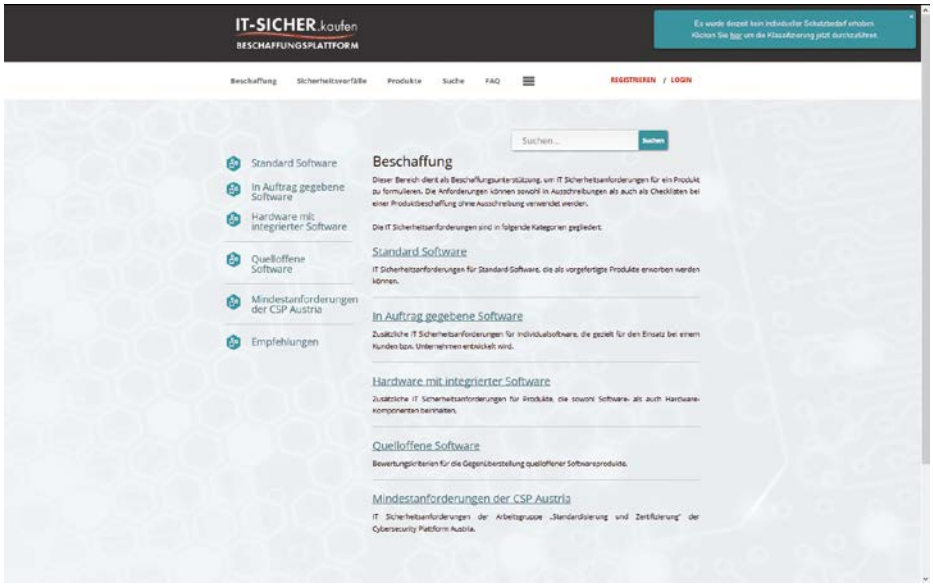
Das Forschungsprojekt ITsec.at beschäftigte sich mit den oben genannten Gefahren für die österreichische IKT-Landschaft und zeigte auf, wie wichtig IT-Sicherheit bereits beim Einkauf jeglicher Software enthaltender Produkte ist. Unter anderem wurden eine umfangreiche Beschaffungsplattform (Entscheidungsunterstützungssystem), eine Vertrauensdatenbank, Anforderungskataloge inklusive Schutzbedarfsklassifikation für die Beschaffung und Qualitätsvorgaben für Anbieter erforscht und ausgearbeitet. Mit der Beschaffungsplattform „www.it-sicher.kaufen" stehen weltweit einzigartig allen Österreichern die wichtigsten Informationen für einen IT-sicheren Einkauf von Hardware und Software zur Verfügung, kostenlos, herstellerunabhängig, werbefrei und passend zu den individuellen Ansprüchen der Benutzer.

Die Plattform enthält Anforderungskataloge wie Checklisten für den Einkauf und Texte (Templates) für Ausschreibungen und Pflichtenhefte, behandelt das Thema Vertrauen in Lieferanten und enthält weitere erforderliche Informationen. Bei den Anforderungskatalogen wird unterschieden zwischen Standardsoftware, Individualsoftware (in Auftrag gegebene Software) und Hardware mit integrierter Software (Firmware, embedded Software). Zudem gibt es Informationen, worauf bei der Beschaffung von quelloffener Software (Open Source SW bzw. freie Software) geachtet werden sollte. Die Kategorie „Empfehlungen" enthält Informationen wie z. B. zu kryptografischen Algorithmen, und welche Kenngrößen bei der Verwendung aktuell zu beachten sind.

Das Projekt ITsec.at ging von jeglichen kaufbaren Produkten aus, die Software in irgendeiner Form enthalten. Weil heute fast alle Produkte direkt oder indirekt eine Gefahr darstellen können, für Organisationen (Behörden, Unternehmen, Verbände etc.) wie auch im Privatbereich (Überwachungskameras, Haushaltsgeräte, Fahrzeuge etc.), betrifft das Problem praktisch alle Menschen, die Produkte einkaufen. Der Schwerpunkt liegt aber bei Personen, die in Unternehmen Beschaffungsprozesse durchführen, für die eigene Infrastruktur des Unternehmens, für die Produktion und im Handel.

Mit dem Projekt ITsec.at und der Beschaffungsplattform erhält der Einkauf jeglicher Software (Standard-SW, Individual-SW, Open Source SW) und Software enthaltender Hardware (Maschinen, Systeme, Steuerungen, Geräte, Kommunikationseinrichtungen, Fahrzeuge, bis hin zu Haushaltsgeräten) den wichtigen Faktor IT-Sicherheit. Indem beim Einkauf von Produkten auf diesen Aspekt geachtet wird, kann Österreich IT-sicherer gemacht werden. Da IT-Sicherheit viel mit Vertrauen zu tun hat und Vertrauen zu Unternehmen, die in Österreich beheimatet sind, leichter aufzubauen ist als z. B. zu Unternehmen aus den USA oder dem asiatischen Raum, kann die vorliegende Beschaffungsplattform auch die österreichische Wirtschaft umsatzmäßig „beflügeln". Vor allem, wenn österreichische Hersteller mit Unterstützung durch die Projektergebnisse ihre Produkte IT-sicherer machen. Dadurch verringert sich die IT-Abhängigkeit von Produkten aus dem Ausland und erhöht sich die Digitale Souveränität Österreichs.

Webseite der Beschaffungsplattform „www.it-sicher.kaufen"



Der Berücksichtigung gesellschaftlicher Fragestellungen wurde Rechnung getragen, indem der Untersuchungsgegenstand aus einer gesellschaftlichen und sozialen Perspektive dargestellt und kritische Bereiche identifiziert wurden, die ins Design von Abwehrmaßnahmen gegen Cyber-Bedrohungen einfließen können. Zur Datenerhebung wurde auf die Methode der Experteninterviews zurückgegriffen.

Projektergebnisse finden sich auf der Beschaffungsplattform „www.it-sicher.kaufen". Des Weiteren entstand eine Publikation im Springer Verlag in der Reihe essentials mit dem Titel „Beschaffung von Hard- und Software unter Berücksichtigung der IT-Sicherheit", welche Projektergebnisse veröffentlicht wurden und eine perfekte Werbung für die Plattform „www.it-sicher.kaufen" und das Projekt ITsec.at darstellen.

Projektleitung
FH St. Pölten, Institut für IT Sicherheitsforschung
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Bundeskanzleramt
- Magistrat der Stadt Wien (MA14)
- SEC Consult Unternehmensberatung GmbH
- ITSV und Cyber Security Plattform der Bundesregierung

Kontakt
Univ.-Doz. D.I. Dr. Ernst Piller
FH Pölten, Institut für IT Sicherheitsforschung
Matthias Corvinus-Strasse 15, 3100 St. Pölten
Tel.: +43 2742 313 228 636
E-Mail: ernst.piller@fhstp.ac.at
www.fhstp.ac.at/its

Mobile eCard

Effekte der Digitalisierung mit Schwerpunkt Sicherheit und Vertrauen

Das Projekt Mobile eCard verfolgt das primäre Ziel, eine innovative, sichere und zuverlässige Möglichkeit zur digitalen Identifikation im Gesundheitswesen zu schaffen, die unabhängig von der physischen Karte verlässlich funktioniert. Das Projekt ist explorativ (Usability, Security, mobile Engineering, End2End) und etabliert keine Technologie, die unmittelbar produktiv zu setzen wäre. Als Identifikations- und Testmedium dient dabei die österreichische (und experimentell auch die Deutsche und Französische) Gesundheitskarte.

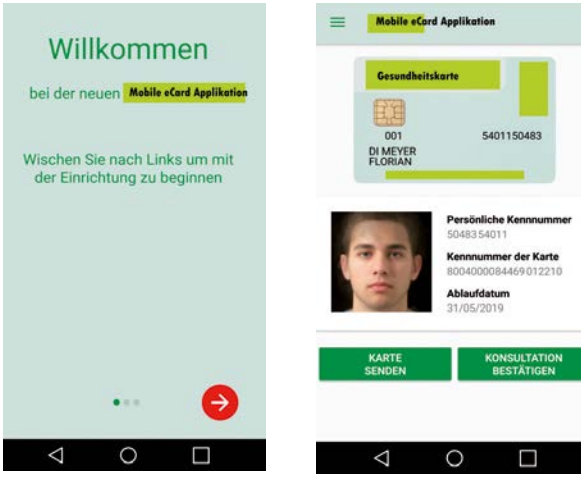
Die Gesundheitskarte der digitalen Welt würde zu einem breit einsetzbaren Identifikations- und Servicemedium, dessen Nutzung längst nicht mehr auf den Gesundheitsbereich eingeschränkt und nicht mehr nur an die bestehende Karten-Leser-Infrastruktur gebunden ist. Diese neugeschaffene Basis (als Ziel) der digitalen Karte, kombiniert mit dem bestehenden Vertrauen in die Institution „Gesundheitskarte", eröffnet die Nutzung als elektronisches Identifikationsmedium für weitergehende elektronische (e-*) Dienste wie e-Schlüssel, e-Identifikation oder als sichere Kommunikationsplattform, außerhalb des bewusst strikter anzulegenden Sicherheits-Konzeptes einer „harten" e-ID z. B. eines Innenministeriums.

Nicht zuletzt schafft eine profunde und sichere Digitalisierung der Karte in einer Applikation die Basis für eine direkte, nachvollziehbare und sichere Kommunikation zu Eigentümern, Ausstellern, Benutzern oder berechtigten Dienstleistern der Karte, wodurch zahlreiche informelle Anwendungsszenarien straffer und verlässlicher für alle Stakeholder werden.

Das Projekt entwirft u.a. eine umfassende Demonstrator-Applikation für Smartphones, die die Gesundheitskarte auf ein Mobilgerät portiert, unterschiedliche Abläufe dort simuliert und im Alltag testbar (Usability, Trust, IT-Security, Performance) macht. Die mobile Applikation soll technisch die Funktionalitäten der physischen Gesundheitskarte vollständig abbilden und in der Praxis gleichgestellt eingesetzt werden können. Eine fundierte und erweiterbare Systemarchitektur soll eine Integration weiterer Funktionalitäten (Abbildung eines Lichtbilds, digitale Unterschrift) eröffnen und in späterer Folge die App für neue Einsatzmöglichkeiten im Bereich Identifikation und Services unkompliziert nutzbar machen.

Die Registrierung für die Mobile Gesundheitskarte auf dem Smartphone basiert auf bestehenden Konzepten der Österreichischen und Europäischen Richtlinien, um die Zukunft digitaler Authentifizierungsverfahren vernünftig zu antizipieren. So erlaubt z. B. in einer Übergangsphase das Auslesen des Passfotos aus dem Reisepass die sichere Integration eines Lichtbildes der PatientInnen. Die Applikation nutzt dabei die erprobte technische Infrastruktur der Gesundheitskarte und wird – für die Benutzer vollständig transparent – in diese eingebettet, damit Funktionen wie die GINA-Box oder die Ordinationskarte weiterhin verwendet werden können. Die Umsetzung erfolgt gemäß den Zielen höchster Sicherheitsstandards.

Ein Schwerpunkt liegt auf der Umsetzung einer möglichst intuitiven grafischen Benutzeroberfläche. Die Integration von Zusatzfunktionen und Services soll die Applikation attraktiv für BenutzerInnen machen und somit die Akzeptanz bei einer möglichen Markteinführung eines weiterentwickelten Produkts steigern. Bestehende Services werden durch die App einfacher zugänglich, transparenter und nachvollziehbarer. Die Berücksichtigung bestimmter Zielgruppen und ihrer Interessen wird durch Zusatzfunktionen gefördert.



Die Applikation für Patientinnen

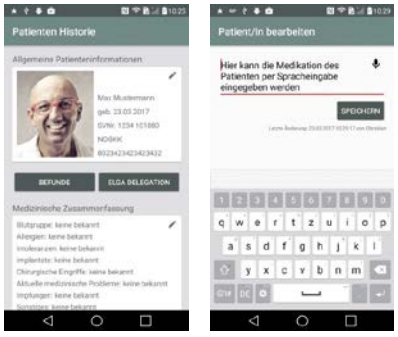
Funktionalitäten der Applikation für PatientInnen:

- Einfache Installation und Aktivierung auf dem Smartphone
- Gesundheitskarte samt Zusatzfunktionen immer am Smartphone dabei
- Verwendung eines verifizierten Lichtbildes in der App als Identitätsnachweis
- Nutzerfreundliches Interface
- Digitale Kommunikation: Erinnerungen an Arzttermine, Impfungen, Arztkontakte u.v.m.
- Notizzettel sicher verwahrt und in der Applikation integriert
- Zusätzliche relevante Information wie z. B. Nachtapotheken

Funktionalitäten der Applikation für ÄrztInnen:

- Unkomplizierte Anmeldung der PatientInnen in der Ordination
- Identitätsnachweis der PatientInnen mittels verifiziertem Lichtbild
- Nahtloser Informations- und Datenaustausch zwischen Patienten- und Ärzte-Applikation auch außerhalb der Ordination
- Verwaltung der Patientendaten
- ELGA-Delegation an Gesundheitsdiensteanbieter
- Dokumentierte digitale Unterschrift von Arztbriefen und anderen Dokumenten
- Diktieren von Texten mittels App
- Sichere Kommunikation mit den PatientInnen

Die Applikation für ÄrztInnen



Das Projekt Mobile eCard erforscht ebenso, welche Auswirkungen eine Digitalisierung auf BürgerInnen hat und welche Aspekte von diesen (vertrauenswürdig) angenommen werden. Die Ergebnisse können als Basis für weitere strategische Entscheidungen bzw. mögliche technische Innovationen und deren sozio-politische Bewertung herangezogen werden. Im Kontext eines immer stärker etablierten e- und m-Governments in Europa kann das Projekt einen wichtigen Beitrag leisten, um im Gesundheitswesen die Digitalisierung noch stärker voranzutreiben und realistische Zukunftsszenarien, u.a. mit folgenden Auswirkungen, zu zeichnen:

- Weitere Reduzierung von Papier und Administration im Gesundheitswesen
- Steigerung der Verwendung elektronischer Services aller Beteiligten; mehr e-Government im Gesundheitswesen
- Mehr automatisierte Prozesse können durch Freigabe von Versicherten oder Gesundheitsdiensteanbietern jederzeit gestartet oder fortgeführt werden
- Bessere Kontrolle über Gesundheitsdaten für PatientInnen
- Anbindung von Diensten privater Anbieter über sichere Schnittstellen, um BenutzerInnen maßgeschneiderte Services zu bieten.

Projektleitung
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH

Projektpartner
- Donau Universität Krems, Zentrum für E-Governance
- Österreichische Staatsdruckerei
- Österreichische Ärztekammer

Kontakt
Dipl.-Ing. Lei Zhu
Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH
Concorde Business Park F, 2320 Schwechat
Tel.: +43 1 9049007-0
E-Mail: lei.zhu@rise-world.com
www.rise-world.com

MODENTITY

Smartphone-basierte hochmobile Dokumenten- und Identitätsverifikation für die Personenkontrolle der Zukunft

Ein Drittel der österreichischen Bevölkerung fühlt sich im Falle nicht ausreichend gesicherter Grenzen bedroht. Dies macht deutlich, dass Grenz- und Personenkontrollen entscheidend für das Sicherheitsgefühl der Bevölkerung sind. Der Erfolg der Bundespolizeibehörden und anderer Einsatzkräfte (first responder) geht mit der stetigen Verbesserung der Methoden zur Dokumenten- und Identitätsverifikation einher. Besonders eine objektive und rasche Dokumentenverifikation, sowie Identifizierungsmöglichkeiten durch biometrische Merkmale stellen einen hohen Mehrwert zur Fahndung nach Personen, zur Bekämpfung und Vermeidung von illegaler Einwanderung, illegalem Aufenthalt und damit verbundener Kriminalität und Terrorismus dar. Ziel des Projektes Modentity war daher eine weitere Verbesserung der Dokumenten- und Identitätsverifikation für die Personenkontrolle der Zukunft. Als Plattform wurden Smartphones mit Android-Betriebssystem gewählt, wodurch eine hohe Leistung bei geringen Anschaffungskosten gewährleistet ist.

Einsatzszenarien

- Zug
- Schiff
- Schwerpunktkontrollen Autobahn
- Polizeiarbeit, Personenfahndung
- Vorfeldkontrollen Flughafen

Modulares Konzept

- Einfache Erweiterbarkeit durch ein Modulsystem
- Die Core-App dient als User-Interface und Datenzentrale
- Die eigentliche Datenerfassung ist über Module implementiert
- Zusätzliche Funktionen können auf einfache Weise integriert werden (z. B. Nummerntafel-Erkennung, Anbindung zusätzlicher Datenbanken etc.)

Datenbank-Abfrage

- Mit den eingelesenen Daten können Abfragen diverser Datenbanken getätigt werden, z. B. VIS, SIS2, Ekis, IFA
- Die Abfrage startet automatisch, sobald die erforderlichen Daten verfügbar sind, ohne separate Passworteingabe für jede Datenbank
- Bei Verbindungsabbruch (z. B. Zug im Tunnel) wird die Abfrage automatisch weitergeführt, sobald die Verbindung wieder verfügbar ist

Pass Einlesen

Dieses Modul kann die Information der Maschinenlesbaren Zone (MRZ) mithilfe der eingebauten Kamera erfassen und einen Konsistenzcheck mit der Visible Zone (VIZ) durchführen, um Manipulationen am Dokument zu erkennen. Außerdem können der Chip des Reisedokuments ausgelesen und die Signaturen auf Echtheit überprüft werden.

Gesichtsvergleich

- Vergleich mittels Face-Matching von Bild im Pass und Live-Bild der Kamera
- Der Algorithmus zeigt eine Ähnlichkeit in Prozent, die endgültige Entscheidung trifft dabei immer der Beamte
- Das Bild aus dem Pass und das Live-Bild werden gleichzeitig angezeigt, mit laufender Bewertung

Modulares Konzept rund um die Core-App

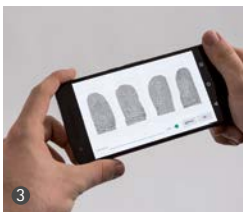
Fingerabdruck-Aufnahme

- Es wurde ein neuartiges kontaktloses Verfahren mittels eingebauter Kamera entwickelt.
- Erlaubt Erfassung aller 10 Finger in 3 Schritten (4 Finger links, 4 Finger rechts, Daumen)
- Zusätzliche Anbindung eines externen Fingerabdruck-Lesegeräts über Bluetooth

Projektleitung
AIT – Austrian Institute of Technology GmbH, Safety & Security Department
Projektpartner
- BM.I – Bundesministerium für Inneres; insbesondere Referate II/2/a und II/2/e.
- Österreichische Staatsdruckerei GmbH
- rubicon IT GmbH
- IFES – Institut für empirische Sozialforschung GmbH
- IFES Feld GmbH

Kontakt
Franz Daubner
AIT – Austrian Institute of Technology GmbH
Safety & Security Department
Donau-City-Straße 1, 1220 Wien
Tel: +43 50550 2800
E-Mail: franz.daubner@ait.ac.at
www.aic.ac.at




❶ Mithilfe der integrierten Kamera wird der Pass optisch eingelesen, Informationen extrahiert und verifiziert
❷ Die NFC-Antenne wird verwendet, um den elektronischen Teil des Passes zu lesen ❸ Aufnahme von Fingerabdrücken mit der Kamera; aus der Aufnahme können die Fingerabdrücke extrahiert werden; Anbindung eines externen Geräts zur Fingerabdruck-Aufnahme

SecuRescue

Echtzeitlageerfassung der örtlichen Situation für Einsatzkräfte bei Katastrophen und Kriseneinsätzen

Bei Katastrophen- und Kriseneinsätzen sowie Einsätzen mit unbekannten Gefahrstoffen sind Einsatzkräfte oftmals großen und nicht vorhersehbaren Gefahren und Risiken ausgesetzt, da bei der Einsatzplanung nur wenige gesicherte Informationen, die aktuelle Lage betreffend, zur Verfügung stehen.

Das Projekt SecuRescue zielt darauf ab, eine Verbesserung der Entscheidungsgrundlage für die Einsatzplanung bei Krisen- und Katastrophenszenarien zu ermöglichen. Eine entscheidende Verbesserung wird durch technologische Unterstützung vor allem durch die Einbeziehung laufend aktueller Erkundungsergebnisse erreicht.

Als wesentlicher Bestandteil werden dazu 3D-Geländedaten eines hochwertigen Laserscanners bzw. Bilder einer neuartigen 3D 360°-Panoramakamera (TUCO-3D) mit Messdaten von Gefahrstoffsensoren (Gas, Radioaktivität etc.) fusioniert. Dabei kommt das Laserscanner-System in Kombination mit einer Gammasonde von einem unbemannten Luftfahrzeug (UAV) aus zum Einsatz. Die TUCO-3D Panoramakamera und ein Gassensor sind auf einem mobilen Roboter montiert. In potentiellen Gefahrensituationen wie z. B. Brand, Austritt von Gefahrstoffen oder Freisetzung von Radioaktivität können das unbemannte Luftfahrzeug (Outdoor) bzw. der Roboter (Indoor) semiautonom und ohne Gefährdung von Menschenleben das Gelände erkunden, um die Erstellung einer interaktiven Lagekarte und Visualisierung auf einem Tablet in sehr kurzer Zeit zu ermöglichen. Die ermittelten Messwerte der Sensoren (Gas- und Schadstoffkonzentrationen, Gamma-Strahlung etc.) werden in Kombination mit den 3D-Daten als Echtzeit-Lagekarte dem Einsatzpersonal zur Verfügung gestellt.

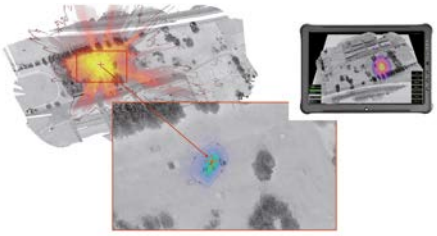
Diese digitale Karte bietet einen schnellen Überblick über die aktuelle Gefahrensituation. Durch die Informationen können Einsatzleiter, Ersthelfer bzw. Spezialisten des jeweiligen Fachgebietes eine bessere Lageeinschätzung vornehmen, bevor sich Einsatzkräfte in den Gefahrenbereich begeben.

Bei den im Projekt durchgeführten Tests konnte erfolgreich gezeigt werden, dass die spezifizierten zeitlichen Echtzeit-Anforderungen – selbst mit dem nicht optimierten Prototypenaufbau – erfüllt werden können und den Einsatzkräften innerhalb kürzester Zeit (< 5 min) ein übersichtliches 3D-Lagebild zur Verfügung gestellt werden kann. Die Echtzeit-Georeferenzierung, -Übertragung und -Auswertung erwiesen sich als überaus schnell und robust. Als sehr präzise erwiesen sich im Outdoor-Feldtest auch die Positionsbestimmung von Gammaquellen und die Vegetationsfilterung (zum Ausblenden von Bewuchs und detaillierterer Erkennung von Terrainstrukturen).

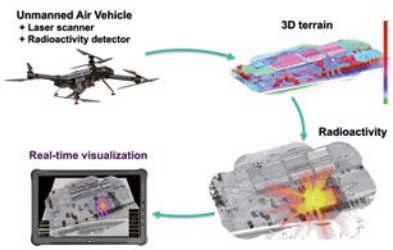
Im Indoor-Szenario ist die Reaktionszeit des Systems im Wesentlichen nur durch die Ansprechgeschwindigkeit der verwendeten Gas-Sensorik beschränkt. Das 360° 3D-Panoramabild hilft in diesem Szenario ebenfalls deutlich bei Navigation und Lageeinschätzung.

Potentielle Endanwender zeigten sich nach Vorstellung des Projekts und der entwickelten Systeme sehr interessiert und bestätigten, dass die im Projekt entwickelten Konzepte ein hohes Umsetzungspotential haben.

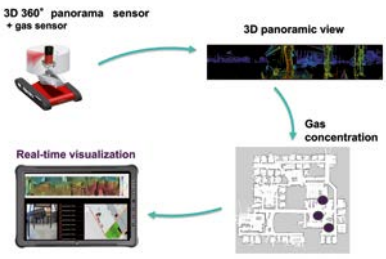
Visualisierung am Einsatztablet für Indoor-Szenario



Verstrahlungsmodel und Quellenposition als Wahrscheinlichkeitsverteilung auf der Geländekarte eingezeichnet. Rechts oben: Visualisierung am Tablett



Übersichtsbild Outdoor-Szenario



Übersichtsbild Indoor-Szenario

Projektleitung
AIT – Austrian Institute of Technology GmbH

Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- TU Wien
- Riegl Research Forschungsgesellschaft
- EYE.AERO GmbH
- Flammpunkt
- CBRN Protection GmbH

Kontakt
DI Michael Hofstätter
AIT – Austrian Institute of Technology GmbH
Safety & Security Department
Donau-City-Straße 1, 1220 Wien
Tel.: + 43 50550 4202
E-Mail: michael.hofstaetter@ait.ac.at

MONITOR

Flexibles echtzeitnahes Multi-Sensor-Monitoring und Kurzfristprognose zur Unterstützung des Sicherheitsmanagements bei Großveranstaltungen

Problemstellung

Der steigende Trend zu geplanten sowie auch zu spontanen Veranstaltungen mit großen Menschenmassen bringt neue Herausforderungen für das zivile Sicherheitsmanagement. Die gezielte und effektive Unterstützung zeitkritischer Entscheidungsprozesse erfordert einerseits die zeitnahe Erstellung eines flächendeckenden Lagebildes und andererseits ein permanentes Monitoring von kritischen Bereichen. Das Projekt MONITOR zielt auf den kombinierten Einsatz von fluggestützten und terrestrischen Aufnahmesystemen sowie eines flexiblen multi-sensoriellen Netzwerks ab, um ein aktuelles und umfassendes Lagebild zu erstellen und damit eine optimierte Einsatzführung zu ermöglichen.

Zielsetzungen

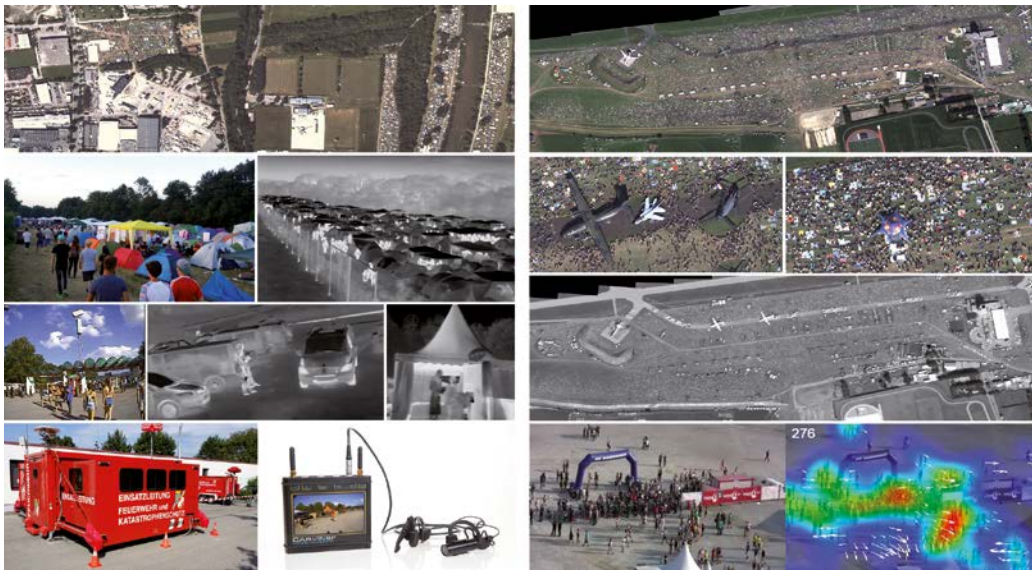
- Entwicklung, Optimierung und Erweiterung eines luftgestützten, multifunktionalen Führungsunterstützungssystems für das Katastrophenmanagement
- Echtzeitnahe, bedarfsorientierte Generierung aktueller Lagebilder und daraus abgeleiteter Informationen
- Methodenentwicklung zur Analyse von Video- und Einzelbildern unterschiedlicher Sensoren und Aufnahmekonfigurationen sowie der Fusion von Multi-Sensor Daten
- Entwicklung innovativer Lösungsansätze für Multi-Sensor Ausstattungsmodule von mobilen „First Responder Teams" und die interaktive Einbindung in die Einsatzzentrale
- Entwicklung von optimierten Simulationsmodellen für Personenströme und Kurzfristprognosen
- Entwicklung von prototypischen Managementmodulen zur Unterstützung des Sicherheitsmanagements, Verbesserung des Situationsbewusstseins und der Interaktion mit mobilen Einheiten.

Der synergetische Einsatz von terrestrischen und fluggestützten Aufnahmesystemen (optisch und thermal) und eines flexiblen Multi-Sensor-Netzwerks aus Mobilfunkdaten, WLAN/Bluetooth-Verortung, Querschnittszählungen, mobilen Video- und Akustiksensoren und „Human Sensors" bietet neue Möglichkeiten für das Sicherheitsmanagement. Eine echtzeitnahe Zusammenführung der Daten mit Verzögerungen bis zu max. einer Minute sowie die Entwicklung von Methoden für eine Analyse multi-sensorieller Daten soll eine flexible und zeitgerechte Verhaltensanalyse der Menschenmassen sowie eine simulationsgestützte Prognose von Personenströmen und somit eine frühzeitige Erkennung kritischer Situationen ermöglichen, wie z. B. überhöhte Menschendichten, Staubildung oder turbulente Personenflüsse. In akuten Krisensituationen können auf dieser Basis gezielte Interventionsmaßnahmen zeitgerecht eingeleitet werden. Die Grunddaten sind derzeit meist jedoch nicht zeitnah bzw. in entsprechender Qualität vorhanden.

Innovative technologische Lösungen im Bereich der multi-sensoriellen Datenakquisition und -vernetzung stellen einen wichtigen Fokus im Projekt dar. Intelligente Managementlösungen ermöglichen eine rollen- und nutzerorientierte Datenaufbereitung und werden dabei auf die Nutzung in mobilen Einsatzständen (Fahrzeugen, Containern, Zelten etc.) optimiert, um mobile Einsatzteams bestmöglich zu unterstützen.

Eine für das Event-Monitoring zugeschnittene Benutzeroberfläche der Simulation ermöglicht es, die Gegebenheiten und die Rahmenbedingungen interaktiv zu verändern, um die Auswirkungen verschiedenster geplanter Sicherheitsmaßnahmen zu überprüfen. Eine Gegenüberstellung der Ergebnisse erleichtert die Entscheidungsfindung für das Sicherheitsmanagement. Die Abbildungen zeigen Beispiele des Einsatzes fluggestützter sowie mobiler Aufnahmesysteme mit RGB- und Thermalkameras im Rahmen von diversen Großveranstaltungen.

Unter starker Einbindung der Bedarfsträger schafft MONITOR eine innovative und leistungsfähige Lagebilderfassung auf Basis umfassender, objektiver und aktueller Daten. Die Ergebnisse der kooperativen Komponentenentwicklung und der Modul- und Systemtests werden zu Projektende evaluiert und die Möglichkeiten zur Weiterentwicklung bis hin zu einer Überführung in ein technisch ausgereiftes modulares und flexibel einsetzbares System erarbeitet. In MONITOR wird auf Entwicklungen der KIRAS-Projekte EN MASSE und EVIVA zurückgegriffen, in welchen bereits themenverwandte wissenschaftliche Vorarbeiten und Untersuchungen durchgeführt wurden. Die realisierten Module wurden bisher in mehreren realen Einsätzen (Landeskatastrophenschutzübung Steiermark 2014; Schutz 2014, Tirol; AIRPOWER 2016, Steiermark) sowie Testsettings (Frequency 2016, Niederösterreich) eingesetzt.



Aufgenommene Bilddaten im Rahmen des Frequency Festivals 2016 und der AIRPOWER 2016

Ein wesentlicher Aspekt ist die internationale Vernetzung des Projekts MONITOR durch die geplante enge Kooperation mit dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) im Rahmen des Projektes VABENE++, wo ähnliche Themen untersucht bzw. technologische Lösungen entwickelt und diese Synergien optimal genutzt werden können. Die Nutzung der Ergebnisse fokussiert auf eine rasche und gezielte Aufnahme sowie Bereitstellung optischer und thermaler Bilder, die echtzeitnahe Lagedarstellung bei Naturkatastrophen sowie eine optimierte Unterstützung von Entscheidungsprozessen im Krisenstab.

Projektleitung
JOANNEUM RESEARCH Forschungsges.mbH

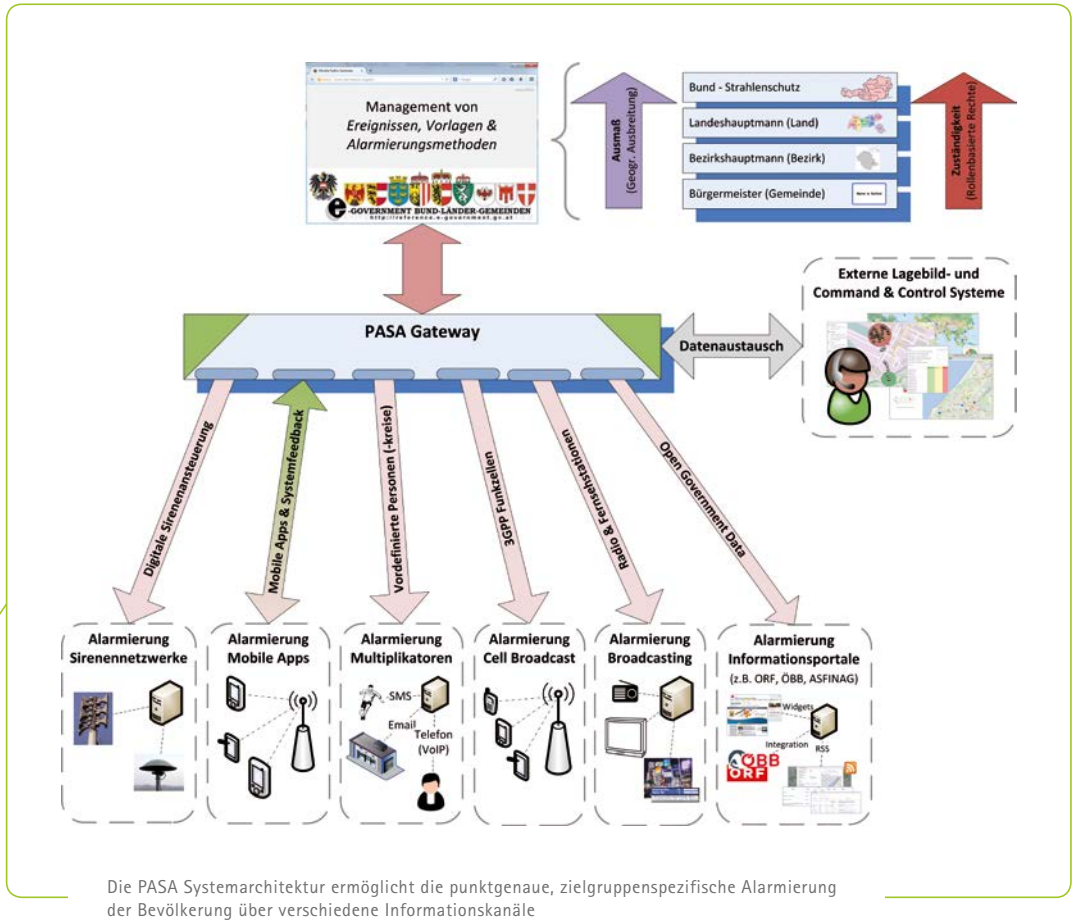
Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Bundesministerium für Landesverteidigung und Sport, Landesverteidigungsakademie
- DI Helmut Schrom-Feiertag, Austrian Institute of Technology GmbH
- DI Mario Schwaiger, Spintower KG
- Ing. Richard Feischl, IFR
- Mag. Herbert Wagner, Wagner Sicherheit GmbH

Kontakt
DI Alexander Almer
JOANNEUM RESEARCH – DIGITAL,
Institut für Informations- und Kommunikationstechnologien
Steyrergasse 17, 8010 Graz
Tel.: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital

PASA – Public Warning and Alert System for Austria

Alarmierungskonzept für Krisen- und Katastrophenereignisse in Österreich

Die Effizienz von Einsatzorganisationen hängt in den meisten Krisen- und Katastrophensituationen stark vom Grad der Mitarbeit oder der Interferenz seitens der Zivilbevölkerung ab, die z. B. helfen kann, Evakuierungsmaßnahmen zügig zu gestalten, sich in kritischen Gefahrensituationen zeitgerecht in die Sicherheit von Gebäuden zu begeben oder wichtige Verkehrsverbindungen zu entlasten. Im aktuellen Ansatz in Österreich erfolgt die Warnung und Alarmierung der Bevölkerung ausschließlich grobgranular über die Sirenen und über den Rundfunk, wohingegen der aktuelle Stand der Technik es ermöglichen würde, die Bevölkerungsgruppen über mehrere Informationskanäle (wie z. B. Mobiltelefone) schnell und mittels georeferenzierter Methoden punktgenau zu erreichen, präzise mit relevanten Informationen zum Geschehen vor Ort zu versorgen und somit deren Zusammenarbeit mit den Einsatzorganisationen im Sinne einer Sicherheits- und Gesamteffizienzsteigerung beträchtlich zu optimieren. Um die Kommunikation der Zivilschutzbehörden mit der Bevölkerung zu verbessern, wird im Projekt PASA in einem interdisziplinären Ansatz ein neuartiges, ganzheitliches Alarmierungs-



Die PASA Systemarchitektur ermöglicht die punktgenaue, zielgruppenspezifische Alarmierung der Bevölkerung über verschiedene Informationskanäle

konzept für Österreich entwickelt. Zu diesem Zweck erhebt PASA die entsprechenden Präferenzen der Bevölkerung sowie der öffentlichen Bedarfsträger, um darauf basierend gezielt soziodemographische, organisatorische und technische Anforderungen zu definieren, die in die Spezifikation einer neuen Alarmierungsarchitektur für Österreich einfließen werden.

Die wichtigsten Bestandteile der neuen Architektur mitsamt der zu untersuchenden Alarmierungskanäle werden in Form eines Proof-of-Concept implementiert und anschließend sowohl mit den Bedarfsträgern als auch mit repräsentativen Gruppen aus der österreichischen Bevölkerung evaluiert, um zu präzisen qualitativen und quantitativen Aussagen zur Reichweite, Akzeptanz und Effizienz des angedachten Lösungsansatzes zu gelangen. Das neue System soll darüber hinaus die komplexe föderale Gesetzeslage in Österreich und die daraus abgeleiteten verschiedenen Zuständigkeiten und Rollen der zuständigen Organe (Gemeinde, Bezirk, Land, Bund) abbilden, wozu das Projekt neben der soziodemographischen und technischen Forschungsarbeit eine laufende Überprüfung der Kompatibilität der angedachten Lösungen mit dem vorgegebenen rechtlichen Rahmen durchführt. Im Sinne einer optimalen Verwertung der Ergebnisse hat das PASA-Projektkonsortium mit den Katastrophenschutzbehörden der österreichischen Bundesländer vereinbart, im Rahmen der gemeinsam seitens des Bundesministeriums für Inneres und der Bundesländer geführten Fachgruppe Technik des Staatlichen Krisen- und Katastrophenschutzmanagements (SKKM) die im Projekt gewonnenen Erkenntnisse laufend in die neuesten Planungen auf Bundes- sowie auf Landesebene einfließen zu lassen. Gleichzeitig sorgt die SKKM-Fachgruppe Technik dafür, dass PASA laufend mit den aktuellsten technischen Anforderungen der wichtigsten öffentlichen Bedarfsträger in Österreich versorgt wird, womit sichergestellt ist, dass die in PASA durchgeführte interdisziplinäre Forschung zu einem optimalen Mehrwert für die gesamte österreichische Gesellschaft führen wird.

Das in PASA entwickelte Alarmierungskonzept ermöglicht es, im Falle eintretender Krisen- und Katastrophenereignisse alle Bevölkerungsgruppen über mehrere Wege (d.h. über mehrere Informationskanäle) schnell und mittels georeferenzierter Methoden punktgenau zu erreichen. Somit wird eine optimale Zusammenarbeit der Bevölkerung mit den Einsatzorganisationen vor Ort ermöglicht, die unmittelbar zu einer signifikanten Steigerung der Gesamteffizienz der Einsatzorganisationen führen wird.

Das Ziel von PASA ist es, in einem mehrstufigen, interdisziplinären Ansatz

1. den Bedarf der österreichischen Bevölkerung und der Behörden in Bezug auf die öffentliche Warnung und Alarmierung zu erheben,
2. basierend auf dieser Informationslage die Anforderungen an eine moderne und zukunftssichere technische Warnungs- und Alarmierungsarchitektur für Österreich zu definieren,
3. die exemplarische Implementierung eines Proof-of-Concept zu erstellen und
4. mittels des Proof-of-Concept die Reichweite, Akzeptanz und Effizienz der angedachten Lösungen mit repräsentativen Gruppen aus der österreichischen Bevölkerung und mit den institutionellen Bedarfsträgern in einem ausgiebigen Feldtest zu verifizieren.

Im Sinne einer möglichst einfachen Verwertbarkeit soll der vorgeschlagene Lösungsansatz dabei die komplexe föderale Gesetzeslage (Gemeinde, Bezirk, Land, Bund) und die daraus abgeleiteten verschiedenen Zuständigkeiten und Rollen der betreffenden Behörden abbilden.

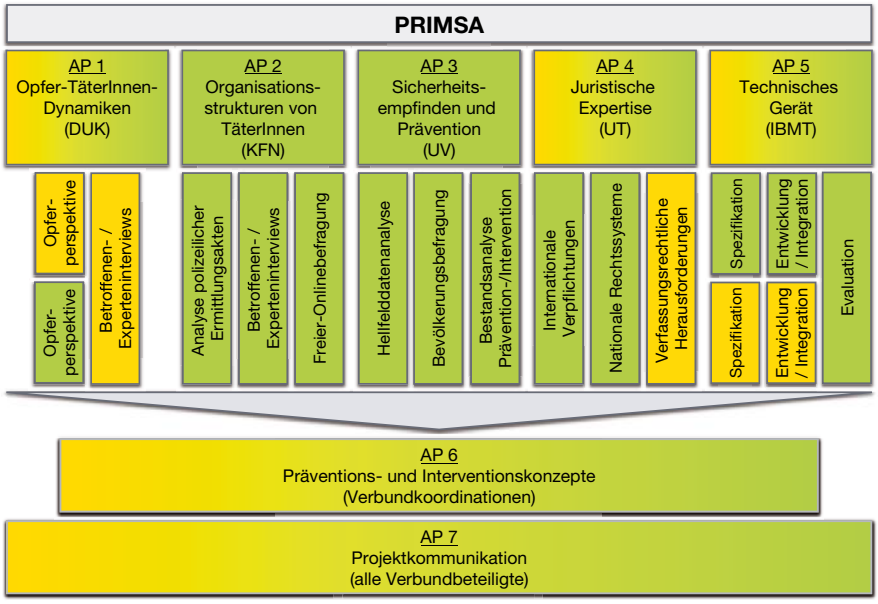
Projektleitung
AIT – Austrian Institute of Technology,
Center Digital Safety & Security

Projektpartner
- Bundesministerium für Inneres
- Universität Wien, Institut für Europarecht, Internationales Recht und Rechtsvergleichung, Abteilung für Völkerrecht und Internationale Beziehungen
- IFES Institut für empirische Sozialforschung GmbH
- IFES Feld GmbH
- JOANNEUM RESEARCH Forschungsgesellschaft mbH
- CPB SOFTWARE (Austria) GmbH
- Rundfunk und Telekom RegulierungsGmbH

Kontakt
Dr. Ivan Gojmerac
AIT – Austrian Institute of Technology GmbH,
Center for Digital Safety & Security
Donau-City-Str. 1, 1220 Wien
Tel.: +43 50550 2826
E-Mail: ivan.gojmerac@ait.ac.at
www.ait.ac.at

PRIMSA

Prävention und Intervention bei Menschenhandel zum Zweck sexueller Ausbeutung: Multidisziplinäre Perspektiven



Aufbau des Projekts PRIMSA

Organisierter Menschenhandel in Form von Zwangsprostitution ist ein global verbreitetes Phänomen und zeigt bei den Opfern gravierende Auswirkungen. In Mitteleuropa sind Deutschland und Österreich bedeutsame Transit- und Zielländer für das Geschehen. Das tatsächliche Ausmaß der Problematik geht Schätzungen zufolge weit über die in den polizeilichen Hellfelddaten dargestellten Dimensionen hinaus. Der Großteil der Betroffenen kann nicht identifiziert werden und wird entsprechend von Hilfsangeboten nicht erreicht. Es bedarf also vielschichtig angelegter, grenzüberschreitender Präventions- und Interventionsstrategien. Das ist insofern erstaunlich, da die UN bereits 2010 einen globalen Aktionsplan zur Bekämpfung des Menschenhandels implementiert hat. Es stellt sich daher die Frage, warum bei einem so eindeutig positionierten Rechtssystem und der Bereitschaft zu nationalen wie internationalen Programmen der Erfolg der Hilfe bisher als so wenig befriedigend bezeichnet werden kann.

Neben den klandestinen Tatstrukturen wird dies bisher vor allem auf die unzureichend ausgebildeten Unterstützungssysteme zurückgeführt, die nicht nur die ökonomisch bedingte Abhängigkeit der Opfer von ihren Zuhältern, sondern auch die komplizierten emotionalen, in der Regel gewaltbelasteten Verstrickungen und emotionalen Bindungen an Personen aus dem Milieu zu sehr außer Acht lassen. Das deutsch-österreichische Forschungsprojekt Prävention und Intervention bei Menschenhandel zum Zweck sexueller Ausbeutung (PRIMSA) widmet sich spezifisch dieser Problemlage. Ziel des Projekts ist, über diesen bilateralen Weg in einem mehrdimensional angelegten Untersuchungsdesign institutionsübergreifend fundierte Präventions- und Interventionsmöglichkeiten zu eruieren und für konkrete Schulungszwecke der beteiligten Berufsgruppen einzusetzen. Das Projekt wird von der Förderrichtlinie „Zivile Sicherheit – Schutz vor organisierter Kriminalität" des deutschen Bundesministeriums für Bildung und Forschung (BMBF) sowie von der österreichischen KIRAS-Ausschreibung 2013 des BMVIT gefördert.

Das Projekt bezieht sowohl technische als auch soziologische, juristische, psychologische, pädagogische und sozialräumliche Perspektiven ein. In sieben unterschiedlichen und transdisziplinär angelegten Arbeitspaketen wird dieser Zielsetzung auf sehr unterschiedliche Weise nachgegangen. An der Donau-Universität Krems werden die zwischenmenschlichen Dynamiken zwischen TäterInnen und Opfern untersucht und es wird der Frage nachgegangen, warum die betroffenen Frauen so schlecht von den helfenden Professionen erreicht werden (Arbeitspaket 1 – AP1). Das Kriminologische Forschungsinstitut Niedersachsen (KFN) geht dem vielschichtigen TäterInnenvorgehen nach (AP2). Durch die Universität Vechta werden themenfeldbezogene Daten zum Deliktaufkommen eruiert und dargestellt sowie bestehende Hilfsangebote von nicht-staatlichen Organisationen evaluiert (AP3), über die Universität Tübingen internationale und nationale Rechtslagen aufgearbeitet (AP4) und vom IBMT Fraunhofer Institut wird ein technisches Gerät zur nicht-invasiven Altersbestimmung der Opfer entwickelt (AP5). Anschließend werden alle Teilergebnisse zu einem Präventions- und Interventionskonzept zusammengefasst, das nicht zuletzt die praktische Arbeit im Feld unterstützen soll (AP6). Das siebte Arbeitspaket dient der Kommunikation innerhalb der verschiedenen PartnerInnen und außerhalb des Projekts zur Publikation der Ergebnisse.

Der österreichische Teil des Projekts – und hier das erste Arbeitspaket – fokussiert zur Aufklärung der oben genannten Widersprüche zwischen Angeboten und Erreichbarkeit der betroffenen Frauen, insbesondere die sexuell ausgebeuteten Frauen selbst. In erster Linie wird der Frage nachgegangen, warum Betroffene häufig nicht in Hilfseinrichtungen ankommen oder gar in die Gewaltverhältnisse zurückkehren und wie diese Lücke im Hilfesystem geschlossen werden kann. Es handelt sich – wie die Soziale Arbeit dies benennt – um eine „hard to reach"-Problematik, um KlientInnen, die sozial schlecht integriert sind und deren Vertrauen in Menschen und Institutionen durch zahlreiche Abbrüche zerstört wurde. Zielsetzung ist, die Passfähigkeit der bestehenden Angebote mit der vorliegenden Problemlage zu verbessern. Es ist nach wie vor z. B. zu wenig darüber bekannt, warum die Unterstützung mal mehr und mal weniger erfolgreich ist. Zur Aufklärung dieser Frage wurde daher in dem adressatInnenorientierten Projekt insbesondere die Perspektive der betroffenen Frauen in das Forschungsvorgehen einbezogen, die in vielen Forschungsprojekten zum Thema Menschenhandel und Gewalt außer Acht gelassen wird, wie die DAPHNE-Forschungsreihe der EU vor einigen Jahren kritisch anmerkte.

Die ersten Ergebnisse des Projekts zeigen: Viele der Frauen werden nicht vom System erreicht und sind massiven Gewalteinflüssen ausgesetzt. Die gesellschaftlichen Bilder über Frauen in Prostitutionsmilieus verstärken diese Auswirkungen und tragen durch die Tabuisierung zusätzlich zur Stigmatisierung und Unglaubwürdigkeit der Opfer bei. Die traumatischen und Ausgrenzungserfahrungen erschweren den sexuell ausgebeuteten Frauen den Zugang zum Hilfesystem. Eine betroffene Frau erklärt treffend: „Ich vertrau' keine (sic!), jede ist gegen mich." Deutlich wird jedoch: Alle beteiligten Fachkräfte können den Hilfeprozess positiv beeinflussen. Von allen befragten betroffenen Frauen wird vertrauensförderndes Verhalten sehr wertschätzend zur Kenntnis genommen. Werden derart positive Erfahrungen – z. B. mit der Polizei oder den Beratungsstellen – möglich, so kann dies große Erfolge hervorbringen. Dafür benötigt es kompetente Fachkräfte mit Wissens- und Kompetenzbeständen aus dem Bereich Trauma, Bindung und Vertrauensanbahnung. Dies gilt für alle am Hilfeprozess beteiligten Fachkräfte aus der Beratungsarbeit, aber auch aus dem Polizei- sowie dem Rechtswesen. Entsprechend werden im Rahmen des Projekts momentan entsprechende Schulungsreihen für beratende SozialarbeiterInnen, Polizeikräfte und RechtsvertreterInnen entwickelt und in verschieden Aus- und Fortbildungszusammenhänge implementiert.

Projektleitung Österreich
Donau-Universität Krems, Department für Psychotherapie und Biopsychosoziale Gesundheit

Projektpartner Österreich
- Bundesministerium für Inneres (.BK und Sicherheitsakademie SIAK)
- Research Institute AG & Co KG – Zentrum für digitale Menschenrechte
- AKAtech Produktions- und Handels GmbH

Projektleitung Deutschland
Universität Vechta, Institut für Soziale Arbeit, Bildungs- und Sportwissenschaften

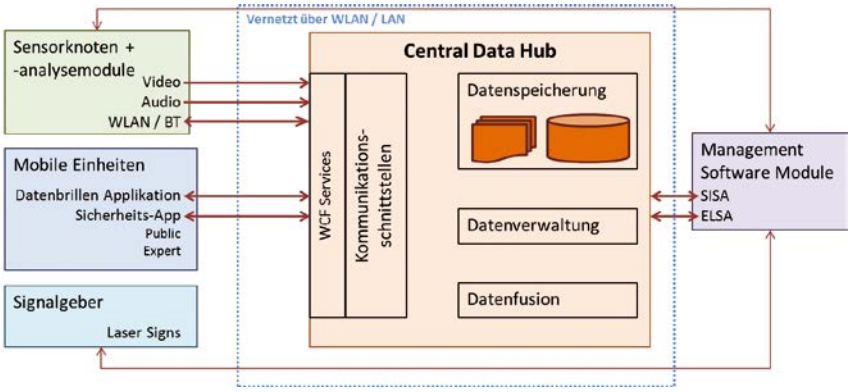
Projektpartner Deutschland
- Fraunhofer Institut für Biomedizinische Technik, St. Ingbert
- Kriminologisches Institut Niedersachsen e.V., Hannover
- Universität des Saarlandes, Saarbrücken
- Universität Tübingen, Juristische Fakultät

Kontakt
Dr. Katharina Gerlich
Donau-Universität Krems
Department für Psychotherapie und Biopsychosoziale Gesundheit
Dr. Karl Dorrek Straße 30, 3500 Krems
Tel: +43 2732 893 2531
E-Mail: katharina.gerlich@donau-uni.ac.at
www.donau-uni.ac.at/psymed

SecureFlex

Optimierung der Gebäudesicherheit durch flexible, multisensorale Module und szenarienoptimierte Interventionsstrategien

Das System ergänzt bestehende Sicherheitssysteme in und um Gebäuden kritischer Infrastruktur und Veranstaltungszentren um flexible, hybride Multisensornetze für eine gebündelte, echtzeitnahe Situationsdarstellung. Unterschiedliche Sensorsysteme liefern Daten in ein zentrales System, das die Daten verdichtet und in ein übersichtliches, aktuelles Lagebild transformiert. Die Kommunikation zwischen Besuchern, Veranstaltern, Sicherheitspersonal und Einsatzkräften wird über das System abgewickelt. Damit wird die Sicherheit vor allem in Notfällen erhöht und das effiziente Zusammenwirken unterstützt. Dabei wurden auch gesellschaftliche und soziale Aspekte sowie das Thema Datenschutz bearbeitet. Anregungen für eine kommerzielle Verwertung runden die Ergebnisse ab.

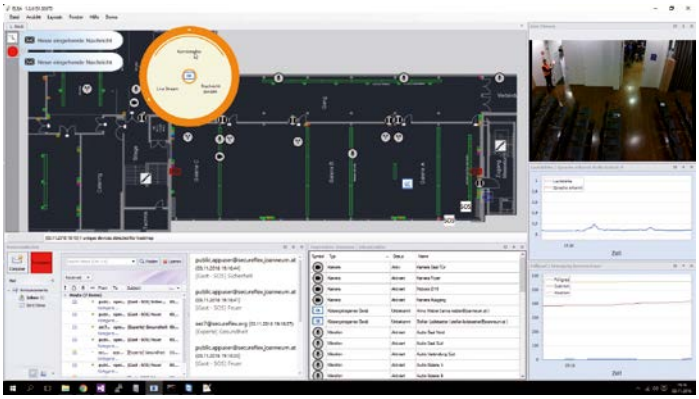


Systemübersicht

Nach der Definition der nötigen Anforderungsspezifikationen, die zielgerichtet auf das Anwendungsszenario bei Großveranstaltungen abgestimmt wurden, wurden auf technischer Ebene folgende Sensoren entwickelt und erprobt:

- BLIDS-Sensoren (kombinierter Bluetooth und WiFi Sensor) zur verorteten Personendichtemessung
- Mobile Videosensoren zur Ermittlung von Personenbewegungen im überwachten Bereich sowie zur Personenzählung
- Audiosensoren zur Erkennung von Schallereignissen sowie zur Abschätzung von Personenmengen
- iBeacon-Sensoren zur Standortberechnung von Personen und indoor Navigation

Die Sensoren sind flexibel und mobil einsetzbar, verfügen über autonome Energieversorgung (mindestens für einen bestimmten Zeitraum) und können über mobile Kommunikationstechnologien autark untereinander bzw. mit dem Leitstandsystem kommunizieren.



ELSA Leitstand-Applikation

Sämtliche Daten dieser Sensoren wurden in einem Central Data Hub (CDH) konsolidiert und über ein zentrales Leitstellensystem (ELSA) dargestellt.

Damit konnten übergreifende Informationen zu Lagebild und Status von Notfallaktivitäten, Standorte von Besucherströmen und Einsatzkräften sowie Statusinformationen zu bestimmten Cases im Szenario übersichtlich dargestellt werden.

Die Kommunikation zwischen Besuchern, Sicherheitspersonal und Einsatzkräften erfolgt ebenfalls über ELSA, wird dort gebündelt und entsprechend gesteuert und verteilt. Als Benutzerschnittstelle für Besucher und Einsatzkräfte wurde eine mobile Applikation sowie eine Anwendung für eine Datenbrille entwickelt, die aktuelle Lageinformationen, Navigation mit Anweisung (z. B. empfohlener Evakuationsweg) sowie die Möglichkeit von Notfallmeldungen (z. B. Anforderung von Rettungskräften) mit einer Kategorisierung des Notfalls sowie Standortinformationen des Vorfalls bietet. Einsatzkräfte können von der Leitstelle mit diesen Informationen gezielt versorgt und zum Einsatzort navigiert werden.

Mobile Applikation (li.) und Datenbrille (re.)

Dynamisch steuerbare Laserkennzeichnungssysteme für die Fluchtwegkennzeichnungen wurden ebenfalls entwickelt und in das ELSA-System integriert. Damit wird die Sichtbarkeit der Kennzeichnungen (z. B. bei Verrauchung) erhöht und die Kennzeichnung kann an die aktuelle Situation angepasst werden. Etwa kann, wenn ein Fluchtweg unpassierbar wird, die Leitstelle auf den Boden oder die Wand projizierte Fluchtwegsymbole auf „gesperrt" umstellen und Richtungsinformationen zur Benutzung alternativer Wege anzeigen.

Durch die Architektur des Systems ist sichergestellt, dass über standardisierte Schnittstellen weitere, zukünftige Sensoren und/oder bereits bestehende Sicherheitssysteme leicht integriert werden können.

Sämtliche Komponenten sowie das vernetzte Gesamtsystem wurden in 2 Feldtests und einer abschließenden Demonstrator-Veranstaltung unter Realbedingungen getestet und erprobt, wobei das System in bestehende Notfallabläufe integriert wurde.

Gesellschaftliche bzw. soziale Aspekte derartiger Systeme wurden erhoben und analysiert. Ebenso wurden unter Berücksichtigung der kommenden EU Datenschutz-Grundverordnung (DSGVO) Datenschutzaspekte und Empfehlungen für die Verwendung des Systems erarbeitet.

Laserkennzeichnung der Fluchtwegsymbole

Für die weitere Entwicklung und den Einsatz in einem kommerziellen Betrieb wurden eine Betrachtung von möglichen Geschäftsmodellen durchgeführt und eine Empfehlung ausgearbeitet.

Insgesamt hat sich gezeigt, dass die Vorteile derartiger Systeme die Sicherheit durchaus heben, allerdings immer noch technische Einschränkungen bzw. Hemmnisse in der Usability bestehen. Dazu zählen die relative Ungenauigkeit und Latenz der indoor-Navigation, die Handhabung von Endgeräten und Applikationen unter Einsatzbedingungen sowie die Latenzzeiten zwischen Ereignissen und den gewünschten Reaktionen. In diesem Bereich ist weitere Forschungs- und Entwicklungsarbeit nötig, damit sich solche Systeme auch am Markt durchsetzen können.

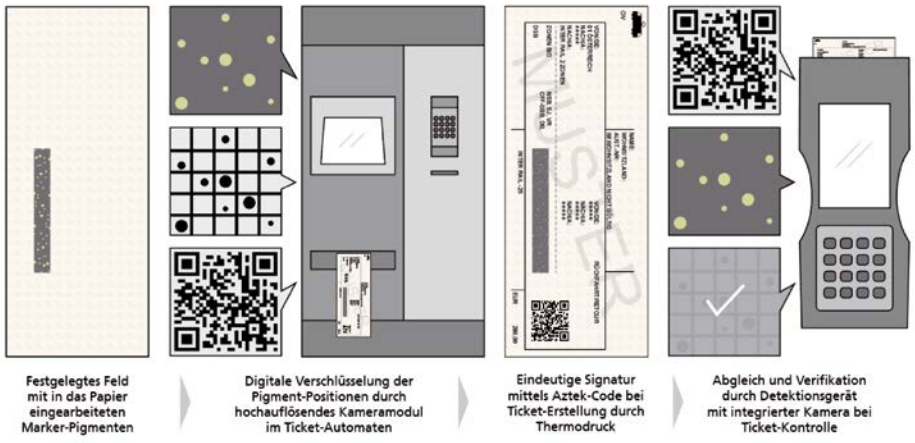
Projektleitung
bit media e-Solutions GmbH

Projektpartner
- Unternehmensberatung bit consulting GmbH
- Joanneum Research Forschungsgesellschaft
- c.c.com GmbH
- Ing. Richard Ferschl, IFR
- Fire Protection Pulker GmbH
- Institut für empirische Sozialforschung GmbH
- Messe Congress Graz Betriebsgesellschaft m.b.H.
- Berufsfeuerwehr Graz
- Externer Datenschutzexperte Dr.iur Ing Eike Wolf

Kontakt
DI Horst Ortmann, MBA
Unternehmensberatung bit consulting GmbH
Kaerntnerstrasse 311, 8054 Graz
Tel.: +43 316 28 55 50 - 0
E-Mail: hortmann@bitonline.com
www.bitonline.com; www.bitmedia.cc

SecureStamp

Fälschungssichere Tickets durch Marker-Pigmente



Darstellung des SecureStamp-Prinzips: Ticket mit Marker-Pigmenten

Die Fälschung von Tickets für den öffentlichen Verkehr oder Veranstaltungen verursacht erheblichen wirtschaftlichen Schaden. Bei der Zugangskontrolle stellen gefälschte Eintrittskarten ein erhebliches Sicherheitsrisiko dar. Tickethersteller integrieren daher Sicherheitsmerkmale wie etwa Kopierschutzfarben, Hologramme oder Diffraktionsfolien in Ticket-Papiere, um sie vor Fälschungen zu schützen. Gelangt allerdings das Original Ticket-Papier in Besitz von Kriminellen, genügt ein einfacher Thermodrucker, um Tickets mit einem hohen Gegenwert zu fälschen. International agierende Fälscherbanden haben sich daher verstärkt auf den Diebstahl von Originalpapier verlegt:

- 6,7 Millionen Euro Schaden durch Reparaturen von aufgebrochenen Automaten alleine bei der Deutschen Bahn AG im Jahr 2014 (Handelsblatt Nr. 29, 11.02.2015).

Optisches Sicherheitsmerkmal digital verschlüsselt

Die JOANNEUM RESEARCH Forschungsgesellschaft hat gemeinsam mit dem deutschen Fraunhofer IPM und Industriepartnern ein Konzept entwickelt, das Fälschungen auf Originalpapier unmöglich macht. Als Sicherheitsmerkmal werden in das Papier eingearbeitete Marker-Pigmente genutzt. Deren stochastische Verteilung ist nicht reproduzierbar und bildet damit einen „Fingerabdruck" des Tickets, der später zur Echtheitsprüfung genutzt wird. Die Verteilung der Pigmente auf einem definierten Bereich des Papiers wird unmittelbar vor dem Ausstellen des Tickets im Automaten mit einer Kamera erfasst und mithilfe eines Verschlüsselungsalgorithmus codiert. Diese codierte Information wird anschließend zusammen mit der zu druckenden Ticketinformation in Form eines Barcodes direkt auf das Ticket gedruckt. Damit entsteht eine eindeutige Signatur im Moment der Ticketerstellung. Bei der Ticketkontrolle erfasst ein Detektionsgerät mit integrierter Kamera erneut die Verteilung der Marker im definierten Papierbereich. Stimmt diese mit der im Code gespeicherten Verteilung überein, ist das Ticket gültig. Für die Verifikation ist keine Datenbankanbindung notwendig. Wird der Barcode auf gestohlenes Originalpapier kopiert, so stimmen Partikelverteilung von Papier und Code nicht überein. Eine ebenfalls mögliche Speicherung der Daten in einer zentralen Datenbank ermöglicht darüber hinaus eine weiter gehende Verwendung der Daten – beispielsweise im Rahmen forensischer Untersuchungen.

Sensor misst Position und Abklingzeit der Pigmente

Zur Markierung des Originalpapiers werden Marker-Pigmente verwendet, die bei Anregung mit Infrarot-Licht lumineszieren. Unmittelbar vor dem Druck eines Tickets werden die Pigmente mittels einer leistungsstarken LED-Ringleuchte bei 980 nm angeregt. Eine in den Fahrkartenautomaten integrierte hochauflösende Kamera erfasst die Position der Pigmente in einem definierten Flächenbereich von zirka 4 x 6 mm mit einer optischen Auflösung von 20 µm. Die anschließende Berechnung der Pigment-Koordination mittels eines speziellen Algorithmus erfolgt bei zirka 8000 Pigmenten in weniger als 250 ms. Zusätzlich zur Verteilung misst das Kamerasystem die Abklingzeit der Pigmente – ein weiteres Merkmal, um für die spätere Authentifizierung einen hohen Fälschungsschutz zu garantieren.

Das kompakte optische Sensorsystem verfügt über eine leistungsstarke Beleuchtungs- und Detektionsoptik und mechanische Schnittstellen für unterschiedliche Automatensysteme.

Robuste Identifikation

Für die Verifikation des Tickets wurde ein handgehaltenes Gerät entwickelt, das technisch dem stationären Auswertemodul möglichst ähnlich ist. Ein Modell der Pigmentverteilung wird wie bei der Ticket-Kodierung mittels einer Kamera detektiert und in komprimierter und verschlüsselter Form im Aztec-Code gespeichert. Der Abgleich des aufgenommenen Musters mit dem im Aztec-Code encodierten Referenzmodell erfolgt mithilfe eines speziell entwickelten Algorithmus, welcher auf der Registrierung von 2D-Punktwolken und Kombination verschiedener Kostenfunktionen für den Abgleich der Modelle basiert. Dabei wird die Partikelverteilung trotz Versatz, Verzerrung oder Abrieb der detektierten Fläche zuverlässig erkannt.

Trotz zunehmender Verbreitung digitaler Tickets werden Papier-Tickets auch auf mittlere Sicht eine wichtige Rolle im Ticketing spielen. Dies gilt für Transport- und Veranstaltungstickets, wo Fälschungen hohe Verluste verursachen, aber auch für sicherheitsrelevante Einmalausweise, etwa für die Zutrittskontrolle.

Links der mobile Systemdemonstrator, rechts die im Automaten verbaute stationäre Einheit

Projektleitung
JOANNEUM RESEARCH Forschungsges.mbH

Projektpartner
- Binder Consulting GmbH
- charismaTec OG
- e-commerce monitoring GmbH
- Holding Graz Linien Kommunale Dienstleistungen GmbH
- Fraunhofer IPM
- Scheidt & Bachmann GmbH
- Diagramm Halbach GmbH & Co KG
- Karlsruher Institut für Technologie (KIT)
- Bundespolizeidirektion München

Assoziierte Partner
- Leuchtstoffwerk Breitungen GmbH
- LINZ AG Linien

Kontakt
DI Andreas Tschepp
JOANNEUM RESEARCH Forschungsges.mbH
Franz-Pichler-Strasse 30, 8160 Weiz
Tel.: +43 316 876 3120
E-Mail: andreas.tschepp@joanneum.at
www.joanneum.at/materials/

SKIN

Schutz der Außenhaut kritischer Infrastrukturen

Ziel des Projekts SKIN ist es, den Schutz der Außenhaut kritischer Gebäude mittels eines intelligenten wissensbasierten Ereigniserkennungssystems mit multimodaler Sensor- und Informationstechnologie zu erhöhen.

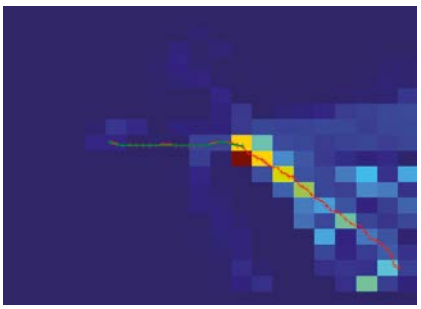
Der Schutz von Fassaden, Dächern und anderen Teilen der Außenhaut von Gebäuden und Denkmälern stellt immer höhere Anforderungen an Behörden und Organisationen mit öffentlichen Sicherheitsaufgaben. Reale Bedrohungsszenarien, wie Terrorangriffe oder gezielte Beschädigung von Kulturgütern, fordern immer zuverlässigere Sicherheitssysteme.

Technisch gesehen haben in jüngster Zeit neue Entwicklungen das Portfolio an für sicherheitstechnische Anwendungen einsetzbaren Sensoriken erweitert.

Gemäß des Projektziels, nämlich der wesentlichen Erhöhung des Schutzes der Außenhaut gefährdeter Gebäude, sollen mittels wissensbasierter Technologien antizipierte oder beobachtete kontext-bedingte Umstände wie Wetter oder Ereignisse in und um das Gebäude berücksichtigt werden, um aus dem Datenbestand mittels Automated Reasoning und Information Fusion Methoden umfassendere Gefahreneinschätzungen abzuleiten. Eine wesentliche Rolle spielt dabei die Fusion der Daten über die Zeit, um aus in der Vergangenheit aufgetretenen Mustern auf die Relevanz aktueller Daten schließen zu können.

Ein besonderes Augenmerk liegt auf der optimal übersichtlichen Präsentation der aktuellen Lage an die Operatoren sowie der effektiven Bedienung, was im engen Zusammenhang mit der GSK-Begleitung steht.

Für eine flächige Überwachung von Fassaden eignen sich besonders Flächensensoren, wie sie in Videokameras bzw.



Originalbild der Wärmebildkamera

Vorhersage der weiteren Objektbewegung durch Neuronales Netzwerk nach Vorgabe der grünen Linie

Bildaufnahmesensoren eingesetzt werden. Mit alternativen Technologien wie Fächerlasern, Ultraschall oder Radar ist es nur mit erheblichem Aufwand möglich, eine vergleichbare Abdeckung zu bewerkstelligen. Bei den Videokameras ist zwischen Kameras für den sichtbaren bis nahen Infrarotbereich (380 – 780 nm Wellenlänge) und so genannten Wärmebildkameras (8 – 15 µm Wellenlänge) zu unterscheiden.

Die genannten optischen Kameras benötigen Lichtquellen, die in diesem Bereich strahlen. Während des Tages übernimmt dies die Sonne, doch in der Dämmerung und bei Nacht muss mit Kunstlicht im sichtbaren oder im Infrarotbereich gearbeitet werden.

Darüber hinaus sind neue Technologien wie „Time-of-Flight"-Sensoren als zusätzliche Informationsquellen durch die dritte Raumdimension für Hochsicherheitsanwendungen in Betracht zu ziehen. Die Eignung speziell im Außenbereich muss dabei in Bezug auf Störlicht-Einflüsse und Witterung noch näher analysiert werden.

Die anfallenden großen Datenmengen sollen auch nachträglich auswertbar sein. Damit können Ereignisse im Videoarchiv gesucht werden, ohne die einzelnen Videos sichten und bei der Aufnahme die Kriterien einer späteren Suche schon festlegen zu müssen, wobei es hierbei datenschutzrechtliche Anforderungen (z. B. Löschungspflichten) entsprechend zu berücksichtigen gilt. Das System soll so ausgelegt sein, dass Datenschutz in das Design eingebaut ist und alle erforderlichen Vorgaben in diesem Bereich bei hoher Funktionalität erfüllt werden.

Im Rahmen der GSK-Begleitforschung werden zentrale datenschutzrechtliche Problemstellungen bzw. Anforderungen im Zusammenhang mit intelligenten wissensbasierten Videoüberwachungssystemen anhand eines konkreten Anwendungsszenarios diskutiert. Der Schwerpunkt der GSK-Komponente liegt jedoch in der organisationsethnografischen Untersuchung operativer Arbeitsabläufe in der Sicherheitszentrale eines am Projekt beteiligten Bedarfsträgers. Hierbei stellen sich insbesondere Fragen nach möglichen Implikationen des Einsatzes neuer Technologien in Hinblick auf eingespielte Arbeitsroutinen in der Gebäudeüberwachung. Dies soll auch Aufschluss über Akzeptanz, Bedarf und Wirksamkeit derartiger Überwachungstechnologien für die Endanwender liefern.

Projektleitung
PKE Electronics AG

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Software Competence Center Hagenberg GmbH (SCCH)
- Vienna Centre for Societal Security (VICESSE)

Kontakt
DI Werner Kloihofer
PKE Electronics AG
Forschung & Entwicklung, Research & Development
Computerstraße 6, 1100 Wien
w.kloihofer@pke.at
www.pke.at

SmartScout

Sensor-basierte Führungsunterstützung bei Einsatzszenarien im Bereich der Öffentlichen Sicherheit

Einsatzanalyse Großveranstaltungen – Nightrace Schladming 2017

Im Rahmen des Projekts SmartScout wird ein auf beweglichen und festen Sensorplattformen bestehendes intelligentes Sensornetzwerk für Überwachungsaufgaben der öffentlichen Sicherheit erarbeitet. Das Besondere an SmartScout ist die intelligente Aufbereitung und integrierte Weiterverarbeitung der erfassten Daten.

Die im Bereich der Öffentlichen Sicherheit tätigen Organisationen sind in zunehmendem Maße mit der Entwicklung konfrontiert, dass sich ihr Einsatzspektrum sowohl in Bezug auf Zuständigkeiten als auch in Bezug auf die Intensität von Einsätzen massiv erweitert. Der gesamte Bereich der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) steht zurzeit vor massiven Herausforderungen. Diese sind u.a. das Management von Großveranstaltungen, der Einsatz in exponierten geographischen Lagen wie beispielsweise dem alpinen Raum oder die Bewältigung von Flüchtlingsströmen und die damit einhergehende Thematik der Grenzsicherung. Zur effektiven und effizienten Bewältigung der vorgenannten Szenarien stellen IKT-basierte Informationsservices, welche einen schnellen Überblick über die aktuelle Lage des Einsatzgeschehens geben, eine unabdingbare Kernkomponente dar. Dazu tragen unter anderem Luftaufnahmen (Fotos, Videos) sowie die Interpretation unterschiedlichster Sensordaten bei. Die zeitnahe Auswertung dieser Daten zur Gewinnung einsatzrelevanter Informationen ist für die handelnden Organisationen eine große Herausforderung. Durch die für sie notwendige Berücksichtigung von Aspekten wie des konkreten Einsatzszenarios, der Einsatztaktik, rechtlicher Rahmenbedingungen und vielen anderen mehr sehen sich die Anwender von Unterstützungstechnologien einer komplexen Aufgabe gegenüber.

Der im Projekt SmartScout im Focus stehende Systemverbund aus statischer oder mobiler Plattform, Sensorik, Schnittstellen zur Steuerung, Datenanalyse, Datenaufbereitung und Visualisierung bietet eine Vielzahl unterschiedlicher Möglichkeiten, um durch schnelleres und sicheres Agieren zum Einsatzerfolg beizutragen. Aktuell gibt es viele technische Ansätze in unterschiedlichen Reifegraden, welche vorwiegend die Lösung von Teilaspekten dieser Aufgaben zum Ziel haben. Ein gesamtheitlicher, nachhaltig in bestehende IT-Landschaften integrierbarer und die speziellen Anforderungen der am Projekt teilnehmenden Bedarfsträger berücksichtigender Ansatz fehlt jedoch. Ziel dieses Projekts ist daher die Erarbeitung eines solchen abgestimmten Ansatzes, bei dem der Aspekt der Skalierung sowohl in ökonomischer als auch technischer Sicht berücksichtigt wird. Neben dem Gesamtsystemdesign ist in SmartScout zur Bearbeitung der geplanten Szenarien sowohl Entwicklungsarbeit an der mobilen Trägerplattform (uLFZ) und dem Flugplanungsmodul erforderlich als auch am zur Anwendung vorgesehenen Sensorium. Daneben bedeuten die automatische Verarbeitung und Auswertung von Bilddaten in einem verteilten Systemverbund eine große Herausforderung. Hinzu kommen die notwendige Einbindung von räumlichen Daten und Modellen, die Verortung von Sensorinformationen und mobiler Trägerplattform sowie die bedarfsgerechte Visualisierung von Informationen und Analyseergebnissen sowohl direkt im Einsatzraum als auch in Leitständen und Zentralen. Zusätzlich stellen rechtliche Rahmenbedingungen einen großen und wichtigen Aspekt im Hinblick auf die Problemstellung von SmartScout dar. Das Projektvorhaben tangiert unterschiedlichste Rechtsmaterien. Durch eine fundierte rechtliche Projektbegleitung werden der jeweilig aktuelle Stand, zukünftige Entwicklungen sowie Potentiale für Änderungen bzw. Anpassungen im Projekt berücksichtigt.

Einsatzanalyse Grenzsicherung – Grenzübergang Spielfeld

Projektleitung
TU Graz, Institut für Maschinenbau- und Betriebsinformatik

Projektpartner
- Bundesministerium für Inneres
- Technische Universität Graz – Institut für Geodäsie, AG Fernerkundung und Photogrammetrie
- Universität Linz, Institute of Public International Law, Air Law and International Relations
- EYE.AERO gmbh
- TeleConsult Austria GmbH
- JOANNEUM RESEARCH GmbH

Kontakt
Prof. Siegfried Vössner
Technische Universität Graz
Kopernikusgasse 24, 8010 Graz
Tel: +43 316 873 8001
E-Mail: voessner@tugraz.at
www.mbi.tugraz.at

VIDRO

Virtueller Drogenhandel – Eine neue Herausforderung bei der Bekämpfung Organisierter Kriminalität

Obwohl der Verkauf und Kauf von psychoaktiven Substanzen mit den Ursprüngen des Internet einhergeht, hat sich seit einer halben Dekade das Phänomen der Kryptomärkte etabliert. Auf diesen Marktplätzen, die ähnlich aufgebaut sind wie weitläufig bekannte Online-HändlerInnenportale, bieten HändlerInnen unter anderem illegale Drogen zum Verkauf an. KundInnen entscheiden auf der Basis von Angaben der HändlerInnen und Kundenbewertungen, bei wem sie welches Produkt in welcher Menge und aus welchem Land bestellen wollen. Während die Transaktionen mit virtuellen Währungen wie Bitcoin abgewickelt werden, erfolgt die Zustellung selber durch reguläre Lieferdienste, die den Inhalt der Sendungen nicht kennen. Das Novum daran: Die physische Identität und der Standort der NutzerInnen dieser Marktplätze werden durch die Nutzung von Anonymisierungssoftware verschleiert. Kryptomärkte ermöglichen somit einen globalen und gleichzeitig anonymen Verkauf und Kauf von illegalen Drogen, 24 Stunden, 7 Tage die Woche. Das erschwert einerseits die Strafermittlung und hat andererseits zahlreiche Implikationen für den Handel selber, denn schließlich werden Transaktionen ohne face-to-face Meetings durchgeführt.

Projektziele von VIDRO

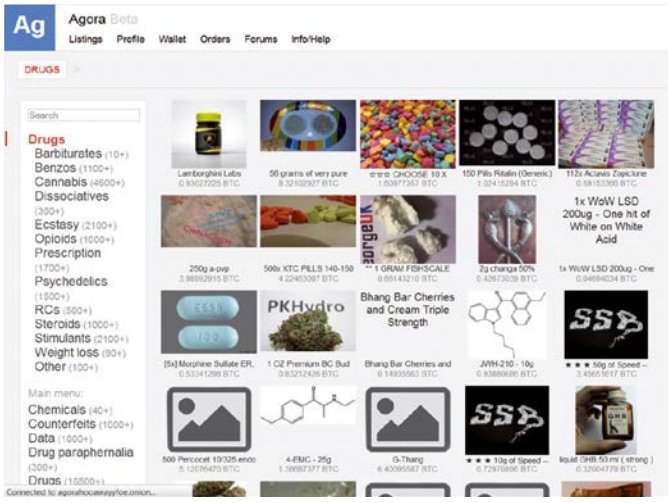
Bei VIDRO handelt es sich um eine der ersten Studien weltweit zu dem Phänomen der Kryptomärkte im Internet. Das Ziel der VIDRO-Studie war die Entwicklung einer automatischen Datengenerierungsapplikation zur systematischen Analyse des Geschehens auf Kryptomärkten. Mithilfe der Analyseapplikation hat das Bundeskriminalamt die Möglichkeit, die Beobachtung der Märkte im Internet zu erweitern und zu optimieren. Diese Studie war Teil einer österreichisch-deutschen Kooperation mit acht Projektpartnern aus Forschung, Industrie und öffentlichen Bedarfsträgern mit dem übergeordneten Ziel, materielle und online-Drogenmärkte im Hinblick auf Verbindungen zur Organisierten Kriminalität zu untersuchen.

Darüber hinaus hatte die Studie das Ziel, Kryptomärkte im Internet systematisch zu analysieren, indem Marktdaten erhoben und ausgewertet worden sind. Die Analyse von Marktdaten ermöglicht die Einschätzung der Veränderung der Struktur und der Funktionsweise der Organisierten Kriminalität im Bereich der illegalen, organisierten Drogendistribution.

In einem ersten Schritt wurden auf der Basis des aktuellen Forschungsstandes relevante Kryptomärkte ausgewählt. Anschließend wurden zum automatischen Auslesen von Marktdaten Web-Scaping-Tools entwickelt. Von den selektierten Kryptomärkten konnten schließlich Marktdaten wie Drogenangebote, Preise, Mengen, Versandländer, Lieferregionen und Bewertungen über einen Zeitraum von zwölf Monaten extrahiert werden. Parallel dazu wurde eine Bedarfserhebung durchgeführt, in der die Perspektive des Bundeskriminalamtes einbezogen wurde.

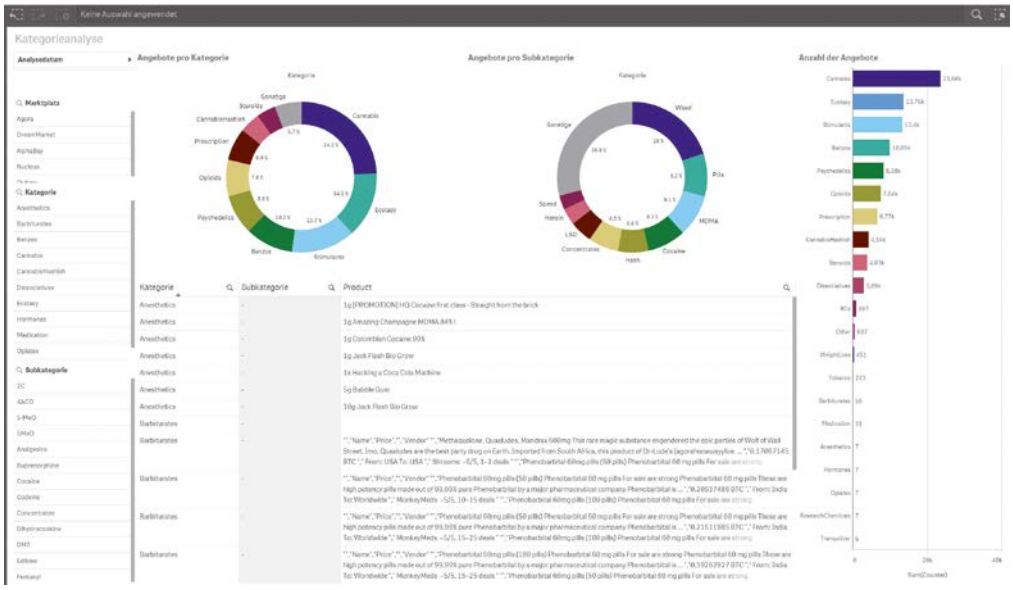
Erfolgreiche Ergebnisse

Die Entwicklung einer interaktiven Analyseapplikation erfolgte prozesshaft mithilfe der Business Intelligence Software QlikView. Die im Rahmen der Studie generierten Daten wurden mittels QlikView geladen, verarbeitet und so aufbereitet, dass deren Auswertung und visuelle Darstellung der Ergebnisse eine systematische Analyse zur Gewinnung von Erkenntnissen im Bereich Kryptomärkte zum Kauf und Verkauf illegaler Drogen optimal unterstützt. In den einzelnen Entwicklungsphasen wurden die Anforderungen an die Analyseapplikation um die spezifischen Bedürfnisse des Bundeskriminalamtes erweitert.



Beispiel eines Krypto-Marktplatzes

VIDRO Analysetool



Die assoziative Datenindexierung und die dynamischen Kalkulationen ermöglichen es dem/der AnwenderIn des Analysetools, komplexe Beziehungen verschiedenster Daten und Datenquellen vereinfacht grafisch darzustellen. Das Analysetool der Studie erfasst etwa unterschiedliche Drogenarten, Unterkategorien dieser Drogenarten, Drogenangebote auf den Marktplätzen, Pseudonyme der HändlerInnen, Kundenbewertungen, Versand- und Zieldestinationen. Damit können mehrere Selektionen miteinander verknüpft und Zusammenhänge unterschiedlicher Kriterien per Klick visuell dargestellt werden. Der weitreichende Funktionsumfang der VIDRO-Analyseapplikation ermöglicht eine umfassende Analyse der Marktdaten von anonymen Plattformen zum Verkauf und Kauf von Drogen, im Besonderen ein detailliertes Verständnis der Entwicklung von angebotenen Drogenarten, erzielten Umsätzen, Anzahl der Drogentransaktionen und Verteilung von HändlerInnen im Analysezeitraum.

Neue Wege gehen!

Mit der im Projekt entwickelten interaktiven Analyseapplikation konnten das Potential und die Vorteile der systematischen Visualisierung von Marktentwicklungen auf anonymen Drogenplattformen erstmals erfolgreich demonstriert werden. VIDRO vermittelt nicht nur den Projektpartnern neue und wichtige Kenntnisse zum Phänomen der Kryptomärkte im Internet, sondern trägt dazu bei, dass die Ergebnisse aus VIDRO der Anfangspunkt für die Entwicklung weiterführender internationaler Forschungsprojekte sind.

Projektleitung
VICESSE – Vienna Centre for Societal Security

Projektpartner
- Bundesministerium für Inneres, Bundeskriminalamt
- LEROX Datenverarbeitung GmbH
- Gesundheit Österreich Forschungs- und Planungs GmbH

Kontakt
Dr. Meropi Tzanetakis
VICESSE – Vienna Centre for Societal Security
Paulanergasse 4/8, 1040 Wien
Tel.: +43 1 929 66 38
E-Mail: meropi.tzanetakis@vicesse.eu
www.vicesse.eu

WatchDog

Mobile Kommunikations- und Multi-Sensorlösung für Sicherheits- und Risikomanagement im Freiland und im Objektschutz

Unterschiedliche, sich oft sehr dynamisch verändernde Sicherheitslagen bei gleichzeitig geforderter Effizienzsteigerung der Personalressourcen erhöhen die Anforderungen an Einsatzkräfte, Sicherheitsdienste und Hilfsorganisationen.
In den letzten Jahren zeigten sich diese Probleme speziell bei Grenzeinsätzen im Rahmen der internationalen Migrationssituation. Ebenso stellen die Sicherheitsanforderungen in Industrieanlagen und bei großen Veranstaltungen dynamische Anforderungen an Sicherheitslösungen und Betreiber. Der Schlüssel für eine optimierte Einsatzführung und erfolgreiche Bewältigung unterschiedlicher Gefährdungslagen besteht in einer innovativen, zeitoptimierten Lagebilderfassung, einer rollen- und szenarienfokussierten, leistungsfähigen Managementlösung sowie einer stabilen Kommunikation unter Berücksichtigung eines flexiblen, multisensoriellen und modularen Systemkonzepts.

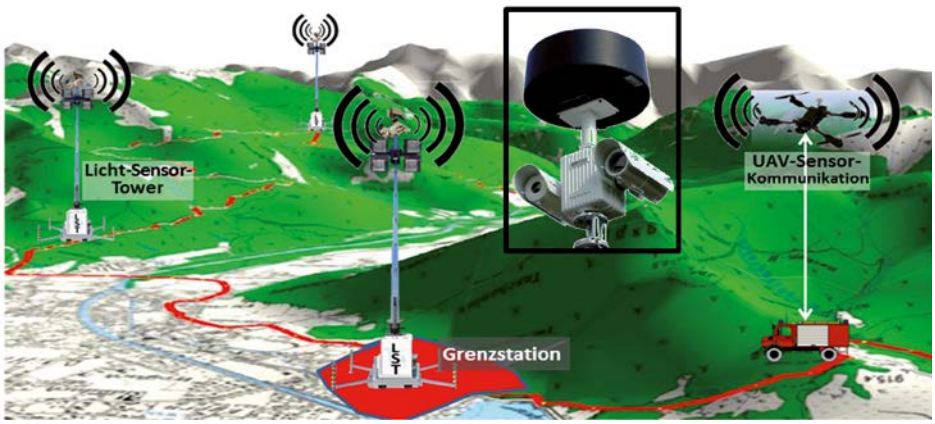
Auf Basis des Know-Hows der Bedarfsträger und Industriepartner wurden für die inhaltliche Umsetzung im Projekt die folgenden fünf Projektszenarien definiert, um ein möglichst breites Einsatzspektrum für öffentliche Bedarfsträger und private Sicherheitsfirmen abzudecken:

- Monitoring von Transitzonen und Grenzräumen
- Freilandüberwachung von Industrieanlagen und kritischen Infrastrukturen unter Einbindung spezieller Sensoren (Gas-Sensor etc.) ins WatchDog-Netzwerk
- Personenmonitoring im Rahmen von Risikomanagement und Sicherungsaufgaben in urbanen, öffentlichen Räumen (kritische dynamische Personenentwicklung etc.) und bei Großveranstaltungen (inkl. Bühnen- und Zeltlagerbereiche)
- Feldlagerschutz im Rahmen humanitärer Einsätze des Österreichischen Bundesheeres
- Spezielle Einsatzszenarien wie z. B. „Brandwache", Monitoring von Hangrutschungs- und Felssturzbereichen, Infrastrukturobjekten in Hochwassersituationen

Die identifizierten Problemstellungen bzw. Sicherheitsaufgaben der für WatchDog relevanten Szenarien erfordern den Entwurf eines flexiblen, mobilen, energie- und kommunikationsautarken multisensoralen Systemkonzepts sowie die Entwicklung und Evaluierung von Komponenten und Modulen für eine gezielte Unterstützung der Sicherheitsszenarien. Die permanente (24/7) und autarke Einsetzbarkeit sowie eine automatisationsgestützte Situationsanalyse für eine optimierte Einsatzführung im Rahmen unterschiedlicher Sicherheitsaufgaben sind weitere wesentliche Zielsetzungen, welche insgesamt einen effizienten Ressourceneinsatz unterstützen. Die Problemstellungen bzw. Sicherheitsaufgaben der für WatchDog relevanten Szenarien erfordern einen Lösungsansatz, der folgende Aspekte berücksichtigt:

- Tag-/Nachtfähigkeit des Systems inkl. einer automatisationsgestützten Datenanalyse
- Gewährleistung einer stabilen, dynamischen Breitbandkommunikation zur sicheren und robusten Übertragung von Multi-Sensor-Daten unabhängig von verfügbaren 3G/4G Funknetzen
- Optimierung von Eigenschaften selbstorganisierender Sensornetze, um Aufwände im Zusammenhang mit manueller Einrichtung und ständiger Anpassung zu minimieren
- Entwicklung von Managementmodulen zur dezentralen manuellen bzw. analysegesteuerten Ausrichtung der genutzten Sensorik zur optimierten Datenaufnahme, Zielführung, strategischen und taktischen Kommunikation sowie Unterstützung der Einsatzführung auf Basis einer optimierten gruppen- und rollenorientierten Datenverteilung
- Gewährleistung einer kostenoptimierten und szenarienorientierten Systemleistung
- Eine gesamtheitliche Betrachtung unter Einbeziehung sozialwissenschaftlicher und rechtlicher Fragestellungen für einen kritischen Zugang zur Wahrnehmung von Überwachungsprozessen

Ziel in WatchDog ist die Entwicklung eines flexiblen, mobilen, energie- und kommunikationsautarken multi-sensoralen Systemkonzepts für die angeführten Sicherheitsszenarien. Um einen flexiblen Einsatz zu gewährleisten, baut das WatchDog-Konzept auf innovative, energieautark betreibbare mobile Teleskopmastsysteme auf, die mit den WatchDog-Kommunikations- und Sensormodulen bestückt werden. Als Unterstützung einzelner Sicherheitsaufgaben werden innovative, LED-basierte Lichtsysteme und Lautsprecher integriert. Bei topographisch schwierigen Situationen werden die Sensormastsysteme mit einem UAV bzw. Ballon ergänzt, welche den Bereich des Kommunikationsnetzwerks absichern, um die Sensormodule gesichert steuern zu können und die Daten an Einsatzkräfte und Leitzentralen stabil weiterzuleiten.



WatchDog-Einsatzszenario „Überwachung Grenzraum/Transitzone"

Das Ergebnis zielt auf die Erstellung eines Proof-of-Concept-Demonstrators ab, der den WatchDog-Ansatz auf Basis definierter Nutzeranforderungen in labornahen Tests evaluiert und einen Funktions-, Performance- und Praxistauglichkeitsnachweis für die relevanten Szenarien erbringt. Hier baut das Projekt auf innovative, kommerziell existierende technologische Lösungen auf, integriert Ergebnisse nationaler bzw. internationaler Forschungsprojekte und fokussiert auf Forschungsthemen wie multi-sensorale Daten- und Situationsanalyse bzw. eine autarke, dynamische sowie stabile Breitbandkommunikationsentwicklung. Ein wesentliches Forschungsthema für das angestrebte Technologiekonzept ist die Entwicklung eines auf die Szenarien abgestimmten, kompakten und kostengünstigen Radarmoduls. Ein weiterer Forschungsschwerpunkt ist die Entwicklung multi-sensor (optisch, thermal, Radar) basierender Analysemethoden und Managementmodule, um eine echtzeitnahe Lagebildgenerierung zur Unterstützung der Einsatzführung sowie zeitkritischer Entscheidungsprozesse zu ermöglichen. Die intensive Einbindung von Bedarfsträgern und eines Expertenboards gewährleistet die fokussierte, praxisrelevante Ausrichtung der Forschungsthemen. Ebenfalls stellen Ergebnisse sozialwissenschaftlicher und rechtlicher Fragestellungen eine wichtige Grundlage bei der Umsetzung der technischen Konzepte dar und sichern somit die Einsetzbarkeit und Akzeptanz von WatchDog ab.

Projektleitung
JOANNEUM RESEARCH Forschungsges.mbH, DIGITAL

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Karl-Franzens-Universität Graz, Institut für Soziologie
- Lakeside Labs Gmbh
- AIT – Austrian Institute of Technology GmbH
- Johannes Kepler Universität Linz; Institut für Nachrichtentechnik und Hochfrequenzsysteme
- Ing. Richard Feischl, IFR
- Kapsch BusinessCom AG
- INRAS GmbH
- Airborne Robotics
- WAGNER Sicherheit GmbH
- Agentur für Europäische Integration und wirtschaftliche Entwicklung GmbH

Kontakt
DI Alexander Almer
JOANNEUM RESEARCH DIGITAL, Institut für Informations- und Kommunikationstechnologien
Steyrergasse 17, 8010 Graz
Tel.: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital


Dienstleistung

F&E Dienstleistungen

ABC-Deko

Großflächige Dekontamination: Lernen aus den praktischen Erfahrungen von Tschernobyl

Ziel des Forschungsprojekts ABC-Deko war, Erfolge und Misserfolge der großflächigen Dekontamination nach dem Unfall im Kernkraftwerk Tschernobyl in Zusammenarbeit mit dem damals technisch Hauptverantwortlichen, Iouli Andreev, und seiner Frau Irina Andreeva in einem „Erfahrungshandbuch" zu dokumentieren und nutzbar zu machen, als Beitrag zur besseren Planung künftiger großflächiger Dekontamination sowie Schonung von Leben und Gesundheit von Einsatzkräften und DekontaminatorInnen.

Es gibt bislang keine systematische Aufarbeitung der im Zuge umfangreicher Dekontaminationsmaßnahmen gewonnenen praktischen Erfahrungen, umgesetzten und verworfenen Lösungen oder der Wirksamkeit getroffener Maßnahmen. Der Großteil in der Literatur vorgefundener Berichte dürfte zudem eher fern vom realen Geschehen verfasst worden sein sowie offizielle und institutionell geprägte Sichtweisen darstellen.

Das im Rahmen von ABC-Deko erstellte „Erfahrungshandbuch Dekontamination" kann diese Defizite nicht wettmachen, aber es stellt systematisch jene Maßnahmen zusammen, über die das Ehepaar Andreev in über 80 Interviews aus eigener Erfahrung berichtet hat. Diese Informationen wurden, wo möglich, Angaben aus der Literatur gegenübergestellt und zuletzt mit neueren Erfahrungen aus Fukushima verglichen.

Die riskantesten Dekontaminationsarbeiten in Tschernobyl fanden in den ersten Monaten im Zuge der Bemühungen um die Beherrschung des Unfalles und des Versuchs, die intakten Reaktorblöcke auf jeden Fall in Betrieb zu halten, statt. Die nachfolgenden Versuche, Kraftwerksstandort, Gelände und Werksiedlung Pripjat mit 50.000 Einwohnern wieder bewohnbar zu machen, erstreckten sich über mehrere Jahre.

Im technischen Teil des Handbuches werden u.a. Maßnahmen zur Unterdrückung radioaktiven Staubes und der Dekontamination von Geräten und Fahrzeugen, unterschiedlicher Oberflächen, Straßen, Gebäude, Siedlungen und Wald beschrieben: wie bei den meist physikalischen Dekontaminationsmethoden des Waschens, Abkratzens, Abdeckens etc. vorgegangen wurde, was sich bewährt hat, was nicht. Dabei zeigt sich, wie weit Anspruch und Wirklichkeit auseinanderklaffen. De facto gelang es jeweils nur in ausgewählten „Inseln" (Straßen, Gebäuden oder kleinen Waldstücken), radioaktive Belastungen auf ein vertretbares Maß zu reduzieren. Die gesamte Fläche wird erst sehr langfristig über geologische Zeiträume durch natürlichen radioaktiven Zerfall dekontaminiert werden.

Ausführlich werden Probleme mit ferngelenkten Maschinen und Robotern geschildert, die in hochradioaktiven Zonen bei Dekontaminationsarbeiten nur sehr begrenzt erfolgreich waren, sich jedoch beim Bau des Sarkophags bewährt haben.

Ein besonderes Thema ist die Frage der Kontamination bzw. Dekontamination von Wasser. Ein Großteil der bleibenden radioaktiven Belastung im Nahbereich ging auf mittelfristig nicht wasserlösliche Keramikteile und -staub zurück, die durch die Explosion des Reaktorkerns entstanden sind. Die Radioaktivität wurde daher in den obersten Bodenschichten zurückgehalten und stellte für das Grundwasser keine unmittelbare Gefahr dar.

Über 800 provisorische Deponien zur Entsorgung kontaminierten Materials wurden angelegt. Hochradioaktives Material wurde in würfelförmige Metallbehälter mit einem Kubikmeter Inhalt gefüllt und in halbfertigen Deponien oder nahe den Blöcken 5 und 6 gestapelt. Für weniger stark verstrahltes Material wurden meist nur Gruben ausgehoben, mit Lehmschichten ausgekleidet und bedeckt. Bei Siedlungen und Wäldern stapelte man das Material eher in langen Wällen und bedeckte diese mit Erde – so blieben Deponien erkennbar. Für Dokumentation blieb keine Zeit.

Neben technischen wird auch auf sozio-politische und organisatorische Aspekte wie Verpflegung, Hygiene, Arbeitsrhythmus, Gemeinschaft sowie Korruption eingegangen.

Versucht man aus den vielen Einzelproblemen und Erfahrungen ein Résumé zu ziehen, so drängen sich einige Erkenntnisse auf:

- Die politischen Zielvorgaben bestimmen Art und Ausmaß der aus technischer Sicht nicht immer sinnvollen Dekontaminationsmaßnahmen.
- Dekontamination ist umso wirkungsvoller und effizienter, je besser man Unfallhergang, Art der Kontamination, ihre Ausbreitung und Verteilung versteht.
- Unter den schwierigen Bedingungen in kontaminiertem Gebiet waren technisch einfache Lösungen oft die wirksamsten.
- Ferngelenkte Maschinen versagten weitgehend bei der Dekontamination in hochaktiven Zonen, vor allem wenn die Flächen mit Trümmern übersät waren.

- Die häufig propagierte Abtragung der obersten Bodenschicht führt sehr rasch zu unbewältigbarer Kubatur radioaktiven Abfalls.
- Allen positiven Meldungen zum Trotz war immer nur punktuelle Dekontamination möglich (einzelne Gebäude, kleine Flächen); Wälder mussten gefällt werden.
- Dekontamination gelingt nie vollständig; die gängigen gesundheitlichen Grenzwerte können in der Regel nicht erreicht oder unterschritten werden.

Interessant gestaltete sich der Vergleich der Erfahrungen der Andreevs mit Erfahrungsberichten aus Fukushima, insbesondere des National Defense Research Institutes der RAND Corporation, USA. Während Publikationen zur Dekontamination in Fukushima beeindruckende Erfolge zu feiern scheinen, zeigt genaueres Hinsehen, dass die referierten Quotienten aus Belastung vor und nach Dekontamination für verschiedene Objekte, Oberflächen und Methoden jeweils zwischen 1, d.h. wirkungslos, und Zahlen bis zu 20 variieren. Aufgrund dieser Streuung kommt die RAND-Studie zu ähnlich ernüchternden Ergebnissen, wie von den Andreevs beschrieben. Fortschritte dürfte es vor allem bei persönlicher Dosimetrie und maschineller Dekontamination von Oberflächen gegeben haben. Trotz industriegetriebener Fortschritte bei Robotern und ferngesteuerten Maschinen wird nicht erwartet, dass in absehbarer Zeit Geräte zur Verfügung stehen werden, deren Elektronik hohe Strahlung aushält sowie ausreichend Kraft zur Hindernisbeseitigung, Reichweite und Betriebsdauer aufbringen. Fortschritte sind am raschesten bei biologischer Dekontamination zu erwarten, allerdings nur bei wasserlöslichen Radionukliden.

Aus den Erkenntnissen wurden einige Empfehlungen abgeleitet:

- Experten, die als Entwickler oder Betreiber an der havarierten Anlage beteiligt waren, sollte bei der Definition der Zielvorgaben sowie Minderungs- und Dekontaminationsmaßnahmen keine Entscheidungsmacht übertragen werden, da potentielle Fachblindheit oder auch (un)bewusstes Bemühen um Exkulpation die Sicht auf bessere Lösungen verstellen kann. Ihre Auskunfts-, Beratungstätigkeit und praktische Mitwirkung bleibt unentbehrlich.

- Betreiberstaaten von nuklearen oder anderen potentiell großräumig gefährdenden Anlagen müssen Pläne und Konzepte für einen möglichen „worst case" vorbereitet haben. Im Ernstfall fehlen Ruhe und Kapazität, solche zu entwickeln.

- Bei Nuklearunfällen wäre ein stationäres, stromnetzunabhängiges Überwachungssystem mit Fernübertragung für den ersten Überblick wesentlich. Luftgetragene Messeinrichtungen dienen der Ergänzung, aber ohne Bodendaten liefern sie nicht die notwendige feine Auflösung. Ein (auf freiwilliger Basis) in Mobiltelefone integriertes Messsystem, das einer Zentrale kontinuierlich Belastungsdaten meldet, könnte sowohl Telefonnutzern Sicherheit geben als auch Einsatzkräften ein besseres und jeweils aktuelles Bild der Belastung liefern. Österreich könnte hier – ähnlich wie vor Jahren beim stationären Messnetz – Vorreiter werden. Ein Beispiel: „Dosis-App", ein Strahlendetektor für's Smartphone, eingereicht bei einem Innovationsbewerb in Niederösterreich.

Projektleitung
Universität für Bodenkultur, Zentrum für Globalen Wandel und Nachhaltigkeit
Projektpartner
- Bundesministerium für Landesverteidigung und Sport

Kontakt
Mag. Richard Kromp
Universität für Bodenkultur, Zentrum für Globalen Wandel und Nachhaltigkeit
Borkowskigasse 4, Baracke 4, 1190 Wien
Tel.: +43 1 47654 – 7708
E-Mail: richard.kromp@boku.ac.at
www.boku.ac.at/wissenschaftliche-initiativen/zentrum-fuer-globalen-wandel-nachhaltigkeit

auxilium:at

Analyse von Beteiligungsformen der österreichischen Bevölkerung bei der Bewältigung intensiver Flüchtlingsbewegungen

Hintergrund zu auxilium:at – Hilfe durch Österreich

Der Hochkommissar der Vereinten Nationen für Flüchtlinge (UNHCR) beschreibt die gegenwärtige Flüchtlingslage als eine der größten humanitären Flüchtlingskatastrophen seit dem zweiten Weltkrieg (UNHCR, 2014), deren Bewältigung nicht nur auf politischer Ebene stattfinden muss, sondern die gesamteuropäische Bevölkerung vor neue Aufgaben stellt. Das Jahr 2015, in dem ca. 90.000 Asylanträge in Österreich gestellt wurden, hat sowohl die Einstellung zu Flüchtlingen und das Engagement der österreichischen Bevölkerung in der akuten Flüchtlingshilfe deutlich gemacht, als auch aufgezeigt, dass aufgrund fehlender Erfahrungen ein bestmöglicher Umgang mit dieser Situation, ein teils improvisiertes Miteinander von Blaulichtorganisationen, NGOs und der Zivilbevölkerung notwendig war. Letztere erwies 2015 ein hohes Maß an sozialer Partizipation, welches ein Wir-Gefühl unter den HelferInnen hervorrief.

Bereits Georg Simmel (1908) war der Meinung, dass die Fürsorge für sozial Schwächere nicht nur der Notlinderung gilt, sondern vor allem zum gesellschaftlichen Zusammenhalt beitragen kann. Diese Annahme, dass aktive soziale Teilnahme die soziale Kohäsion einer Gesellschaft beeinflusst (Dobbernack, 2014) und dadurch der soziale Frieden wächst, wird auch von der Europäischen Union durch ihre Pläne unterstützt (European Commission, 2015).

Einzelne Untersuchungen setzten sich zwar mit der ehrenamtlichen Flüchtlingshilfe und Flüchtlingsintegration in Aufnahmegesellschaften auseinander, jedoch finden sich keine Studien wie auxilium:at, die aufbauend auf Erfahrungen die Grenzen in der Flüchtlingsarbeit der österreichischen Zivilgesellschaft und die Kooperation zwischen Blaulichtorganisationen und NGOs untersuchen und darauf basierend Empfehlungen an politische AkteurInnen abgeben.

Darüber hinaus schließt die bisherige Flüchtlingsforschung einen weiteren Bereich weitgehend aus: Neben der Tätigkeit von ehrenamtlichen FlüchtlingsarbeiterInnen leisten PolizistInnen, haupt- und ehrenamtliche MitarbeiterInnen von NGOs und anderen Institutionen in der Akuthilfe einen wesentlichen Beitrag. Obwohl diese Organisationen ihre Aktivitäten teilweise dokumentieren, fehlen Berichte über Erfahrungen betreffend Kooperationen mit der österreichischen Zivilgesellschaft, ebenso wie Informationen zu organisationsinternem oder -externem Unterstützungsbedarf. Genau das ist jedoch relevant, wenn aus Erlebnissen für künftige ähnliche Situationen gelernt werden soll und im Sinne eines Bottom-Up-Ansatzes Empfehlungen für politische EntscheidungsträgerInnen und in der Akutversorgung von Flüchtlingen involvierte Organisationen formuliert werden sollen. Auch wenn die Zahl der Asylanträge 2016 im Vergleich zu 2015 um 52,4 Prozent gesunken ist (42.073 Ansuchen; BM.I 2016), braucht es für die (Weiter)Entwicklung einer nationalen und globalen Flüchtlingspolitik Analysen von Vergangenem. Diesen Ansatz untermauert die Denkrichtung von Kleist (2015), der die Notwendigkeit der praktischen Umsetzung von Forschungsergebnissen der Flüchtlingsforschung unterstreicht, um politische AkteurInnen beeinflussen zu können.

Methodische Umsetzung

In auxilium:at erfolgt dies mittels eines Mix aus qualitativen und quantitativen sozialwissenschaftlichen Methoden, der regelmäßig mit VertreterInnen der Bedarfsträgerorganisationen (BM.I, BMLVS, Caritas Österreich und Rotes Kreuz Österreich) inhaltlich und methodisch reflektiert wird:

Zunächst werden bestehende sowie seit 2015 neu entstandene staatliche und private Akuthilfe-Initiativen für Flüchtlinge in einem Bericht zusammengeführt, um einen Überblick über unterschiedliche Tätigkeiten zu geben und Möglichkeiten zur Vernetzung zu fördern.

Im Zuge einer diskursanalytischen Medienanalyse wird untersucht, wie Webseiten und Social Media-Plattformen im Zeitalter neuer Medien zur Koordination von akuter Flüchtlingshilfe genützt werden und welche BenutzerInnen-Rollen davon abgeleitet werden können. Des Weiteren wird untersucht, welche thematischen Diskurse in der Flüchtlingsdebatte gegenwärtig vorherrschen, um so ein Stimmungsbild der österreichischen Bevölkerung zu erstellen. Letzteres wird durch eine quantitative CAPI-Befragung (Computer Assisted Personal Interview), bei der 2000 ÖsterreicherInnen über ihre Bereitschaft zu Aktivitäten in der ehrenamtlichen akuten Flüchtlingsarbeit ebenso wie zu Vorstellungen über Flüchtlinge befragt werden, ergänzt.

Zusätzliche Daten werden durch qualitative Feldforschungseinsätze in Traiskirchen und Nickelsdorf erhoben, bei der u.a. dort Ansässige und Freiwillige über ihre Erfahrungen wie auch über persönliche, organisatorische und strukturelle Herausforderungen befragt werden.

Die Erhebung von persönlichen, strukturellen und organisatorischen Merkmalen bei der Akutversorgung von Flüchtlingen steht neben Formen von Kooperationen mit der Zivilbevölkerung und anderen Einsatzorganisationen im Zentrum der quantitativen Onlinebefragungen, bei denen neben PolizistInnen auch Haupt- und Ehrenamtliche von NGOs (Caritas Österreich und Rotes Kreuz Österreich) zu dieser Tätigkeit befragt werden.

Die durch die unterschiedlichen Erhebungen gewonnenen Erkenntnisse werden analysiert und fließen in einen Empfehlungskatalog mit unterschiedlichen Vorschlägen für Optimierungsmaßnahmen ein, der mit den Bedarfsträgern im Zuge eines Workshops hinsichtlich Inhalt und Umsetzbarkeit diskutiert wird.

Projektleitung
IHS – Institut für Höhere Studien, Wien

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport
- Institut für empirische Sozialforschung IFES
- IFES Feld GmbH
- Caritas Österreich
- Österreichisches Rotes Kreuz

Kontakt
Mag. Dr. Elisabeth Frankus
IHS – Institut für Höhere Studien, Wien
Josefstädter Straße 39, 1080 Wien
Tel: 01 59991 – 270
E-Mail: frankus@ihs.ac.at
www.ihs.ac.at

Bontempiorgel

Behördennetzwerk – Implementierungsvorschlag für eine Staatsgrundnetzlösung

Ein Behördennetzwerk dient dazu, sowohl Versorgungssicherheit für die Kommunikation zwischen staatlichen Behörden als auch den Austausch von Informationen und Daten in sicherheitspolitischen Ausnahmefällen sicherzustellen. Es impliziert einerseits risiko-, sicherheits- und compliance-bezogene, andererseits auch technische, rechtliche, organisatorische und politische Aspekte, die im Rahmen dieser Studie umfassend beleuchtet werden.

Seit dem großen Durchbruch der Internetnutzung Mitte der neunziger Jahre entwickelte sich das Internet in den letzten Jahren zu einer der wichtigsten Infrastrukturen überhaupt. Es ermöglicht, dass heterogene, vernetzte Geräte mittels eines standardisierten Internet-Protokolls (IP) und praktisch ohne technische Inkompatibilitäten miteinander kommunizieren können. Diese breite Eignung des Internets führte in den letzten Jahren aus Effizienzgründen zu einem Bedeutungsverlust anderer dedizierter Kommunikationsnetze, wofür die Umstellung der klassischen Telefonnetze auf IP ein Paradebeispiel ist. Die Sicherstellung von ausreichender Zuverlässigkeit, Verfügbarkeit und Sicherheit IP-basierter Netze ist essentiell, da immer wichtigere gesellschaftliche Bereiche auf die Internet-Technologie umgestellt werden. Somit wurde das Internet wie in vielen Lebensbereichen auch zu einer Voraussetzung für das Funktionieren der wichtigsten Bereiche der öffentlichen Verwaltung. Im Rahmen der Österreichischen Sicherheitsstrategie sowie der Österreichischen Strategie für Cyber-Sicherheit (ÖSCS) werden nun gezielt Maßnahmen gesetzt, um die Sicherheitslage im Zusammenhang mit der Telekommunikationsinfrastruktur zu erhöhen.

Im Zuge der Liberalisierung des Telekommunikationsmarktes wurde die zuvor lange Jahre in staatlicher Hand befindliche kritische Infrastruktur der Kommunikations- und Datennetze privatwirtschaftlich organisierten Unternehmen überantwortet. Damit sollte in die zuvor geschützten Bereiche mehr Wettbewerb einziehen, jedoch arbeiten diese Organisationen primär gewinnorientiert, richten sich nach kleinräumigeren Organisationszielen aus und berücksichtigen nationale Anforderungen und Interessen nicht in dem Maße, welche die Republik besonders in Ausnahmesituationen an ein Kommunikationsnetzwerk hat. Durch die Bedeutungszunahme des Internets für die Kommunikation im Allgemeinen, die gleichzeitige Funktionalitätserweiterung und zunehmende Kapazitätsanforderungen dieser Netze verschärft sich diese Situation zusehends. Gewissermaßen hat sich der Staat in eine technologische Abhängigkeit begeben; er ist zum Servicekunden mutiert.

Behörden müssen also aus ihrer Perspektive heraus Überlegungen anstellen, eine dedizierte Kommunikationsstruktur zu etablieren, die eine sichere integre Kommunikation im Lichte der bestehenden technischen Heterogenität der aktuellen Netzlandschaft im Behördenumfeld ermöglicht. Dies gilt nicht nur während der täglichen operativen Tätigkeit, um Vertraulichkeit gegenüber Dritten sicherzustellen, sondern auch in Ausnahmesituationen, welche die Verfügbarkeit – insbesondere von IKT-Serviceprovidern – beeinträchtigen können.

Zielsetzung des Projekts Bontempiorgel ist die Erstellung einer Studie, die nach einer formalen Dokumentation der Ziele im ersten Teil das Begriffskonzept absteckt, mögliche Stakeholder – definitiv nicht ausschließlich Behörden – nennt und aus diesen den möglichen Anwenderkreis rekrutiert. Zusätzlich muss definiert werden, was ein Staatsgrundnetz leisten kann und wie die verschiedenen Kommunikationsformen, welche mit Sicherheit über reine Sprachkommunikation hinausgehen, gestaltet werden können. Diese Anwenderservices müssen in sicherheitspolitischen Anwendungsfällen für den Anwenderkreis nutzbar sein, um den vitalen Kommunikationsbedarf der Behörden und Betreiber kritischer Infrastrukturen in derartigen Situationen decken zu können. Grundlegende Designanforderungen und Gestaltungsaspekte aus praktischen Einsatzerfahrungen runden den Begriffsteil ab.

Im zweiten Teil werden kurz historische Netzwerkstrukturen und ihre damaligen Möglichkeiten vorgestellt, die im Zuge der fortschreitenden technologischen Entwicklungen mittlerweile nicht mehr nutzbar sind. Darüber hinaus werden bestehende Netzwerkstrukturen in Österreich beleuchtet, die potentiell Teil eines Behördennetzwerks sein oder zumindest zur Funktionalität beitragen

können. Diese können staatlichen Initiativen oder Strukturen entspringen, aber auch privatwirtschaftlicher Natur sein. Dieses Kapitel wird durch die Vorstellung von entsprechenden Staatsgrundnetz-Initiativen von Ländern der europäischen Nachbarschaft – soweit hier Informationen verfügbar sind – abgeschlossen.

Im dritten Abschnitt der Studie werden zunächst die verschiedenen Anforderungen an eine Staatsgrundnetzlösung wie technische Leistungsqualität und technisch-operative Sicherheitsaspekte formuliert. Dabei werden die technischen, organisatorischen, rechtlichen und politischen Einflussfaktoren als Überbegriffe gewählt. Anschließend wird ein Architekturvorschlag für ein österreichisches Behördennetzwerk mit Realisierungsvarianten formuliert. Es werden zudem die möglichen Handlungsoptionen diskutiert, wobei auch technische Teilumsetzungen und ein realistischer Zeithorizont thematisiert werden.

Im Anschluss daran wird im vierten Kapitel der postulierte Architekturvorschlag einer vorbereitenden Risiko- und Sicherheitsanalyse unterzogen. Hierbei fließen operative, technologische sowie organisatorische Risiken ein. Die Sicherheitsanalyse liefert dazu passende Schutzmaßnahmen, welche auf die kritischen Versorgungspunkte eines Staatsgrundnetzes angewendet werden können.

Im letzten Teil der Studie werden Nutzenaspekte der hier propagierten Staatsgrundnetzlösung diskutiert und argumentative Grundlagen dargelegt.

Das Gesamtergebnis ist eine grobe Anforderungsanalyse, welche als Diskussionsgrundlage für eine politisch-strategische Entscheidung zur Implementierung eines Behördennetzwerks dienen kann. Diese thematisiert Herausforderungen sowie Implikationen und formuliert Gestaltungsoptionen für die zukünftige Architektur, die Implementierung und den Betrieb. Abgerundet wird die Studie durch eine explizite Analyse von Risiko-, Sicherheits- und Nutzenaspekten eines Behördennetzwerks in Österreich.

Dieses Projekt wurde als eines der ersten KIRAS-Vorhaben eingeschränkt informationsklassifiziert. Im Zuge dessen wurden ein organisatorisches Verfahren definiert und technische Voraussetzungen formuliert, um den erhöhten Informationssicherheitsanforderungen Rechnung zu tragen. Alle beteiligten MitarbeiterInnen des AIT wurden von BM.I und BMLVS sicherheitsüberprüft und eine anerkannte Verschlüsselungsinfrastruktur für die elektronische Kommunikation zwischen den ProjektpartnerInnen wurde etabliert.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Projektpartner
- Bundesministerium für Inneres
- Bundeskanzleramt
- Bundesministerium für Landesverteidigung und Sport

Kontakt
Mag. Martin Latzenhofer
AIT – Austrian Institute of Technology GmbH
Donau-City-Straße 1, 1220 Wien
Tel.: +43 50550 4134
E-Mail: martin.latzenhofer@ait.ac.at
www.ait.ac.at

CANNDAT

Erstellung einer Datenbank für Chemotypen von Cannabis sp. (Hanf) zur Unterstützung der kriminaltechnischen Analyse von Rauschdrogen

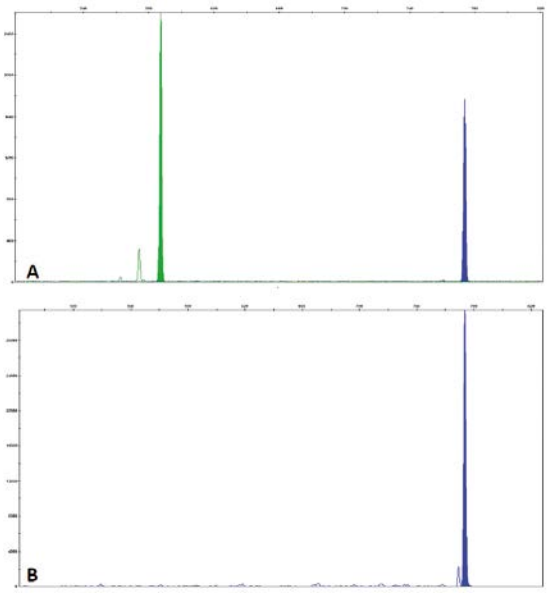
Im europäischen Verkehrsraum stehen etwa 50 Sorten von Cannabis (Hanf) zur Produktion von Nutzhanf zur Verfügung, deren durchschnittlicher Gehalt an Tetrahydrocannabinol (THC), einem halluzinogenen Cannabinoid, bei < 0.2 % liegt. Daneben werden zahllose Hochertragssorten mit dem Ziel des Suchtmittelmissbrauchs illegal angebaut, sog. „Drogenlinien", deren THC-Gehalt bis über 20 % liegen kann. Eine Unterscheidung von sog. „Drogenhanf" und Nutzhanf ist nach dem derzeitigen Stand der Kriminaltechnik nur durch die quantitative chemische Untersuchung bestimmter Cannabinoide in blühendem Pflanzenmaterial möglich. Nicht selten gehen sichergestellte nichtblühende Pflanzen (im Jahr 2014 ca. 30 mal in Niederösterreich) oder Pflanzenteile, die keine oder wenig Cannabinoide enthalten (z. B. Saatgut oder Wurzeln bzw. Sprossen; im Jahr 2014 mehr als 50 Proben in Niederösterreich), der Ermittlungsarbeit verloren oder müssen für eine Klassifizierung unter erheblichem pflanzenbaulichen Aufwand in Gewächshäusern zur Blüte gebracht werden – etwa in sehr jungen oder bereits abgeernteten Indoorplantagen, bei gehandeltem Saatgut oder in aufgefundenem Wildwuchs im Freiland.

Die genetische Bestimmung des sog. Chemotyps, einer dem Sortenbegriff übergeordneten qualitativen Kategorie, ermöglicht mittels der gegenständlichen Studie eine effizientere Zuordnung zu einer der beiden Gruppen. Eine genetische Analyse ist in allen Entwicklungsstadien und Geweben der Hanfpflanze möglich und kann schneller und kostengünstiger als die quantitative Cannabinoid-Bestimmung und ohne zusätzliche kosten- und zeitaufwändige Pflanzenanzucht durchgeführt werden. Das Bundeskriminalamt (.BK) betont einen deutlichen Bedarf für die ergänzende Verwendung der vor kurzem veröffentlichten genetischen Methode (Markersystem D589; Staginnus et al., 2014) in der Kriminaltechnik. Eine zukünftige Anwendung in der Fallarbeit wird durch die Österreichische Agentur für Ernährungssicherheit AGES ausgeführt.

Abhängig von dem Verhältnis der beiden Cannabinoide THC und CBD (Cannabidiol, eine nicht-halluzinoge Komponente) in der Blüte, können drei sog. Chemotypen für Cannabis definiert werden: „vorwiegend CBD-haltige", „vorwiegend THC-haltige" Cannabis-Pflanzen sowie ein „Mischtyp". Die Verwendung von bestimmten Chemotypen in Nutzhanfsorten bzw. sog. „Drogenlinien" ist durch den Züchter bestimmt und muss nicht zwingend mit dem THC-Ertrag gekoppelt sein. Allerdings lässt sich das Zuchtziel einer THC-Hochertragssorte mit Pflanzen des Chemotyps „vorwiegend THC-haltig" bzw. „Mischtyp" leichter erreichen. Die hauptsächliche Verwendung des Chemotyps „vorwiegend CBD-haltig" ist dagegen in der Nutzhanfzüchtung anzunehmen, da sie die Einhaltung des Grenzwerts von 0.2 % THC eher erlaubt. Die tatsächliche Verwendung wurde bisher jedoch nicht systematisch untersucht. Die genetische Chemotypbestimmung kann nur dann kriminaltechnisch zur Unterscheidung von „Drogenlinien" und Nutzhanfsorten eingesetzt werden, wenn eine hauptsächliche oder ausschließliche Verwendung des Chemotyps „vorwiegend CBD-haltig" in allen europäischen Nutzhanfsorten bestätigt wird und so als Klassifizierungsmerkmal dienen kann.

Ziel ist es, mit den Erhaltungszüchtern der Sorten in den jeweiligen Ländern in Kontakt zu treten, die Sorten bzw. Saatgutproben anzufordern und als Referenzmaterial vorzuhalten.

Für eine repräsentative Stichprobe von 100 Samen pro Kultivar sollen mit Hilfe der DNA-PCR-Methode die genetischen Anlagen für die beiden Chemotypen „vorwiegend THC-haltig" und „Mischtyp" einerseits bzw. den Chemotyp „vorwiegend CBD-haltig" andererseits auf DNA-Ebene ermittelt werden. Die Ergebnisse sollen in einer Datenbank gesammelt werden. Somit kann festgestellt werden, inwieweit der für illegale, sog. „Drogenlinien" bekannte „vorwiegend THC-haltige" Chemotyp bzw. der „Mischtyp" auch in der Nutzhanfzüchtung anzutreffen ist und wie homogen die einzelnen Sorten hinsichtlich des Chemotyps sind.



Elektropherogramm mit den Signalen des Markers D589 beim Vorliegen von Cannabis-Material des Chemotyps „vorwiegend THC-haltig" oder „Mischtyp" (A) bzw. „vorwiegend CBD-haltig" (B). „Vorwiegend THC-haltig" oder „Mischtyp" weisen ein Markersignal bei ca. 589 bp auf (grün), die interne Kontrolle liefert ein Signal bei ca. 770 bp (blau).

Der so gewonnene Überblick ermöglicht eine Entscheidung darüber, ob die genetische Bestimmung des Chemotyps eine Zuordnung zum züchterischen Verwendungszweck der Pflanzen als Nutzhanf bzw. „Drogenhanf" erlaubt und eine sinnvolle Ergänzung zur Bestimmung des absoluten Wirkstoffgehalts mittels chemischer Analytik in der Kriminaltechnik darstellt.

Die gleichzeitige Etablierung der Methodik in der AGES soll eine kriminaltechnische Anwendung des Verfahrens im Auftrag der Justiz (.BK) ermöglichen. Ebenfalls soll eine parallel zur Sortenbeschaffung angelegte Referenzsammlung aller untersuchten Sorten bei der AGES die kriminaltechnische Fallarbeit des .BK unterstützen. Die AGES soll künftig als nationales Referenzlabor für die genannten forensischen Analysen dienen.

Projektleitung
AGES – Österreichische Agentur für Gesundheit und Ernährungssicherheit
Projektpartner
• Bundeskriminalamt
Kontakt
Dipl.-Ing. Verena Peterseil
Institut für Lebensmittelsicherheit Wien
Spargelfeldstraße 191, 1220 Wien
+43 50555 32203
verena.peterseil@ages.at
www.ages.at

CybSiVerkehr

Cyber Sicherheit für zukünftige Verkehrssysteme

Unser Verkehrssystem unterliegt durch die breite Anwendung von Informations- und Telekommunikationstechnologien einem grundlegenden Wandel. IT im Fahrzeug sowie Kommunikation und Koordination zwischen Fahrzeugen und Infrastrukturelementen für Straße, Schiene, Wasser und Luft ermöglichen kooperative und intelligente Verkehrssysteme (Cooperative Intelligent Transport Systems, C-ITS). Disruptive Technologien wie autonome Autos mit entsprechender künstlicher Intelligenz werden unser Verständnis von Mobilität und Logistik grundlegend ändern. Die technologischen, wirtschaftlichen, sozialen und politischen Auswirkungen dieser Technologien sind tiefgreifend.

Als ein Teil der kritischen Infrastrukturen haben Ausfälle von Transportsystemen auf nationaler und europäischer Ebene eine verheerende Auswirkung auf alle Branchen und das Leben in der Gesellschaft. Die zugrundeliegende IT-Infrastruktur, wie beispielsweise C-ITS und Cyber-Systeme autonomer Fahrzeuge, werden ein Ziel von Cyber-Attacken. Aufgrund der Komplexität, Funktionalität und Konnektivität sind moderne Transportsysteme dafür besonders anfällig. Neben großangelegten Angriffen auf die Infrastruktur werden neue Angriffsmethoden wie z. B. Ransomware in Zukunft auch Fahrzeuge betreffen. Angreifer können den Zugriff auf ein Fahrzeug aus der Ferne sperren und nur gegen Bezahlung wieder freigeben. Diese komplexen Infrastrukturen sind verteilt und schwer vor Cyber-Angriffen zu schützen. Cyber-Sicherheit und Resilienz müssen schon beim Design und in der Konzeption fundamental berücksichtigt werden.

Die Studie CybSiVerkehr erstellt einen systematischen und Österreich-fokussierten Überblick über die sich entwickelnde Bedrohungslage. CybSiVerkehr wird im Rahmen der globalen industriellen und technologischen Entwicklung eine eingehende Analyse der für Österreich relevanten Cyber-Herausforderungen durchführen. Die Studie wird aktuelle Forschungstrends und Entwicklungen mit dem Fokus auf Cyber-Sicherheit einbeziehen, um so die spezifischen Herausforderungen und Auswirkungen auf die österreichische Gesellschaft zu identifizieren. Zudem wird die Studie sowohl zu technischen als auch gesellschaftlichen Aspekten die Meinungen von ExpertInnen und Interessensgruppen erfassen. Ein wichtiges Ergebnis der Studie werden umfassende Handlungsempfehlungen an die entscheidenden Stakeholder sein, um Österreich auf die Cyber-Herausforderungen künftiger Verkehrssysteme vorzubereiten.

Die Studie wird Leitlinien zu relevanten Themen wie Risikomanagement, Prävention, Cyber Situational Awareness, gesellschaftliche Bereitschaft zur Nutzung dieser Fahrzeuge und Privatsphäre der Nutzer enthalten und Hinweise geben, wie Österreich sich an die Spitze der Europäischen Union im Bereich Cyber-Sicherheit von Transportsystemen stellen kann.

In einem ersten Schritt wurden Informationen zu connected vehicles und C-ITS gesammelt, um den aktuellen Stand und Entwicklungen zu erfassen. Dabei ist klar, dass es immer wichtiger wird, das Thema Cyber-Sicherheit in Bezug auf connected, autonomous und automated vehicles zu betrachten. Bereits jetzt werden kooperative Dienste zwischen Infrastruktur und Fahrzeugen durch ITS-Standards von ETSI (European Telecommunications Standards Institute) und CEN (Comité Européen de Normalisation) spezifiziert. In Österreich werden im Testprojekt Eco-AT kooperative Verkehrssteuerungen erprobt und Schnittstellen zwischen Fahrzeug und Verkehrsmanagement definiert.

Für das Fahrzeug selber entstehen bei der International Organization for Standardization (ISO) und der Society of Automotive Engineers (SAE) Standards, die die Cyber-Cicherheit im Fahrzeugnetz und den Zugriff auf Fahrzeugdaten (extended vehicle) behandeln. Dabei existiert noch kein Gesamtkonzept, und jeder Standard definiert nur seinen Teilbereich. Gerade an den Schnittstellen und Systemgrenzen entstehen Angriffspunkte. Im rechtlichen Bereich besteht in erster Linie ein Bedarf an international gültigen Regeln, um die Cyber-Sicherheit zu verbessern und Verantwortlichkeiten zu definieren. Wir benötigen in Zukunft global akzeptierte Standards für den grenzenlosen Cyberspace. Die gesellschaftlichen Ansätze adressieren das Verhältnis zwischen Einzelperson und Technik bzw. Maschine und in weiterer Folge die Beziehung zwischen Gesellschaft und Technik. Dabei wird das Mensch/Maschinen-Verhältnis näher beleuchtet, in dem auf notwendige Kompetenzen im Umgang mit autonomen Fahrzeugen eingegangen wird. Das Vorhandensein dieser Fähigkeiten hat Auswirkungen darauf, ob neue Technologien von der Gesellschaft akzeptiert und genutzt werden. Ein zentrales Thema stellen außerdem die möglichen Auswirkungen einer Implementierung von connected und autonomous vehicles für die Gesellschaft dar.

Das Ziel der Studie CybSiVerkehr ist die Entwicklung von Handlungsempfehlungen zum Thema „Cyber-Sicherheit für autonomes Fahren und C-ITS Verkehrssysteme in Österreich".

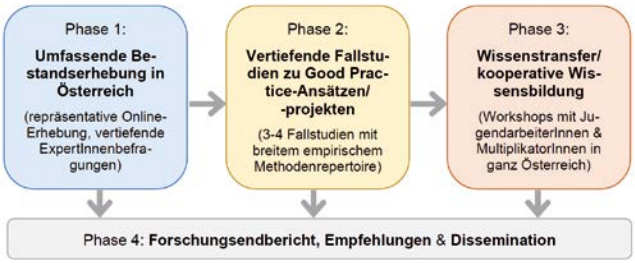
Projektleitung
AIT – Austrian Institute of Technology GmbH
Digital Safety and Security Department

Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- Donau Universität Krems
- Kuratorium Sicheres Österreich

Kontakt
Dr. Zhendong Ma
AIT – Austrian Institute of Technology GmbH
Digital Safety and Security Department
Donau-City-Straße 1, 1220 Wien
Tel.: +43 664 6207839
E-Mail: zhendong.ma@ait.ac.at
www.ait.ac.at/dss

E-YOUTH.works

Offene Jugendarbeit in und mit neuen Medien als Schutzmaßnahme gegen radikalisierende Internetpropaganda



Projektphasen der Studie E-YOUTH.works

Ausgangslage, Problematik und Motivation

Jugendliche sind eine besonders vulnerable Zielgruppe von über Internet und neue Medien verbreiteter extremistischer Propaganda. Sie weisen einerseits eine höhere Empfänglichkeit für radikale Positionen und Gruppen auf, diese Medien spielen andererseits eine essenzielle Rolle in ihrem Leben und bei der Identitätsentwicklung im Heranwachsen. Für einen adäquaten und wirksamen Schutz junger Menschen sind nicht nur Instrumente zur Eindämmung extremistischer Internetpropaganda notwendig, sondern ist vor allem auch medienbezogene sozialpädagogische Präventions- und Deradikalisierungsarbeit erforderlich. Diese muss zugleich in der Lage sein, auch Jugendliche mit geringen ökonomischen, kulturellen und sozialen Ressourcen zu erreichen.

Internet- und medienbezogene Interventionen Offener Jugendarbeit (= e-youth work) bieten hierfür einen besonders vielversprechenden Ansatz an, da sie durch die Verbindung von Online- mit Offline-Interventionen auf Basis persönlicher Vertrauensbeziehungen kritisch-reflexive Medienkompetenz stärken und junge Menschen zu konstruktiv-partizipativem Medienhandeln befähigen können. Offene Jugendarbeit realisiert durch eine niederschwellige Arbeitsweise zugleich Zugänge zu grundsätzlich schwer erreichbaren, aber hoch relevanten AdressatInnengruppen für präventive (Medien-) Interventionen. Allerdings kommt e-youth work gegenwärtig in Österreich nur wenig systematisch zum Einsatz, es besteht beachtlicher professioneller Reflexions- und Entwicklungsbedarf. Zugleich fehlt es an wissenschaftlicher Forschung in diesem Handlungsfeld Offener Jugendarbeit.

Ziele und Innovationsgehalt:

Das Forschungsprojekt verfolgt die Zielsetzung,

- evidenzbasiertes Wissen über den Einsatz, die Arbeitsweisen und Wirkmöglichkeiten von e-youth work mit speziellem Fokus auf medienbezogene Radikalisierungsprävention zu generieren, um eine professionelle Praxis Offener Jugendarbeit zu fördern.
- Das Forschungsvorhaben greift einen großen Entwicklungsbedarf in der Offenen Jugendarbeit zur stärkeren und vielfältigeren Nutzung neuer Medien für nachhaltige Schutzstrategien gegen extremistische Internetpropaganda auf und bindet hierfür maßgebliche nationale Akteure als Projektpartner ein.

Methodisches Vorgehen & angestrebte Ergebnisse

Die methodische Umsetzung des Forschungsprojekts gliedert sich in vier aufeinander aufbauende Phasen, wobei Phase 1 und 2 die zentralen Forschungsphasen darstellen:

1. Repräsentative Forschungsergebnisse über vorhandenes Knowhow sowie konkrete Schulungs- und Entwicklungsbedarfe bzgl. e-youth work zur Radikalisierungsprävention. Folgende Inhalte werden u.a. in einer aktuell laufenden österreichweiten Online-Umfrage unter Einrichtungen Offener Jugendarbeit erhoben:
   - die mediale Ausstattung der Einrichtungen und Praktiken der Mediennutzung der JugendarbeiterInnen in der Offenen Jugendarbeit
   - vorhandenes und fehlendes Knowhow bzw. Ressourcen für onlinebasierte Jugendarbeit
   - Praktiken der Mediennutzung jugendlicher NutzerInnen der Einrichtungen Offener Jugendarbeit
   - eventuelle Berührungspunkte dieser Jugendlichen zu extremistischen/radikalisierenden Inhalten und daraus folgende medienpädagogische Interventionen
   - Online- bzw. Social Media-Regelungen in der Einrichtung
2. Vertiefende Erkenntnisse über innovative Good Practice-Ansätze (mit Bezug zu extremistischer Online-Propaganda), ihre Arbeitsformen, Beziehungsqualität und Wirkweisen. Die in den Fallstudien zu untersuchenden Projekte bzw. Arbeitsansätze werden auf Basis der in Phase 1 gewonnenen Einblicke ausgewählt.
3. Workshops zur kooperativen Wissensbildung mit Professionellen und relevanten Stakeholdern der Jugendarbeit, Jugend- und Sicherheitspolitik etc. zur praxiswirksamen Rückkopplung der Erkenntnisse.
4. Guideline für PraktikerInnen: e-youth work als Instrument zur Radikalisierungsprävention & Deradikalisierung; Katalog mit Maßnahmenempfehlungen für Träger Offener Jugendarbeit, die Aus- und Weiterbildung sowie die Jugend- und Sicherheitspolitik in Österreich.

Projektleitung
IRKS – Institut für Rechts- und Kriminalsoziologie

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Familien und Jugend
- bOJA – Bundesweites Netzwerk Offene Jugendarbeit
- VJZ – Verein Wiener Jugendzentren

Kontakt
Mag. Dr. Hemma Mayrhofer
IRKS – Institut für Rechts- und Kriminalsoziologie
Museumstraße 5/12, 1070 Wien
Tel.: +43 1 526 15 16-20
E-Mail: hemma.mayrhofer@irks.at
www.irks.at

EBeCa

Evaluation & Begleitung der Einführung von Body Worn Cameras

Das Projekt EBeCa „Evaluation & Begleitung der Einführung von Body Worn Cameras. Resonanzanalyse, Wahrnehmung, Begleitmaßnahmen und Empfehlungen" gewährleistete im Zeitraum 01. Oktober 2015 bis 31. Dezember 2016 die sozialwissenschaftliche, kommunikative und frühzeitige Begleitung und Unterstützung der testweisen Verwendung von Köperkameras bei der österreichischen Polizei.

Body Worn Cameras (BWCs) werden seit mehr als zehn Jahren z. B. in Großbritannien, Deutschland oder den USA im polizeilichen Einsatz getestet und angewandt. Der steigende Anspruch an immer höhere Transparenz und bessere Dokumentation von Amtshandlungen befürworten den zukünftigen, ausgerollten Einsatz von BWCs bei Exekutivbediensteten (EB) in Österreich.

EBeCa geht von einer umfassenden internationalen Bestandsaufnahme mit SWOT-Analyse und Szenario-Technik aus. Zur Bildung einer Evidenzbasis sowie zur Erhebung von Erfahrungswerten beim Testeinsatz von BWCs wurden zwei groß angelegte qualitative und quantitative Befragungszyklen durchgeführt, welche die Sicht aller drei identifizierten Stakeholder-Gruppen (Exekutivbedienstete, polizeiliche Führungsebene und Bevölkerung) beleuchten. Für die Praxisrelevanz wurden zum Einsatz von BWCs drei Test-Fälle narrativ sowie qualitativ ausgearbeitet. Unterschiedliche Rahmenbedingungen beziehen sich auf mögliche, typische Einsatzszenarien der Polizei (z. B. Großveranstaltung, im Streifendienst und im Fall von häuslicher Gewalt).

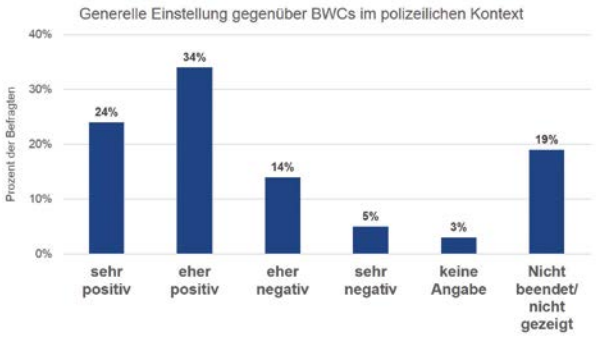
Die Vorerhebung zeigte bei allen Stakeholder-Gruppen eine überwiegend positive Einstellung gegenüber der Verwendung von BWCs. Faktoren, die bei der Technologieakzeptanzanalyse bedeutend sind, wie Offenheit, Neugier, Technikerfahrung, erwarteter Nutzen und erwartete Einfachheit der Anwendung, haben sich bei den Befragten eher positiv abgezeichnet. Die wesentlichste Stärke von BWCs wird von allen befragten Gruppen vor allem im Schutz der handelnden Personen vor ungerechtfertigter Behandlung bzw. Beschuldigung gesehen.

Dennoch fühlt sich ein Teil der direkt betroffenen Berufsgruppe der Exekutivbediensteten sowie die breite Bevölkerung im Hinblick auf Prozesse oder genaue Abläufe des Einsatzes von BWCs wenig informiert. Mit dem zusätzlichen, starken Faktor der Kostenfrage und der Befürchtung der totalen Überwachung durch den Staat wird auch die Befürchtung einer Beliebigkeit des Datenmiss- bzw. -gebrauches und der Überforderung der Einsatzkräfte erwähnt. Die Führungskräfte andererseits sehen neben diesem letzten wesentlichen Gesichtspunkt die Schwächen eher im technischen Bereich (z. B. Bildqualität, Perspektiveneinschränkung).

Während der Testphase wurden durch die Befragten die vorher erhobenen Stärken von BWCs deutlich unterstrichen und bestätigt: Schutz der EB, Objektivierung, Nachvollziehbarkeit, Beweisführung, Prävention von Gewalt, Signalwirkung und Transparenz. Berichtet wurde ebenfalls, dass das Deeskalationspotenzial im Einsatz von BWCs höher als erwartet ausfiel. Zu den angegeben Schwächen zählen unter anderem die Unklarheit über den Aktivierungszeitpunkt, die Verunsicherung der EB (Gefühl der Überwachung) und der erhöhte Verwaltungs- und Administrationsaufwand. Die Stakeholder weisen darauf hin, dass u.a. Schulungen, Rechtssicherheit, Nutzungsfreundlichkeit sowie leichte Handhabung im Umgang mit der BWC-Technologie wesentliche Voraussetzungen für den erfolgreichen Einsatz von BWCs in der österreichischen polizeilichen Praxis sind.

Body Worn Cameras im österreichischen Polizeikontext.
Quelle: Copyright BM.I: Alexander Tuma

Szenarien zum Einsatz von Body Worn Cameras.
Quelle: Eigendarstellung AEI



„Wie sind Sie generell der Verwendung von BWCs im polizeilichen Kontext gegenüber eingestellt?" Quelle: Eigendarstellung AEI

Die Begleitstudie EBeCa trägt durch die Anwendung eines transdisziplinären und multidimensionalen, in der Praxis fundierten Zuganges in verschiedenen Beteiligtengruppen zu einem umfassenden Wissen zur Einführung von BWCs bei der Exekutive bei.

Die generell positive Einstellung aller Stakeholder-Gruppen der BWC-Technologie gegenüber kann als Herausforderung wie auch als großes Potenzial für die Weiterentwicklung der Nutzung und Akzeptanz des Systems betrachtet werden. Wird diese generell positive Einstellung konstruktiv genutzt und kommunikativ mit offener und transparenter Information unterstützt, können künftig auch systemisch gegebene Erfordernisse im Hinblick auf die zu erwartenden positiven Gesamteffekte erfüllt werden.

Die Testung und Einführung der BWCs in den Exekutivdienst können als eine umfassende Thematik angesehen werden, die sowohl systemische und soziale Aspekte, Prozesse, Hard- und Software als auch Informationsarbeit und Rechtssicherheit für ein reibungsloses Ablaufen voraussetzt.

Projektleitung
AEI – Agentur für Europäische Integration und wirtschaftliche Entwicklung

Projektpartner
- Bundesministerium für Inneres

Kontakt
MMag. Dr. Karin Rainer
AEI – Agentur für Europäische Integration und wirtschaftliche Entwicklung
Bräunerstraße 11A, 1010 Wien
Telefon: +43 1 9054621 12
E-Mail: karin.rainer@aei.at
www.aei.at

FlashBang

In-situ Risikobeurteilung der akustischen Wirkung von Blendgranaten

Einspannvorrichtung für das kontrollierte Auslösen von Blendgranaten für das standardisierte Messverfahren

Die Entwicklung und Erprobung Nicht-letaler Wirkmittel (NLW) wird bereits seit den späten 1960er Jahren vorangetrieben. In das breite Licht der Öffentlichkeit rückten dieser aber erst etwa 1990. Seit damals kann ein Trend zu neuen Arten von NLW beobachtet werden, der dem Militär als auch den Sicherheitskräften wie Polizei und Justizwache neue Möglichkeiten in der Bewältigung Ihrer Aufgaben eröffnet.

Der Ruf nach Verhältnismäßigkeit und die starke Präsenz der Medien zwingen Sicherheitskräfte heutzutage, speziell im urbanen Umfeld angepasst vorzugehen und dabei möglichst geringe Folgeschäden zu verursachen. Dabei helfen Ihnen Nicht-letale Wirkmittel, die – wie ihr Name schon sagt – bei richtigem Einsatz nicht tödlich wirken.

Das Risiko unbeabsichtigter Wirkungen ist derzeit jedoch nicht auszuschließen, da die Untersuchungen der Wirkungsweisen von NLW nur rudimentär sind. Problematisch ist dabei, dass bis dato keine standardisierten Messverfahren zur Erstellung von Spezifikationen existieren. Speziell die Wirkungen beim Einsatz von sogenannten Blendgranaten (engl. auch flash-bang oder stun grenades genannt) sind nur sehr unzureichend untersucht. Dadurch kommen Einsatzkräfte vorort immer wieder in die Lage, das Gebot der Verhältnismäßigkeit bzw. der Diskriminierung nicht entsprechend einschätzen zu können, wodurch Dritten Leid zugefügt werden kann und z. B. Kollateralschäden entstehen. Daraus folgt für Einsatzkräfte eine Rechtsunsicherheit, wodurch weitere rechtliche Folgen wie Schadenersatzansprüche etc. unvermeidbar sind.

Ziel der Studie ist es, die akustische Wirkung von Blendgranaten beim Einsatz im Freien und in Räumen zu untersuchen und weiters die Grundlagen für ein Simulationswerkzeug zu schaffen, das es Einsatzkräften erlaubt, die akustische Wirkung einer Blendgranate auf Menschen in-situ vor dem Gebrauch abzuschätzen.

Im ersten Schritt wurde ein standardisiertes Messverfahren zur schalltechnischen Vermessung von Blendgranaten entwickelt. In der Literatur wie auch in den Spezifikationen der Hersteller ist meist der Schalldruckpegel angeführt. Im Rahmen des Projekts wurde aus physikalischen Gründen der Schallleistungspegel zur schalltechnischen Charakterisierung untersucht und eingeführt. Die Schallleistung bzw. der Schallleistungspegel Lw ist für eine Schallquelle die kennzeichnende schalltechnische Größe. Im Gegensatz zum Schalldruckpegel Lp ist der Schallleistungspegel Lw vollkommen unabhängig vom Schallfeld, also von der Größe und Form des Messraumes und der Entfernung zur Quelle. Die Schallleistung beschreibt somit die gesamte wirkliche Schallenergie, die von einer Schallquelle abgegeben wird.

Weiters wurden Spezifikationen für einen standardisierten Messplatz erstellt und gemeinsam mit dem BMLVS Begehungen durchgeführt, um potenzielle Areale zu finden. Daraus hat sich ergeben, dass ideale Voraussetzungen am Fliegerhorst Hinterstoisser und am Schießplatz Felixdorf vorliegen. Diese beiden Messorte werden daher auch für die standardisierten Messungen genützt.

Als Sensoren kommen spezielle Messmikrofone, die auf hohe Schalldruckpegel ausgelegt sind, sowie spezielle Prüfspitzen in Frage. Mit beiden Sensorarten wurden Untersuchungen durchgeführt. Im Zuge einer Evaluation wurden verschiedene Sensoren mit verschiedenen Messsystemen aufgezeichnet und auf deren Eignung und Robustheit getestet.

Um eine Datenbasis für die Entwicklung der Simulation zu generieren, wurden umfangreiche Messungen mit verschiedenen Blendgranaten durchgeführt.

Im nächsten Schritt soll untersucht werden, wie ein Gerät und dessen Benutzerschnittstelle für Einsatzkräfte beschaffen sein muss, damit dies im realen Einsatz verwendet werden kann und im Krisenfall auch klare Vorteile für die Einsatzkräfte bringt. Abschließend sollen die Berechnungsalgorithmen und das Gerät in einem umfangreichen Test evaluiert und so weitere Erkenntnisse für den realen Einsatz gewonnen werden.

Schematische Darstellung des Demonstrators mit der Grafischen Benutzeroberfläche auf einem feldtauglichen Tablet

Projektleitung
JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner
- Bundesministerium für Landesverteidigung und Sport

Kontakt
DI Dr. Franz Graf
JOANNEUM RESEARCH
Forschungsgesellschaft mbH
Steyrergasse 17, 8010 Graz
Tel: +43 316 876 1631
Email: franz.graf@joanneum.at
www.joanneum.at

MOMA

Modernes Management im Polizeianhaltewesen: Safe & Healthy Prisons

Das Projekt MOMA untersucht Polizeianhaltezentren (PAZ) bzw. Anhaltezentren (AHZ) und liefert damit Einsichten in ein bislang wenig erforschtes Feld der Sicherheitsforschung. Gegenwärtig drängende Fragen, wie Schubhaft oder Flüchtlingsbewegungen, laufen im Polizeianhaltewesen zusammen, das auch mit der Organisation der Verwaltungs- und Verwahrungshaft vielseitig herausgefordert ist. Um auf aktuelle Fragen angemessen antworten zu können, braucht es umfassendes Wissen. Das Projekt MOMA greift hier eine Lücke auf und liefert wissenschaftlich abgesicherte Informationen zum Anhaltewesen sowie Innenansichten der PAZ/AHZ.

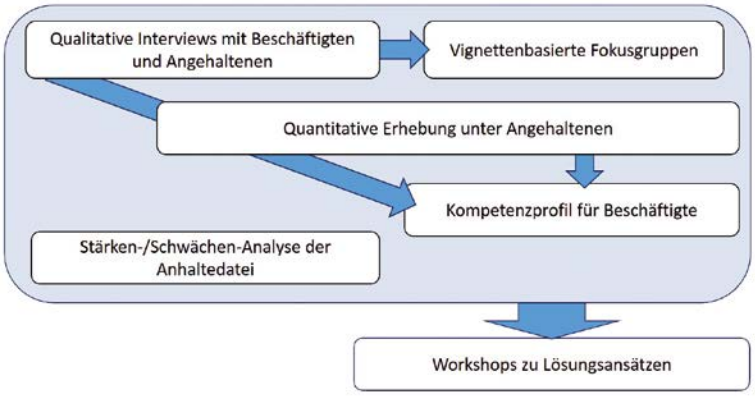
MOMA arbeitet mit einem multimethodischen und lösungsorientierten Forschungsansatz. Die enge Zusammenarbeit mit dem Bedarfsträger ist dabei richtungsweisend. Der Bedarfsträger wird partizipativ in den Forschungsprozess eingebunden. Instrumente und Ergebnisse der Forschung werden in Feedbackschleifen auf die tatsächlichen Erfordernisse und die Anwendbarkeit in PAZ/AHZ abgestimmt. Das partizipative und lösungsorientierte Vorgehen stellt sicher, dass MOMA dem Bedarfsträger konkrete Instrumente in die Hand gibt, die für ein zeitgemäßes Management im Anhaltewesen zielführend sind.

Folgende Forschungsprodukte erarbeitet das Projekt:

- Wissenschaftlich abgesichertes Wissen zur sozialen und gesundheitlichen Situation von Beschäftigten und Angehaltenen sowie zu organisationalen und strukturellen Bedingungen in PAZ/AHZ; diese Informationen werden mittels qualitativer Interviews mit Beschäftigten und Angehaltenen in vier unterschiedlichen PAZ/AHZ erstellt.
- Statistische Daten zu Lebenslage und Lebenssituation der Angehaltenen, die in einer Fragebogenumfrage unter Angehaltenen erhoben werden.
- PAZ-/AHZ-typische Vignetten, die in vignettenbasierten Fokusgruppendiskussionen spezifische Perspektiven situationsrelevanter AkteurInnen ausdifferenzieren und Zugang zu Problembereichen und Lösungsansätzen liefern; hier wird gleichzeitig ein Methodeninstrument getestet und weiterentwickelt, das vom forschungsleitenden Netzwerk für die Sicherheitsforschung konzipiert wurde.
- Ein Kompetenzprofil, das Fertigkeiten, Fähigkeiten und Wissensbestände darstellt, die Beschäftigte in PAZ/AHZ benötigen und das basierend auf den qualitativen und quantitativen Ergebnissen in Entwicklungsgesprächen erarbeitet wird.
- Einen Fahrplan für die Reformierung der Anhaltedatei durch eine Stärken-/Schwächen-Analyse der bestehenden Datensätze und ihrer Anwendung.
- Einen Lösungsatlas zu identifizierten Problembereichen der AHZ/PAZ, der in der partizipativen Diskussion mit Bedarfsträger und ExpertInnen entwickelt wird.

Die Arbeitsschritte des Projekts sind so gewählt, dass die Perspektive der Beschäftigten und die Perspektive der Angehaltenen berücksichtigt werden. Im Projektverlauf werden die unterschiedlichen Sichtweisen zu einer ganzheitlichen zusammengeführt. Durch den multiperspektivischen Zugang liefert MOMA eine Grundlage für ein modernes Management, das die Grundrechte und Unversehrtheit der involvierten Personen gewährleisten kann.

Das Projekt ist darüber hinaus für die Aus- und Weiterbildung wirksam. Das Kompetenzprofil fließt direkt in die im Umbau befindliche Ausbildung von Beschäftigten der PAZ ein. Situationsvignetten und der Lösungsatlas können als Schulungsmaterial verwendet werden.



Projektleitung
WU Wien, Kompetenzzentrum für empirische Forschungsmethoden

Projektpartner
- Bundesministerium für Inneres
- queraum. kultur- und sozialforschung
- Institut für Rechts- und Kriminalsoziologie IRK

Kontakt
Dr[in] Katharina Miko-Schefzig
WU Wien, Kompetenzzentrum für empirische Forschungsmethoden
Welthandelsplatz 1, 1020 Wien
Tel.: +43 1 31336 5319
katharina.miko-schefzig@wu.ac.at

FSAA-NLW

Feasibility Study für alternative Antriebstechniken im Bereich „Non Lethal Weapon Systems" (Nicht-letale Waffensysteme)

Systeme mit chemischer Antriebstechnik (SKILL-Prototyp, NATO Testvorrichtung), mit mechanischer Antriebstechnik (Harpune) und pneumatischer Antriebstechnik (Herstal FN 303, VAUST System)

Basierend auf den Ergebnissen der Entwicklungen im KIRAS-Projekt SKILL (Soft Kinetic Impact Less Lethal) und dort offen gebliebenen Fragestellungen in Bezug auf Effizienz und Maßhaltigkeit beim Einsatz von Einsatzorganisationen zum Schutze der Bürger, wird im Rahmen von FSAA-NLW eine Feasibility Study über Alternative Antriebstechniken für Nicht-letale Waffensysteme mit kinetischer Wirkung durchgeführt. Dazu wird ein Kriterienkatalog für Qualitätsanforderungen festgelegt, um die Selbstgefährdung und Gefährdung von beteiligten Personen bei der Erfüllung der Aufgaben der Einsatzkräfte zu minimieren. Die Problemstellung ergibt sich aus dem Bedarf der Entwicklung eines Nicht-letalen Waffensystems für den Einsatz durch das Militär oder die Exekutive mit ausreichend guter Regelung der Energie im Wirkungsbereich von 70 bis zu 140 Joule (J). Die Auftreffenergie soll zwischen 10 m und 100 m mit sehr guter Trefferlage zur gezielten Schonung Nichtbetroffener erreicht werden können.

Das Design des verwendeten Geschosses ist wesentlich für die letale oder weniger letale Wirkung ausschlaggebend. So ist zum Beispiel bei Weichgummigeschoßen die reduzierte Letalität auch noch bei 100 J – 140 J gegeben. Daher werden unterschiedliche Geschosstypen mit regelbaren Systemen basierend auf chemischer und pneumatischer Antriebstechnik untersucht. Als Ergebnis werden der Geschwindigkeitsverlauf und die Energie über die Einsatzreichweite von bis zu 100 m anhand von erarbeiteten Qualitätskriterien beurteilt.

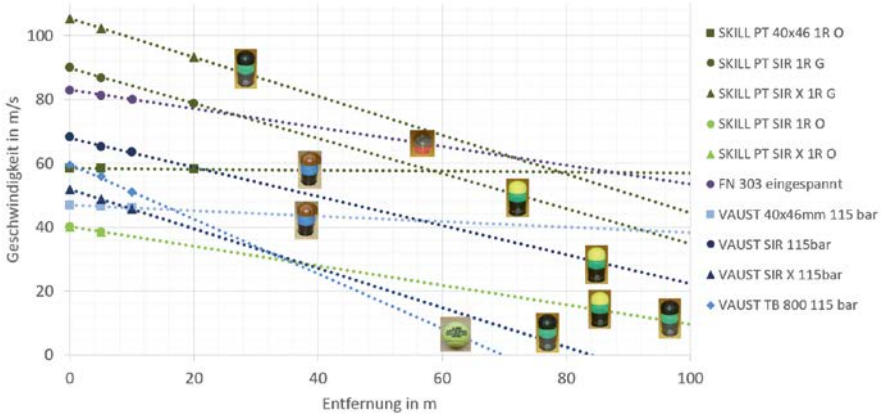
Die Recherche umfasst am Markt befindliche Wirksysteme zur Verbringung von Wirkkörpern auf kinetischer Wirkbasis und eine Patentrecherche über nicht bzw. wenig letale Waffensysteme. Außerdem werden Antriebe wie das Paintball-System, der Aerosolantrieb einer Kartoffelkanone, der Leichtgasantrieb, der elektromagnetische Antrieb einer Rail-Gun etc. betrachtet und deren Einsatz für den nicht-letalen Bereich bewertet. Basierend auf Recherche und Ideenfindung werden

- das Antriebsprinzip chemische Energieträger mit dem SKILL-Prototypen (entwickelt im SKILL-Projekt),
- das Antriebsprinzip mechanische Energieträger mit einer Harpune und
- das Antriebsprinzip Druckluft mit dem VAUST-System (Ventile und Fittings Austria) und mit dem System HERSTAL FN303 (Fabrik National)

experimentell mit unterschiedlichen Geschossen (40 mm- bzw. 32 mm-Geschosse, Tennisbälle, Harpunenpfeil und Bismutgeschosse) untersucht. Für die Bewertung der Systeme wird die Geschwindigkeit an drei Stellen und die Treffpunktlage herangezogen.

Die Ergebnisse der Studie zeigen, dass die Flugbahn der 40 mm-Geschosse mit chemischem Antrieb stabiler ist als mit pneumatischem Antrieb. Zusätzlich zeigen die 40 mm Safe Impact Round-Geschosse ohne Treibladung die konstantesten Trajektorien bei der Beschleunigung mit dem pneumatischen VAUST-System.
Die Untersuchungen zeigen daher großes Entwicklungspotential für den Einsatz dieser Geschosse mit pneumatischem Antrieb. Das VAUST-System ist außerdem sehr genau regelbar, wodurch die Austrittsgeschwindigkeit und damit die Energie nach Bedarf definiert werden kann.

Die Auswertung der Versuchsreihen mit chemischer Antriebstechnik mit den drei getesteten Systemen ergibt für die 40 mm-Geschosse ein regelbares Geschwindigkeitsfenster von 105 m/s bis 40 m/s. Da ein wesentlicher Einfluss auf das Flugverhalten in der Wahl des Geschosses liegt, sind leichte Geschosse eher



Ballistisches Verhalten auf eine Entfernung von 100 m Flugbahn, Auftreffenergie und Energiedichte für die untersuchten Systeme abhängig von der Geschwindigkeit

für den Einsatz bis zu 40 m und schwerere bis zu 100 m geeignet. Die Grafik oben zeigt die extrapolierten Geschwindigkeiten über die Entfernung von 0 m – 100 m. Den geforderten Energiebereich zwischen 70 J und 140 J erreichen der SKILL-Prototyp (SKILL PT) durch die Regelung des Gasdrucks mit den 40 mm-Geschossen SIR und SIR-X und das VAUST-System mit den Geschossen SIR, SIR-X und den Tennisbällen. Dabei ist zu beachten, dass der Energieabfall bei den Messungen mit chemischem Antrieb (SIR und SIR-X) nicht so steil ausfällt wie bei den Messungen mit pneumatischem Antrieb. Allerdings könnte bei letzterem die Energie durch eine weitere Erhöhung des Drucks gesteigert werden.

Zusammenfassend bilden die beiden regelbaren System SKILL-Prototyp mit chemischem Antrieb und VAUST-System mit pneumatischen Antrieb eine gute Grundlage zur Entwicklung eines Waffensystems für den nicht bzw. wenig letalen Einsatz. Der Regelbereich ist bei beiden Systemen groß genug, aber vom verwendeten Geschoss abhängig. Zusätzlich zur Entwicklung des Systems ist auch eine Entwicklung am Geschoss eine Grundlage für die Sicherstellung der Regelbarkeit im geforderten Einsatz- und Energiebereich, wobei Geschossform und Geschossverformbarkeit für die tatsächliche Energiedichte beim Auftreffen des Geschosses den Regelbereich wesentlich mitbeeinflussen können.

Projektleitung
SciReAs Scientific Research Association
Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- Bundesministerium für Inneres

Kontakt
Prof. Dipl.-Ing. Dr.mont. Monika Grasser
Prof. Dipl.-Ing. Ing. Florian Mayer
SciReAs Scientific Research Association
Schulhausgasse 10, A-9170 Ferlach
Tel.: +43 664 1954021
E-Mail: monika.grasser@scireas.org,
florian.mayer@scireas.org
www.scireas.org

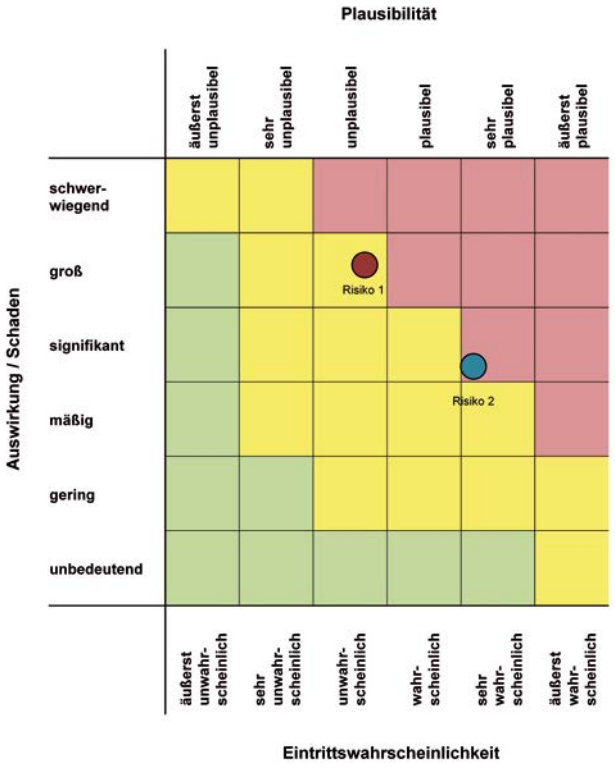
GeRiAn

Gesamtstaatliche Risikoanalyse

Im Jahr 2013 wurde von der Europäischen Kommission in der Decision 2013/1313/EC der „Union Civil Protection Mechanism" beschrieben, welcher eine gesamtstaatliche Risikoanalyse in den Mitgliedsstaaten vorsieht. Diese Risikoanalyse soll auf das Gefahren- und Bedrohungsspektrum zugeschnitten sein, mit dem sich Staaten aktuell konfrontiert sehen. Die Studie GeRiAn beschreibt einen Ansatz für eine nationale Risiko- und Bedrohungsanalyse in Österreich, welcher bereits bei den Ministerien bestehende Methoden integriert und deren Ergebnisse auf einem höheren Abstraktionslevel zu einem einheitlichen sicherheitspolitischen Lagebild zusammenfasst.

Aufgrund der zunehmenden und komplexer werdenden Vernetzung der heutigen Gesellschaft, der steigenden Abhängigkeit von kritischen Infrastrukturen sowie der wachsenden Bevölkerung und Bevölkerungsdichte verursachen Katastrophen immer größere Schäden. Darunter fallen klassische Bedrohungen wie Naturkatastrophen als Folge des Klimawandels oder Umweltschäden aber auch neuartige Bedrohungen wie etwa Cyber-Attacken, internationaler Terrorismus, politische Veränderungen in Staaten oder die Auswirkungen der Finanz- und Wirtschaftskrise. Die Vorbereitung auf deren Bewältigung wird daher zu einer immer wichtigeren Aufgabe.

Ein geeignetes Mittel hierfür stellt eine gesamtstaatliche Risiko- und Bedrohungsanalyse dar. Sie bildet eine wichtige Grundlage für die vorsorgliche Planung zum Schutz der Bevölkerung auf allen staatlichen Ebenen. Sie hilft, mögliche Gefährdungen besser zu verstehen, Maßnahmen der Prävention und Vorsorge aufeinander abzustimmen, Prioritäten bei der Vorbereitung zu setzen und Defizite in der Bewältigung zu erkennen.



Schematische Darstellung einer Risikomatrix als Basis für eine gesamtstaatliche Risikoanalyse

Somit wird auf Basis der gesamtstaatlichen Risiko- und Bedrohungsanalyse ein tieferes Verständnis über die Dynamik von Ereignissen sowie über deren Auswirkungen geschaffen. Vor allem bei der Vorbereitung auf die Bewältigung dieser Ereignisse stellt dieses Verständnis einen zentralen Erfolgsfaktor dar, da die Bewältigung eine enge Zusammenarbeit zwischen den verantwortlichen Stellen auf Bundes- und Landesebene sowie mit Dritten erfordert.

Sowohl im Bereich der Risikoanalyse als auch im Bereich der Bewältigung von Katastrophen existieren in den einzelnen Sektoren der Bedarfsträger (BKA, BM.I, BMLVS) auf Bundes- und auf Landesebene bereits spezifische Ansätze und Methoden. Allerdings ist noch keine einheitliche, gesamtstaatliche Lösung existent, welche die einzelnen Methoden integriert. Im Detail ist man auf einer gesamtstaatlichen sicherheitspolitischen Ebene mit dem Problem konfrontiert, dass die bestehenden Konzepte und Methoden in ihren Inputs

und Outputs sehr unterschiedlich definiert sind. Dies macht einen direkten Vergleich der Ergebnisse von Risikoanalysen aus den unterschiedlichen Sektoren sehr schwierig, zudem diese Resultate auch nicht einheitlich darstellbar sind.

Ziel der Studie GeRiAn ist daher die Definition von Methoden und Konzepten für eine derartige Risikoanalyse auf nationaler Ebene. Nachdem auf Bundes- und Landesebene bereits Ansätze und Methoden im Bereich der Risikoanalyse und der Risikobewältigung existieren, liegt das Hauptaugenmerk der Studie auf der Identifikation von Integrationsmöglichkeiten dieser bestehenden Ansätze in eine gesamtstaatliche Risikoanalyse. Dabei wurden speziell die Bereiche des staatlichen Krisen- und Katastrophenschutzmanagements (SKKM), des Schutzes kritischer Infrastrukturen (SKI) sowie der Cyber-Sicherheit betrachtet. In enger Kooperation mit den Bedarfsträgern wurden die bestehenden Methoden analysiert und Berührungspunkte abgeleitet, welche in die nationale Risikoanalysemethode einfließen können. Die Studie liefert somit eine „Toolbox" für eine gesamtstaatliche Risiko- und Bedrohungsanalyse in Form von generischen Beschreibungen besonders geeignet erscheinender und bereits eingesetzter „Methoden-Cluster".

Ein weiterer Fokus der Studie ist die Identifikation von Aggregationsmöglichkeiten der Ergebnisse aus den Risikoanalysen der einzelnen Sektoren. Dadurch wird sichergestellt, dass eine konsistente Darstellung der Ergebnisse auf einem höheren Abstraktionslevel möglich ist. Dies dient der Erstellung eines einheitlichen sicherheitspolitischen Lagebildes. Beim Aufbau einer gesamtstaatlichen Risiko- und Bedrohungsanalyse kann aufbauend auf den Ergebnissen der Studie ein Raster entwickelt werden, in dem bestimmte „Methoden-Cluster" gewissen Analysefeldern zugeordnet werden. Damit entsteht eine leicht handhabbare „Gebrauchsanweisung" für die praktische Umsetzung.

Im Allgemeinen wird auf Basis der gesamtstaatlichen Risiko- und Bedrohungsanalyse ein tieferes Verständnis über die Dynamik von Ereignissen sowie über deren Auswirkungen geschaffen. Vor allem bei der Vorbereitung auf die Bewältigung dieser Ereignisse stellt dieses Verständnis einen zentralen Erfolgsfaktor dar, da die Bewältigung eine enge Zusammenarbeit zwischen den verantwortlichen Stellen auf Bundes- und Landesebene sowie mit Dritten erfordert.

Bei einer gesamtstaatlichen Risikoanalyse gilt es daher, die unterschiedlichen Inputs der einzelnen Sektoren in einer einheitlichen Methode zusammenzufassen. Diese ermöglicht es, eine Darstellung der Auswirkungen in einer zentralen Form sowie einen Überblick über alle möglichen Auswirkungen für eine Anzahl an betrachteten Bedrohungsszenarios zu geben.

Durch die Vielzahl an bereits bestehenden Konzepten und Methoden stellt sich die Integration in eine derartige gesamtstaatliche Risikoanalyse als ein komplexer Prozess dar. Deshalb bildet die Definition von potentiellen Ansätzen und die Formulierung von Empfehlungen für diese Integration in einen einheitlichen Risikoanalyseprozess ein Hauptziel dieser Studie. Die praktische Umsetzung dieser Empfehlung mit dem Ziel des Aufbaus einer gesamtstaatlichen Risiko- und Bedrohungsanalyse obliegt den Bedarfsträgern.

Projektleitung
AIT – Austrian Institute of Technology GmbH
Projektpartner
- Bundeskanzleramt
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport

Kontakt
Dipl.-Ing. Dr. Stefan Schauer
AIT – Austrian Institute of Technology GmbH
Lakeside B10a, 9020 Klagenfurt
Tel.: +43 50 550 4055
E-Mail: stefan.schauer@ait.ac.at
www.ait.ac.at

IMOPOL+

iMobility und Polizei: Technologien, Konzepte und Lösungen im Kontext sicherheitsrelevanter Einsatzszenarien

Ziele des Projekts IMOPOL+ waren
- die Themenfeldexploration, Bedarfsträgerbefragung und Anforderungsanalyse im Bereich iMobility,
- die Erfassung und Analyse von iMobility-Software und -Hardware sowie
- die Vernetzung, Wissensaggregation und Strategieentwicklung.

IMOPOL+ nutzte einen breiten Ansatz zum Erreichen der Projektziele: Basierend auf der Grundlagen- und Umfelderhebung für iMobility im polizeilichen Kontext, wurden technische Lösungen analysiert und ein neuartiges Kategorisierungssystem entwickelt. Des Weiteren wurden relevante iMobility-Stakeholder betrachtet. Darauf aufbauend wurde mittels Szenario-Entwicklungsprozess eine Aufbereitung der Herausforderungen und Chancen für die Bedarfsträger erreicht, die spezifisch die Kommunikation der Erkenntnisse nach Informationsbedürfnissen ermittelt. Die Priorisierung der iMobility-Einsatzszenarien im polizeilichen Kontext durch die Bedarfsträger trieb die Aufbereitung und Analyse weiter voran. Parallel zu allen Aktivitäten wurden in regelmäßigen Abständen die Perspektive und das Wissen der Bedarfsträger in die Projektergebnisse eingearbeitet, etwa durch Workshops, Interviews und regelmäßige bi-direktionale Kommunikation. Das Vorhaben wurde durch effektives und effizientes Projektmanagement begleitet.

Kernergebnisse von IMOPOL+ umfassen eine grundlegende Analyse und Exploration von iMobility im polizeilichen Kontext, eine Strukturierung der iMobility-Landschaft in acht Themenfelder, die Identifikation und Beschreibung von Kommunikationspfaden zwischen relevanten Akteuren sowie die Entwicklung 25 neuartiger Einsatzszenarien für iMobility im polizeilichen Kontext. Des Weiteren wurden rechtliche Fragestellungen identifiziert und ein Ausblick auf zukünftige Entwicklungen geboten. Sämtliche Ergebnisse zeichnen sich einerseits durch eine hohe Verwertbarkeit für die Bedarfsträger und Forschungspartner und andererseits durch das Erreichen eines internationalen Publikums aus. Dies ist auch auf die umfangreichen Tätigkeiten des Konsortiums im Projekt zur Kommunikation und Dissemination der Ergebnisse zurückzuführen.

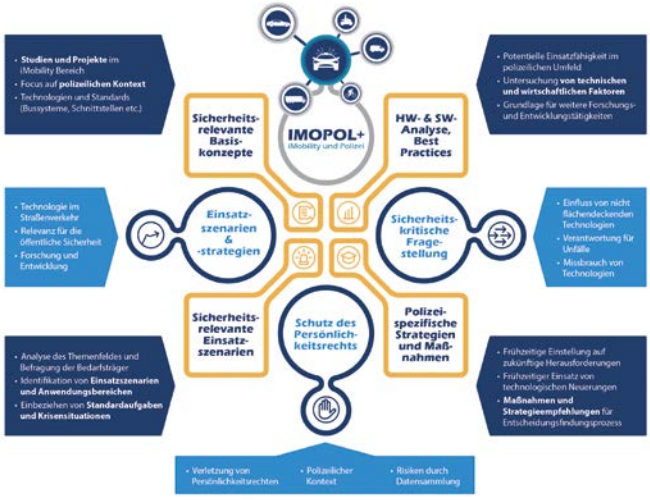
Durch eine Exploration von iMobility-Grundlagen im polizeilichen Kontext und eine Analyse des Umfeldes wurde der Ausgangspunkt für alle nachfolgenden Analysen und Entwicklungen im Projekt geschaffen. Ein Überblick über aktuelle Themen, Trends, Standards und wissenschaftliche Vorarbeiten sowie eine Einbeziehung des medialen Interesses ermöglichte die Schaffung einer erweiterten Stakeholder-Landschaft und Absteckung relevanter Themenfelder in der iMobility.

Die Analyse von iMobility-Hardware und -Software ermöglichte die Generierung eines neuartigen Systems zur Kategorisierung von Lösungen nach acht Themenfeldern: Assistenzsysteme, Car-2-X Kommunikation, Autonomes Fahren, Cyber Security & Privacy, Mobile Lösungen, Backend Systeme, Fahrzeugidentifikation und Unterhaltungstechnik. In der detaillierten Untersuchung von Technologien wurden diese Kategorien um weitere Sub-Kategorien erweitert, um ein flexibles Werkzeug zur Einteilung und Beurteilung von iMobility-Lösungen und Projekten für die Bedarfsträger zu schaffen.

Aufbauend auf der iMobility-Stakeholder-Landschaft wurden relevante Akteure im polizeilichen Kontext identifiziert, die über Technologien miteinander kommunizieren. Neben Beamten und den Polizeifahrzeugen wurden einerseits zivile Fahrzeuglenker und Fahrzeuge sowie autonome Fahrzeuge und unbeteiligte Dritte, andererseits Akteure der Polizei (Leitzentrale, Unterstützungskräfte) und anderer Organisation in der Straßensicherheit sowie die technische Verkehrsinfrastruktur als relevante kommunizierende Akteure identifiziert. In diesem Kontext wurde auch Ereignissen im Straßenverkehr eine Funktion als kommunizierender Akteur zugeordnet.

Die nachfolgende Identifikation und Beschreibung neuartiger iMobility-Einsatzszenarien im polizeilichen Kontext wurde als zentrales Ergebnis für die Bedarfsträger durchgeführt, um eine bessere Vorstellung von Möglichkeiten, Chancen und Herausforderungen durch innovative Technologien zu bieten. Die gewonnenen 25 Einsatzszenarien wurden mit Themenfeldern, Anforderungen, polizeilichen Anwendungsbereichen und kommunizierenden Akteuren in fünf Clustern (Einsatztaktik, Außendienst, Cybersecurity, Car-2-X, Autonomes Fahren) gruppiert dargestellt und zur Präsentation und Kommunikation aufbereitet.

IMOPOL+ Projektüberblick



Projektleitung
SYNYO GmbH, Research & Development Department

Projektpartner
- Bundesministerium für Inneres
- Kuratoriums für Verkehrssicherheit
- Universität Wien, Austrian Center for Law Enforcement Sciences ALES
- Virtual Vehicle Research Center VIF
- Österreichischer Automobil-, Motorrad- und Touring-Club ÖAMTC

Kontakt
Mag. Bernhard Jäger
SYNYO GmbH
Otto-Bauer-Gasse 5/14, 1060 Wien
E-Mail: bernhard.jaeger@synyo.com
www.synyo.com

Im Zuge des Projekts wurden immer wieder rechtliche Fragestellungen und Unklarheiten aufgedeckt, deren detaillierte Diskussion zwar außerhalb des Projektrahmens lag, die jedoch zukünftig maßgeblich die Entwicklung von iMobility beeinflussen. Die rechtlichen Kernthemen, die für einen weiterführenden Diskurs festgehalten wurden, beziehen sich primär auf Datennutzung, Privacy und autonome Fahrzeuge.

Während der gesamten Projektlaufzeit wurde intensiv an der effektiven europaweiten Kommunikation der Ergebnisse gearbeitet. Eine Projektidentität und Visualisierungen von Ergebnissen ermöglichten den effizienten Wissenstransfer zu internen und externen Bedarfsträgern sowie internationalen Polizeikräften und Forschungsteams. Dazu wurden Workshops, Präsentationen, wissenschaftliche Publikationen und die Veröffentlichung von digitalem und Druckmaterial genutzt.

Da das Projekt in einer Umbruchphase in der Entwicklung von Automobiltechnologie stattfand, wurden auch zukünftige Trends analysiert und aufbereitet. Dabei wurden das zunehmende Interesse an vernetzter Mobilität, die Entwicklung neuer Schnittstellen im Fahrzeug, die Steigerung der intrinsischen Sicherheit im Fahrzeug sowie rechtliche Entwicklungen dargestellt.

Die gemeinsame Leistung von Forschungspartnern und Bedarfsträgern ermöglichte ein umfangreiches und verwertbares Projektergebnis für alle Projektpartner, dessen Nutzung über den Projektzeitraum hinweg gesichert ist. Durch die hervorragende Kooperation aller Partner und den Einsatz geeigneter Maßnahmen für effizientes Projekt- und Risikomanagement wurde das Projekt innerhalb der vorgesehenen Laufzeit zur vollsten Zufriedenheit aller Partner abgeschlossen.

Internet Studie

Digitaler Atlas Österreich

In einem sich global verschärfenden Wettbewerb der Standorte ist eine leistungsfähige digitale Infrastruktur für Nationen ein entscheidendes Differenzierungsmerkmal. Diese für die Anbindung der nationalen Volkswirtschaft an internationale Wertschöpfungsprozesse unerlässliche Infrastruktur ist allerdings auch verwundbar. Cyberkriminalität, Wirtschaftsspionage, technische Fehler und Versagen infolge äußerer Ursachen sind nur einige der Risiken, die die Leistungsfähigkeit der digitalen Infrastruktur beeinträchtigen können.

Je stärker Wirtschaft, Staat sowie Bevölkerung vom Funktionieren der digitalen Infrastruktur abhängen, desto mehr wird die Absicherung gegenüber einem möglichen Ausfall zum integralen Bestandteil der persönlichen, unternehmerischen und nationalen Sicherheitsvorsorge.

Das Projekt Digitaler Atlas Österreich setzte an dieser sicherheits- und wirtschaftspolitischen Bedeutung der digitalen Infrastruktur an.

Der Digitale Altas Österreich:

- gibt Aufschluss über die für Österreich relevanten digitalen Infrastrukturkomponenten und -netze,
- illustriert exemplarisch anhand zweier konkreter Beispiele (Volumen, Richtung) aus dem Kontext kritischer Infrastrukturen den Verlauf des digitalen Datenflusses in Österreich und
- vermittelt einen Einblick in die für die relevanten digitalen Infrastrukturkomponenten und -netze maßgeblichen Markt- und Besitz- resp. Eigentumsverhältnisse.

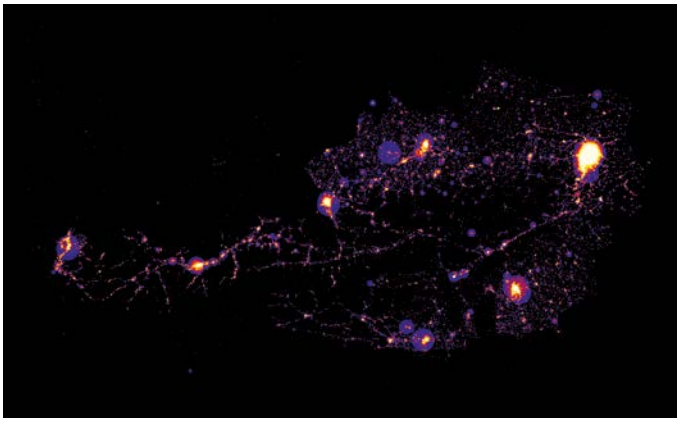
Der Digitale Atlas Österreich verdeutlicht die vielfältigen infrastrukturellen Abhängigkeiten in einem für Staat, Gesellschaft und Wirtschaft essentiellen Bereich der Vorsorge. Die aufbereiteten Fakten sind eine wichtige Entscheidungsgrundlage für die Sicherheitspolitik (z. B. Investitionen in die Resilienz kritischer Komponenten), die Wirtschafts- und Industriepolitik (z. B. Förderung nationaler Technologieakteure in relevanten Marktsegmenten) sowie die Forschungspolitik (z. B. Unterstützung der Grundlagenforschung und der angewandten Forschung im Kontext der digitalen Technologieentwicklung). Nachfolgend werden zwei ausgewählte Grafiken der Studie vorgestellt.

Netzzuteilungen, verbunden via Traceroute

Die Karte stellt alle in Österreich geographisch lokalisierbaren Netzzuordnungen (inkl. aller Hops, d.h. Routern und Layer 2) dar. Mehrere Router bzw. Hops in der gleichen Netzzuordnung (inetnum-Eintrag) wurden zusammengezogen, da diese mit derselben geographischen Adresse vermerkt sind. Die Karte wurde aus allen 206.000 Netzzuordnungen der RIPE-Datenbank für Österreich generiert. Jede Netzzuordnung ist eine fixe Zuteilung von IP-Adressen an Kunden. Das sind in der Regel Büros, Niederlassungen von Firmen u. ä. Private Endkunden und Mobilfunk erhalten normalerweise dynamische IP-Adressen und haben weder einzelne Zuweisungen, noch sind sie verortbar.

Das österreichische Internet ist sehr Wien-lastig, wobei das nur zu einem Teil der Messmethode zugeschrieben werden kann. Tatsächlich befinden sich in Wien die größten Rechenzentren (z. B. Interxion) und die größten Übergabepunkte (VIX); viele internationale Tier-1-Provider haben ihren sog. „Point of Presence" ausschließlich in Wien. Das lässt vermuten, dass ein Ausfall im Raum Wien (z. B. längerer Stromausfall) große Teile des Internets beeinträchtigen könnte. Gut zu erkennen sind die Landeshauptstädte und andere Ballungsräume. Im Westen ist die Bevölkerungskonzentration entlang der großen Täler klar ersichtlich, die sich natürlich auch in der Internet-Dichte niederschlägt.

Netzzuteilungen, verbunden via Traceroute



Heatmap über die Adresszuteilung (Adressdichte) in Österreich in Falschfarbdarstellung (Schwarz | Blau | Rot | Gelb | Weiß)

Heatmap

Die Karte zeigt die IP-Adress-Dichte in Österreich. Je mehr Zuteilungen und je größer die IP-Bereiche, desto heller erscheint die Region:

Die Ballungsräume sind gut zu erkennen. Eine Abweichung von der Bevölkerungsverteilung zugunsten Wiens ergibt sich daraus, dass dynamische IP-Bereiche (DHCP, DSL, Kabel) sowie Mobilfunk tendenziell bei der Firmenzentrale registriert werden, unabhängig von der tatsächlichen Verwendung. Überregionale ISPs haben ihre Firmenzentralen überwiegend in Wien.

Zusammenfassend ist festzuhalten, dass im Rahmen der Erstellung der Studie wesentliche Fragestellungen für die IKT-gebundene Struktur der in und für Österreich relevanten Services und Servicedienstleister ermittelt wurden. Neben der Entwicklung einer Topologie und zahlreichen Visualisierungen, die unter anderem den digitalen Datenfluss in Österreich aufzeigen, gelang es, wichtige Antworten auf die wirtschaftliche und infrastrukturelle Lage Österreichs im digitalen Raum in Erfahrung zu bringen und Vorschläge für eine Verbesserung sowie zukünftig relevante Handlungsfelder aufzuzeigen.

Projektleitung
SBA Research gGmbH

Projektpartner
- REPUCO Unternehmensberatung GmbH
- IFES Institut für empirische Sozialforschung GmbH
- Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

Kontakt
Mag. Michael Stephanitsch
SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
Tel: +43 1 505 36 88
MStephanitsch@sba-research.org
www.sba-research.org

Lob versus Strafe

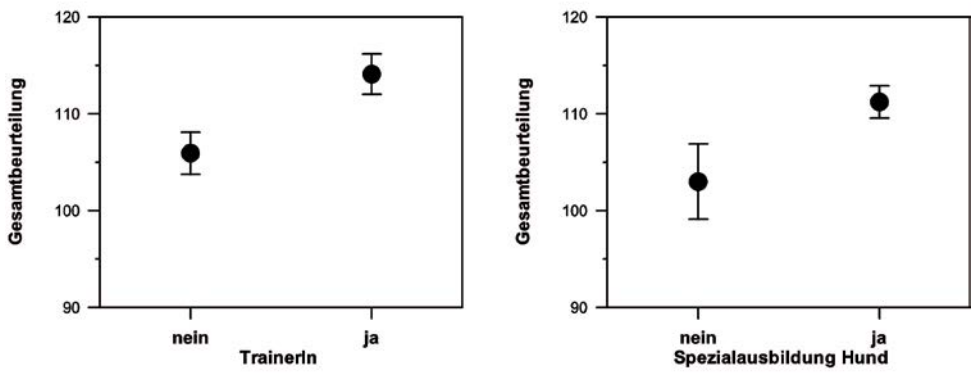
Neue Wege in der Polizeihundeausbildung

Anfang Februar 2017 wurde die im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS finanzierte Studie Lob versus Strafe fertiggestellt. Unter der Leitung von Prof. Dr. Ulrike Berninger von der Universität Salzburg, Fachbereich für Ökologie und Evolution, evaluierten Salzburger und Wiener WissenschaftlerInnen aus den verschiedensten Fachrichtungen gemeinsam mit ExpertInnen des Bundesausbildungszentrums für PolizeidiensthundeführerInnen die Ausbildung der Polizeidiensthunde in Österreich.

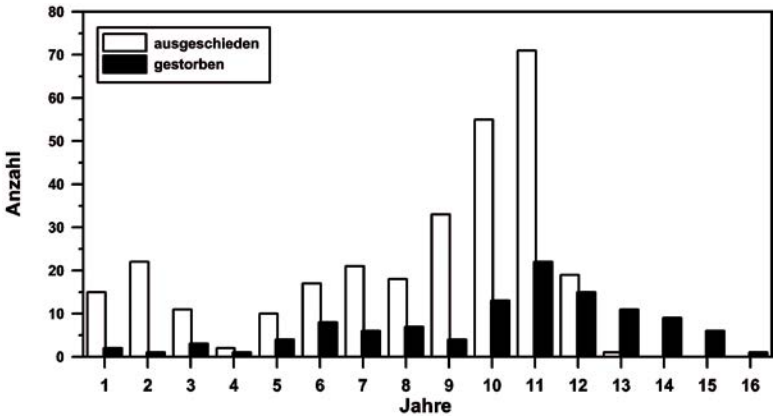
Als Polizeidiensthunde besonders geeignet sind selbstsichere, charakterstarke und belastbare Hunde mit dem nötigen Triebpotential. Im polizeilichen Einsatz müssen Polizeidiensthunde in jeder Situation führ- und lenkbar sein, auch in Extremsituationen und unter massivem Stress den Befehlen der HundeführerInnen folgen. Mag. Dr. Karin Rainer und Ines Levy, MA der Agentur für europäische Integration und wirtschaftliche Entwicklung AEI, untersuchten das Ausbildungssystem bzw. die Einstellung zu den Ausbildungsmethoden. Das Ergebnis der Befragung zeigt beim Großteil der Befragten eine positive Einstellung zur Ausbildung mittels positiver Bestärkung. Diese wird von den Befragten insgesamt als stressmindernder, langfristig wirksamer und effizienter eingestuft.

Das Thema „Stress und Leistung der Polizeidiensthunde" wurde von dem Salzburger Biologen Mag. Dr. Leopold Slotta-Bachmayr genauer bearbeitet. So hat sich die Leistung der Polizeidiensthunde in den letzten 10 Jahren nicht wesentlich verändert. Daraus kann gefolgert werden, dass die Ausbildung der Polizeidiensthunde schon bislang mit sehr viel Fachwissen und unter Anwendung positiver Verstärkung durchgeführt wurde. Der Biologe konnte weiters zeigen, dass Vorerfahrung der PolizeidiensthundeführerInnen bei der Ausbildung von Polizeidiensthunden nur eine untergeordnete Rolle spielt. Viel wichtiger sind die Aus- und Fortbildung von Hund und Mensch. Anhand von Videoanalysen wurde eindeutig nachgewiesen, dass stressfrei arbeitende Hunde auch bessere Leistungen z. B. beim Auffinden von Gegenständen erbringen.

Dass Polizeidiensthunde mit den Anforderungen des Exekutivdienstes gut umgehen können, zeigte Ass.-Prof. Dr. Gerhard Loupal, Pathologe an der Veterinärmedizinischen Universität Wien. So haben Polizeidiensthunde die gleiche Lebenserwartung wie Familienhunde vergleichbarer Rassen. Sie haben ähnliche Todesursachen, und auch das Muster etwaiger Verletzung unterscheidet sich z. B. nicht von denen bei Rettungshunden. Dass die Polizeidiensthunde gut betreut sind, zeigt außerdem die Analyse der Tierarztbesuche. Über die Hälfte der



Zusammenhang zwischen der Qualifikation der HundeführerInnen (TrainerIn ja/nein) bzw. des Polizeidiensthundes (Spezialausbildung Hund ja/nein) und der Leistung bei der Polizeidiensthundemeisterschaft. Menschen und Hunde mit höherer Qualifikation schneiden bei der Polizeidiensthundemeisterschaft insgesamt besser ab



Alter des Ausscheidens (n=295) bzw. Todesalter (n=113) von Polizeidiensthunden.
Polizeidiensthunde werden im Schnitt genauso alt wie Familienhunde vergleichbarer Rassen

Tierarztbesuche entfallen auf prophylaktische Maßnahmen wie Impfungen oder diverse vorbeugende Untersuchungen.

Die JuristInnen Mag. Julian Sixtl vom Bundesministerium für Inneres sowie Mag. Dr. Heike Randl von der Universität Salzburg, Fachbereich Öffentliches Recht, Völker- und Europarecht, haben Ausbildung und Einsatz von Polizeidiensthunden aus dem Blickwinkel geltenden Rechts betrachtet. Es geht dabei um die menschen-, sicherheits- und tierschutzrechtlichen Voraussetzungen, unter denen Polizeidiensthunde ausgebildet und eingesetzt werden dürfen, bzw. um die Frage, wer haftet, wenn etwas passiert. Besonders im Hinblick auf das geltende Tierschutzrecht beleuchteten die JuristInnen auch die Möglichkeiten sowie Grenzen für die Ausbildung von Polizeidiensthunden und identifizierten entsprechenden Veränderungsbedarf.

Der Tierethiker Mag. Erwin Lengauer von der Universität Wien, Forschungsstelle für Ethik und Wissenschaft im Dialog, erarbeitete dazu Grundsätze für die Verwendung der Hunde bei der Polizei. Diese Grundsätze sollen einen aus Sicht des Ethikers tierschutzgerechten Umgang und eine entsprechende Lebensqualität für die Polizeidiensthunde garantieren.

Die WissenschaftlerInnen sind sich einig, dass durch die Umstrukturierung der Ausbildung und das Verbot von Disziplinierungsmaßnahmen die Leistung der Polizeidiensthunde nicht schlechter geworden ist. Auch wenn in einigen Bereichen Verbesserungspotenzial aufgezeigt werden konnte, findet die Ausbildung der Polizeidiensthunde in Österreich auf sehr hohem Niveau statt. Das zeigt sich letztendlich auch in den optimalen Leistungen der BeamtInnen mit ihren Hunden.

Projektleitung
Paris-Lodron Universität Salzburg (PLUS),
Fachbereich für Ökologie und Evolution

Projektpartner
- Bundesministerium für Inneres
- Agentur für europäische Integration und wirtschaftliche Entwicklung AEI
- Veterinärmedizinische Universität Wien
- Universität Wien, Forschungsstelle für Ethik und Wissenschaft im Dialog

Kontakt
Dr. Leopold Slotta-Bachmayr,
Prof. Dr. Ulrike Berninger
Universität Salzburg, Fachbereich für Ökologie und Evolution
Hellbrunnerstr. 34, 5020 Salzburg
Tel.: +43 664 2828667
E-Mail: Leopold.Slotta-Bachmayr@sbg.ac.at
www.uni-salzburg.at

ÖMun

Entwicklung von Qualitätskriterien für die Einsatzmunition der österreichischen Exekutive

Die sog. „Teilmantel-Flachkopf-Munition" der österreichischen Exekutive wird seit der Einführung der Dienstpistole Glock im Jahr 1984 verwendet. Eine wissenschaftliche Untersuchung des 30 Jahre alten Munitionstyps in Bezug auf die objektive Wirksamkeit wurde bisher nicht durchgeführt, wobei moderne wissenschaftliche Prüfmethoden auch erst in den vergangenen 15 Jahren entwickelt wurden. Nach Schusswaffengebräuchen der letzten Jahre wurde immer wieder Kritik laut, da es durch die Notwendigkeit einer hohen Anzahl von Schüssen zu einer höheren Gefährdung von unbeteiligten Personen und ExekutivbeamtInnen kam.

In anderen europäischen Ländern gelten grundsätzlich vergleichbare gesetzliche Regelungen für den Waffengebrauch der Exekutive wie in Österreich. Um rechtlichen und ethischen Anforderungen an Schusswaffengebräuche so gut wie möglich zu entsprechen, wurden von einigen Ländern aufbauend auf wissenschaftlich fundierten ballistischen und medizinischen Untersuchungen spezifische Wirksamkeitskriterien der Munition definiert, um einerseits die Angriffs-, Widerstands- und Fluchtunfähigkeit zuverlässiger herstellen zu können und andererseits die direkt betroffenen Personen und Sachen gleichzeitig möglichst zu schonen. Dabei tauchen immer wieder die Begriffe der „Mannstoppwirkung" und „Hintergrundgefährdung" auf. Letzterer Begriff beinhaltet das Risiko primär unbeteiligter Personen, durch Querschläger, Projektile mit hoher Restenergie nach Durchschüssen oder auch Splitter von Projektilen verletzt zu werden.

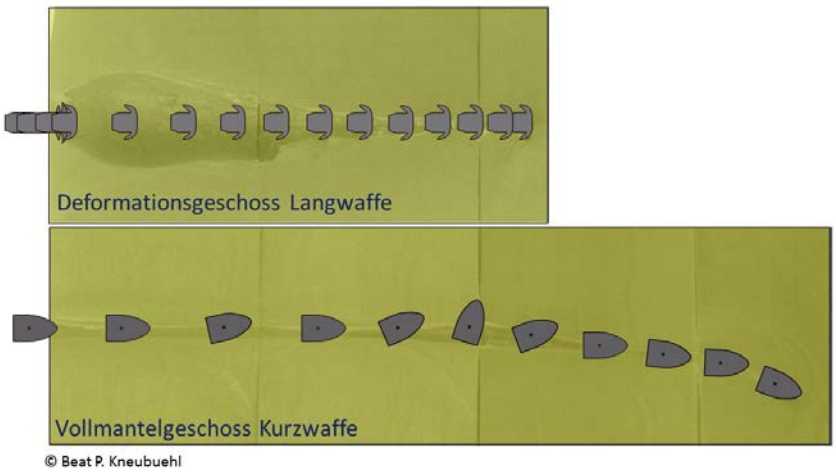
Ziel der Studie ÖMun war es daher, die derzeitige Einsatzmunition der österreichischen Exekutive wissenschaftlich zu evaluieren und Optimierungsmöglichkeiten auszuarbeiten. Zu diesem Zweck arbeiteten WissenschaftlerInnen aus Forensik und Ballistik, Bedarfsträger und GSK-Partner in einer ARGE zusammen und schufen im Laufe der Projektumsetzung eine wichtige Datengrundlage, die den Entscheidungsträgern als Basis für eine mögliche Änderung der Einsatzmunition dient. Zudem erreichte die Zusammenarbeit über das Projekt hinaus einen wichtigen Kompetenzaufbau der österreichischen Sicherheitsforschung.

In einem ersten Projektschritt wurde die Ausgangslage erhoben. Dies geschah auf Basis wissenschaftlicher Erfassung und Auswertung tatsächlich stattgefundener Schusswaffengebräuche. Dazu wurden die Akten zu Schusswaffengebräuchen durch Exekutivbeamte der Jahre 2002-2012 vom Institut für Gerichtsmedizin der Medizinischen Universität Innsbruck analysiert und statistisch ausgewertet. Die Ergebnisse zeigten, dass es in den 61 untersuchten Fällen mit 115 Schussabgaben in rund 70 % aller Fälle zu einem Durchschuss durch den Körper und somit zu einer relevanten Hintergrundgefährdung kam.

Parallel dazu wurde das Zentrum für forensische Physik und Ballistik des Instituts für Rechtsmedizin der Universität Bern unter der Leitung des renommierten Ballistikers Beat P. Kneubuehl beauftragt, die Wirksamkeit und das Deformationsverhalten der aktuell verwendeten Munitionssorte (TMFK) und einer Deformationsmunitionssorte (EMB) wundballistisch zu untersuchen. Zur Wirksamkeitsbestimmung wurde auf ballistische Seife geschossen, für die Knochentrefferuntersuchung wurden Röhrenknochensurrogate aus Polyurethan mit Silikonüberzug (zur Simulation der Knochenhaut) verwendet, das Weichgewebe wurde mit 10 %-iger ballistischer Gelatine simuliert.

Die Resultate zeigten einen deutlichen Unterschied der Wirksamkeit der beiden Geschosstypen, sowohl im weichen Gewebe als auch beim Knochentreffer. Die reproduzierbare und beschränkte Deformation des EMB-Geschosses ist für die höhere Energieabgabe im Gewebe verantwortlich, was zu einer geringeren Eindringtiefe des Geschosses führt. Auf der anderen Seite deformiert sich das TMFK-Geschoss praktisch nicht, erreicht dadurch eine sehr große Eindringtiefe und erhöht das Durchschussrisiko mit einer höheren Restenergie. Taumelbewegungen der Munition führten zudem zeitweise zu einem größeren Wundkanal.

Als nächster Schritt wurden der Vergleich und die Erfahrung internationaler Systeme, allen voran die Technische Richtlinie (TR) der deutschen Hochschule der Polizei, aber auch Definitionen aus den Niederlanden und der Schweiz als mögliche Grundlage für eine österreichische Definition der Wirksamkeitskriterien herangezogen. Hierauf wurden weitere Gesichtspunkte der Bedarfsträger und GSK-Partner miteinbezogen. Dies waren einerseits nationale Vorgaben, wie z.B. der in Österreich höchstzulässige Gasdruck in den Waffen, andererseits aber auch menschenrechtliche Aspekte in Bezug auf Schweregrad der Verletzungen und psychologischer Wirkung, die in die Ausarbeitung des Kriterienkatalogs einflossen. Auf Basis dieser Daten und Erkenntnisse formulierten die Partner ideale österreichspezifische Wirksamkeitskriterien für eine Munition der Exekutive aus.



Schematische Darstellung der Schusskanäle: Vollmantelgeschoss im Vergleich zu Deformationsgeschoss; Quelle: Kneubuehl B. 2013, Kick-off Meeting Ömun

In einem nächsten Schritt wurde versucht, die erarbeiteten Kriterien simulierend auf die erfassten Schusswaffengebräuche anzuwenden. Dabei muss klar zwischen Wirksamkeit und Wirkung eines Geschosses unterschieden werden. Während erstere normiert und beschrieben werden kann, hängt letztere vom individuellen Fall und seinen Umständen ab. Der Gerichtsmediziner Univ.-Prof. Dr. Walter Rabl bescheinigte – bestätigt durch die ballistischen Untersuchungen in der Schweiz – den definierten Kriterien ein potenzielles Verletzungsmuster, das den menschenrechtlichen Kriterien nicht widerspricht, das heißt es wären keine Gefäßeinrisse abseits des Schusskanals oder irreversible Knochenzerstörungen zu erwarten.

Für die mögliche Planung und Umsetzung einer Munitionsänderung wurden im Rahmen des Projekts von den Bedarfsträgern des Weiteren bereits Überlegungen zu psychologischen Aspekten, Einsatztraining sowie Öffentlichkeitsarbeit diskutiert.

Mit einer Anwendung der neu definierten Kriterien könnte sichergestellt werden, dass den Exekutivorganen künftig eine Einsatzmunition zur Verfügung steht, die den Anforderungen in Extremsituationen besser gerecht wird. Eine Gesamt-Risikoreduzierung für alle betroffenen Personen kann erwartet werden, allerdings wird sich im Falle einer Umsetzung der Empfehlung die Veränderung des Risikos durch eine neue Munition für den spezifischen Einzelfall wegen der vielen zu berücksichtigenden Faktoren nicht nachweisen lassen.

Projektleitung
CEMIT – Center of Excellence in Medicine and IT GmbH

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Justiz
- Medizinische Universität Innsbruck, Institut für Gerichtsmedizin
- Mag. Gudrun Rabussay-Schwald, GSK-Partner
- Andreas Zembaty, GSK-Partner

Kontakt
Dr. Barbara Frick
CEMIT – Center of Excellence in Medicine and IT GmbH
Karl-Kapfererstr. 5, 6020 Innsbruck
Tel: +43 512 576523 239
E-Mail: barbara.frick@cemit.at
www.cemit.at

PoRIS

Potentiale transnationaler River Information Services zur Gewährleistung der öffentlichen Sicherheit und Reduktion von Belastungen für die Schifffahrt

Die Wasserwege zwischen West- und Osteuropa stellen eine wichtige Transportverbindung für den europäischen Binnengüterverkehr dar. Die logistische und exekutive Verwaltung dieser Verkehrsinfrastruktur obliegt den jeweiligen Nationalstaaten. Bereits seit mehreren Jahren sind entlang des hochrangigen europäischen Wasserwegenetzes Informationssysteme für die Zurverfügungstellung von sogenannten River Information Services (RIS) im Einsatz. Diese werden bis dato hauptsächlich zum Zwecke des Verkehrsmanagements und für die Verbreitung von Fahrwasserinformationen eingesetzt.

Im Rahmen der Machbarkeitsstudie PoRIS wurden die Potentiale der transnationalen Nutzung von Binnenschifffahrts-Informationssystemen als Instrument zur risikobasierenden Durchführung polizeilicher Schiffsüberprüfungen zum Zwecke der Vermeidung von Mehrfachkontrollen untersucht. Bei diesem Unterfangen wurde zwei grundsätzlichen Zielvorgaben Rechnung getragen:

- Verbesserung des polizeilichen Ressourceneinsatzes im operativen Bereich
- Vermeidung unnötiger Belastungen für die Schifffahrt

In Anbetracht der voranschreitenden europäischen Integration wurde mit der vorliegenden Studie die Nutzung der österreichischen Donau River Information Services (DoRIS) für Aufgaben im Kontext der öffentlichen Sicherheit analysiert. Darüber hinaus ist geplant, in einem Anschlussprojekt auch die Möglichkeiten einer erweiterten transnationalen Kopplung von DoRIS mit den in den übrigen Donau-Anrainerstaaten eingesetzten Systemen zu beleuchten. Im Zuge des PoRIS-Projekts wurden die Potentiale anhand folgender Aspekte einer genauen Analyse und Bewertung unterzogen:

- Organisation und Struktur der Bedarfsträger
- Prozesse und Nutzenhebel
- Kommunikation und Information
- Datensicherheit/-schutz
- Rechtliche Rahmenbedingungen

Als Vorgehensweise wurde dazu eine durchgehende, systematische und standardisierte Kombination von IST-Analyse, Ermittlung von Anforderungsprofilen und das Aufzeigen von Verbesserungsansätzen mittels Nutzenhebeln gewählt.

Im Rahmen eines Proof of Concepts (PoC) wurde ein Kontrollremindersystem entwickelt, welches es dem Anwender (Schifffahrtspolizei, Schifffahrtsbehörde) ermöglicht, die Planbarkeit von Kontrollen zu verbessern. Durch einen Austausch von Kontrolldaten mit den entsprechenden Organen anderer EU-Länder können somit unnötige Mehrfachkontrollen von Schiffen vermieden werden.

Wichtig dabei war auch, dass der PoC zwar für Österreich erstellt, das Design aber so ausgelegt wurde, dass es leicht für andere Länder angepasst werden kann.

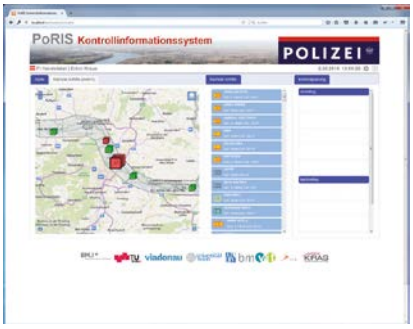
Durch eine Abschlussevaluierung des PoC mit den Bedarfsträgern wurde die Nützlichkeit noch einmal überprüft. Alles in allem wurde das System als sehr positiv wahrgenommen und ihm großes Potential seitens des BMVIT und der FI Handelskai zugesprochen.

Projektleitung
TU Graz, Institut für Maschinenbau- und Betriebsinformatik

Projektpartner
- Bundesministerium für Inneres
- via donau – Österreichische Wasserstraßen-Gesellschaft mbH
- Uni Wien, Rechtswissenschaftliche Fakultät, Austrian Center for Law Enforcement Sciences (ALES)

Kontakt
Prof. Siegfried Vössner
TU Graz, Institut für Maschinenbau- und Betriebsinformatik
Kopernikusgasse 24, 8010 Graz
Tel: +43 316 873 8001
E-Mail: voessner@tugraz.at
www.mbi.tugraz.at

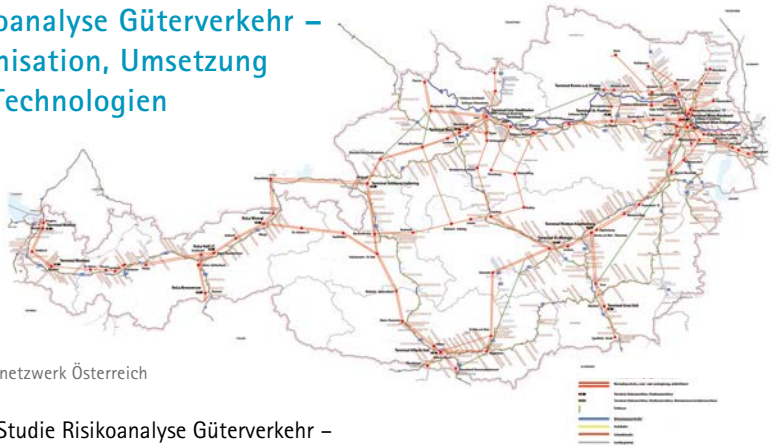
Projektteam bei der Einsatzanalyse der FI Handelskai



Hauptseite des PoRIS Kontrollinformationssystems (li.) und „U-Bahn" Darstellung der nächsten ankommenden Schiffe an der FI Handelskai (re.)

RAGOUT

Risikoanalyse Güterverkehr – Organisation, Umsetzung und Technologien



Transportnetzwerk Österreich

Die Studie Risikoanalyse Güterverkehr – Organisation, Umsetzung und Technologie, kurz RAGOUT fokussiert auf eine umfassende Risikoanalyse für den Güterverkehr im alpinen Bereich mit Schwerpunkt auf die Brennerachse in Tirol zwischen der deutsch-österreichischen und der österreichisch-italienischen Grenze. Insbesondere standen dabei Störfallanalysen und -potenziale für regionale, nationale und übergreifende Wirkungen bei längeren Unterbrechungen der beiden Verkehrsträger Schiene (EU-Nord-Süd-Transversale) und Straße in Tirol im Fokus der Studie. Untersucht wurden mögliche Wirkungen im Störungsfall auf das Transportsystem und in weiterer Folge die Versorgungssituation der Wirtschaftsbetriebe im Einzugsgebiet. Aufbauend auf einer umfassenden Analyse der zugrundeliegenden Systemkomponenten wurden mögliche Szenarien von Störanfällen abgeleitet, definiert und simuliert, um Gefahrenpunkte für alpenquerende Transportketten zu visualisieren. Die spezifischen Risiken und die in weiterer Folge damit verbundenen Störfälle im alpenquerenden Güterverkehr wurden systematisch evaluiert, dargestellt und die Erkenntnisse aufbereitet.

Die Arbeiten der vorliegenden Studie konzentrierten sich auf das komplexe Zusammenspiel der Verkehrsträger innerhalb alpenquerender intermodaler und kombinierter Transportketten. Die korrespondierenden Systemkomponenten, wie Transportinfrastruktur, Umschlageinrichtungen, umliegende Infrastrukturen, Informations- und Kommunikationsinfrastruktur und rollendes Material wurden dafür auf Schwachstellen und Risikopotenziale analysiert.

Darauf aufbauend wurden potenzielle Szenarien von Störfällen modelliert und deren Wirkungen auf das Transportsystem und die Unternehmen mit einem speziell entwickelten Simulationsmodell analysiert. Die Vorgehensweise der vorliegenden Untersuchung basiert auf der Kombination der Erkenntnisse bestehender Analysetools und -komponenten. Die Intention der Zusammenführung und Integration der vorhandenen Tools liegt in der Schaffung eines aus der Kombination der Erkenntnisse resultierenden zusätzlichen Mehrwertes. Weiters wurden die Erkenntnisse der „Schutz 14", einer der größten Bundesheerübungen in Nenzing, und die Ergebnisse einer „Vor-Ort-Begehung" durch das Bundesheer herangezogen. Diese wurden mit den Erkenntnissen einer Erhebung und Analyse der transportrelevanten Informations- und Kommunikationstechnologie verschnitten und für die Entwicklung eines breiten Spektrums an Analyse- und Simulationsszenarien herangezogen.

Die entwickelten Szenarien stellen die Vielfältigkeit möglicher Störfallquellen dar und bilden die Basis für weitere Analysen, die durchaus über den Rahmen dieser Studie hinausgehen. Im Rahmen von RAGOUT wurde eine Auswahl dieser Szenarien einer vertiefenden Analyse und Simulation unterzogen, um die Auswirkung einer Unterbrechung auf einem bestimmten Abschnitt und die damit verbundenen Wirkungen für die gesamte Strecke sowie die Betriebsansiedlungen in der Region aufzuzeigen. Die einzelnen Schritte und die dafür notwendigen Erhebungen und Quellen für Informationen wurden in einer „RAGOUT-Standardvorgehensweise" zusammengefasst und aufbereitet. Diese Standardvorgehensweise bildet eine Roadmap für EntscheidungsträgerInnen, um für Analysen oder im Fall realer Störfälle einen Standardprozess für die notwendige Vorgehensweise in der Informationsbeschaffung und -aufbereitung zur Verfügung zu haben.

Analysiert wurde, welche Auswirkung eine Unterbrechung/Störung der Transportinfrastruktur auf Betriebsansiedelungen in der Region Tirol entlang der Brennerachse haben kann. Mit Hilfe einer speziell entwickelten Simulation kann die zeitliche und räumliche Auswirkung der Unterbrechung eines Streckenabschnittes analysiert werden. Die daraus resultierenden Erkenntnisse bilden die Basis für die Ableitung entsprechender präventiver und reaktiver Schritte durch die Bedarfsträger. Die Studie erhebt den Anspruch, durch ihre umfassenden, aus Blickwinkeln der Wissenschaft und der Praxis betrachteten Analysen sowie der daraus gezogenen Schlüsse einen Beitrag zur Erhöhung der Sicherheit in der Versorgung aller Unternehmen im Kontext der Brennerachse und damit auch in der Güter-Versorgung der BürgerInnen des Landes Tirol zu leisten. Darüber hinaus können die Ergebnisse dieser Arbeit auf andere sensible Regionen übertragen werden.

Projektleitung
Boku Wien, Institut für Produktionswissenschaft und Logistik

Projektpartner
- Universität Wien, Fakultät für Informatik
- Landesverteidigungsakademie, Militärkommando Tirol
- AIT – Austrian Institute of Technology GmbH
- Österreichisches Rotes Kreuz
- Freiwillige Rettung Innsbruck

Kontakt
Prof. Manfred Gronalt
Boku Wien, Institut für Produktionswissenschaft und Logistik
Feistmantelstrasse 4, 1180 Wien
Tel.: +43 1 47654 73411
E-Mail: manfred.gronalt@boku.ac.at
www.wiso.boku.ac.at/pwl.html

R-Cubed

Request a Rescue Robot – Einsatzmodelle für Assistenzroboter für Einsatzkräfte

Einleitung

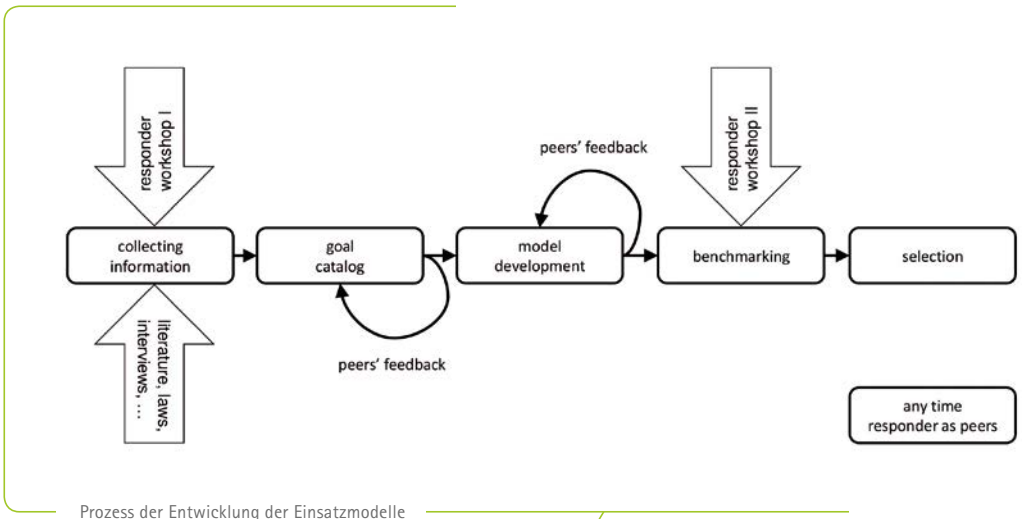
Einsatzkräfte kommen immer wieder in Krisensituationen, deren Aufklärung und Abhandlung mit erheblichen persönlichen Risiken behaftet ist. Moderne Robotertechnologie kann helfen, diese Risiken zu minimieren. Es gibt viele Beispiele für den erfolgreichen prototypischen Einsatz von Robotik in Krisenszenarien (Hurrikan Ike in den USA 2008, Explosion eines Militärlagers in Zypern 2011, Erdbeben in Mirandola, Italien 2012). Auf Grund von technischen, organisatorischen, rechtlichen und ökonomischen Gründen findet sich diese Technologie jedoch heute noch kaum im Regelbetrieb der Einsatzorganisationen. Ziel des Projekts R-Cubed war es, tragfähige Modelle zu entwickeln, die es Einsatzkräften einfach und schnell erlauben, auf Robotertechnologie und ExpertInnen in Krisensituationen zuzugreifen. Der Vorteil solcher Modelle ist, dass die Rahmenbedingungen für Taktik, Training, Wartung und Bedienung genau und praxisgerecht festgelegt sind. Im Zuge des Projekts werden die technischen, taktischen und rechtlichen Rahmenbedingungen ausgearbeitet, damit eine schnelle und sichere Integration von Robotern und ExpertInnen in Einsätze möglich wird. Neu in diesem Zusammenhang ist, dass systematisch aufgearbeitete und mittels eines methodischen Ansatzes neuartige sowie realisierbare Einsatzmodelle generiert werden. Insbesondere sollten folgende Fragen geklärt werden:

- Identifikation realistischer Anwendungsfälle
- Wie kann die Befehlskette bei externen ExpertInnen aufrechterhalten werden?
- Welche rechtlichen Einschränkungen sind zu beachten, z. B. Arbeitsrecht, Haftungsfragen, Genehmigungen, Datenschutz?
- Wie kann eine kurze und verbindliche Reaktionszeit garantiert werden?
- Welches Training müssen ExpertInnen aufweisen?
- Wie ist das technische Gerät zu warten und zu zertifizieren?
- Wie sieht ein geeigneter Aktivierungsmechanismus auf regionaler, bundesweiter und internationaler Ebene aus?

Modellentwicklung

Um eine systematische Aufarbeitung der Anforderungen und Rahmenbedingungen zu ermöglichen und innovative, tragfähige Einsatzmodelle zu generieren, wurde ein methodischer Ansatz aus dem Bereich „Systems Engineering" gewählt.

Zuerst wurde eine systematische Analyse des Problems, möglicher Einsatzszenarien und der Rahmenbedingungen (technisch, taktisch, rechtlich) durchgeführt. Im Rahmen der Analyse wurden die aktuelle Literatur aufgearbeitet, aktuelle Regulatorien studiert, ExpertInneninterviews im Bereich Recht und Verwaltung geführt und ein erster Workshop mit Einsatzkräften durchgeführt. Die direkte Einbindung der Einsatzkräfte ist unumgänglich, um die Akzeptanz der entwickelten Methoden bei den Endnutzern zu



Prozess der Entwicklung der Einsatzmodelle

ermöglichen. Wichtige Punkte, die hier identifiziert wurden, waren die Sicherheit und Authentizität von Daten, die strikten Regeln für Drohnen in Österreich und die Sinnhaftigkeit bodengestützter Roboter. Die ersten interessanten Ergebnisse waren eine Priorisierung der Reaktionszeit für verschiedene Lagen (< 1h; 1-3h; zeitunkritisch) und die Identifikation konkreter Einsatzszenarien für Robotertechnik (Lageerfassung, Suchen und Bergen – Lawinen, Detektion von Schadstoffen, Dokumentation der Lage).

Aus dieser Aufarbeitung wurde gemeinsam mit den Einsatzkräften ein Zielkatalog erarbeitet, der zum Einen die gewünschten Eigenschaften und Grenzen der Modelle definiert und zum Anderen zur Bewertung der generierten Modelle herangezogen werden kann. Dieser Zielkatalog stellt auch Parameter zur Verfügung, die systematisch variiert werden können, um verschiedene Modelle (Lösungen) zu generieren. Folgende Kategorien wurden für den Zielkatalog verwendet: funktionelle Ziele (Organisationsformen, technische Anforderungen, Logistik, Reaktionszeit, Verfügbarkeit), personelle Ziele (Training, Qualifikationen, Zertifizierung), rechtliche Ziele (Betriebsgenehmigungen, Haftung, Datenschutz) und finanzielle Ziele (Investmentkosten, Kosten für Einsätze, Regelungen für Kostenersatz).

Aus den identifizierten Anwendungsfällen und dem Zielkatalog wurden Parameter abgeleitet, die zur Generierung von Einsatzmodellen variiert werden. Die zentralen Parameter umfassen: Organisationsform und rechtlicher Rahmen (Einsatzorganisation, Verein, öffentliche Einrichtung, Firma), Verfügbarkeit (< 1h; 1-3h; zeitunkritisch), abzubildende Anwendungsfälle (Lagebild, Deduktion von Glutnestern, zusätzliche Messungen, präventive Inspektion), Alarmierung (Integration in bestehende Alarmpläne, Nachalarmierung), Logistik (integriert in Einsatzkräfte, Spezialfahrzeug, externes Ready-To-Go Setup), Training und Zertifizierung (simple Drohnen, spezielle Robotersysteme, erweitere Sensorauswertung). Folgende Parameter sind unabhängig vom jeweiligen Modell immer vollständig zu berücksichtigen: Wartung, Interfaces, Haftung, Datensicherheit und Betriebsgenehmigungen. Eine detaillierte Beschreibung der Parameter und des Prozesses ist im wissenschaftlichen Endbericht beziehungsweise in weiteren Publikationen zu finden (J. Maurer, G. Lichtenegger, G. Steinbauer, 2016).

Modellgenerierung

Dem systematischen Ansatz folgend, wurden die Parameter systematisch variiert und eine größere Anzahl möglicher Einsatzmodelle generiert. Hier ist anzumerken, dass es systematische Abhängigkeiten zwischen den Parametern gibt und nicht alle Parameter beliebig verändert werden können, ohne nichtrealisierbare Modelle zu generieren. So hat die Reaktionszeit eine direkte Abhängigkeit zur Organisationsform (z. B. kann nur eine Einsatzorganisation realistischerweise eine Reaktionszeit von < 1 Stunde garantieren). Primär wurden entlang der beiden Hauptachsen Organisationsform und Reaktionszeit 12 verschiedene Modelle generiert. Diese wurden auf 8 Templates reduziert (z. B. kann nur eine Einsatzorganisation realistischerweise alle Reaktionszeiten bieten). Aus diesen wurden 4 Referenzmodelle ausgewählt: Einsatzorganisation mit Reaktion < 1 Stunde (direkte Integration der Roboter in die Einsatzkräfte, einfaches Lagebild), Verein oder Firma mit Reaktionszeit bis 3 Stunden (Integration in Spezialfahrzeug, erweitertes Lagebild), Einsatzorganisation mit unkritischer Reaktionszeit (speziell geschulte Einsatztruppe, Personensuche, Fernmanipulation gefährlicher Stoffe) und Verein oder Firma mit unkritischer Reaktionszeit (externe Version des vorherigen Modells).

Diskussion und Ausblick

Die entwickelten Einsatzmodelle erlauben es, moderne Robotertechnik in den Routineeinsatz bei Krisensituationen zu bringen. Dazu wurden Anforderungen und Rahmenbedingungen erstmalig systematisch aufgearbeitet und mittels des Ansatzes des „System Engineering" tragfähige Einsatzmodelle generiert. Im finalen Workshop mit den Einsatzkräften wurden zwei Modelle für eine Realisierung ausgewählt: direkte Integration von Drohnen in die Einsatzkräfte für ein einfaches Lagebild und eine externe akkreditierte Organisation, die mittels Robotik zusätzliche hochklassige Daten und Analysen bieten kann. Im Moment wird an einer ersten praktischen Realisierung der Modelle in einem grenzüberschreitenden Projekt gearbeitet. Ziel ist es, in 3 Jahren die angedachten Services in den Regelbetrieb bei Feuerwehren in Österreich und Slowenien zu integrieren.

Projektleitung
TU Graz, Institut für Softwaretechnologie
Projektpartner
• Landesfeuerwehrverband Steiermark
Kontakt
Ass.-Prof. Dr. Gerald Steinbauer
TU Graz, Institut für Softwaretechnologie
Inffeldgasse 16b/2, 8010 Graz
Tel: +43 316 873 5723
E-Mail: steinbauer@ist.tugraz.at
www.ist.tugraz.at

SECCAT

Kriterienkatalog, Gütesiegel und Plattform für die Cloud-Sicherheit in Österreich

Ausgangsbasis

Die technologischen Entwicklungen rund um die voranschreitende digitale Revolution führen zu rasanten technischen Entwicklungen und Möglichkeiten. Cloud-Computing wurde dabei lange Zeit unterschätzt, stellt sich aber nunmehr als einer der wesentlichsten Treiber für eine Vielzahl von Veränderungen beim Einsatz von Informationstechnologie heraus.

Mit der rasanten Entwicklung, der Vielzahl neuer Möglichkeiten und der teilweise sehr von Anbietern dominierten Marktsituation sehen sich Cloud-Marktteilnehmer in Österreich vor neue und mittlerweile dringliche Herausforderungen gestellt. Dies gilt gleichermaßen für den sicheren und qualitativ hochwertigen Einsatz von bzw. das Angebot an Cloud-Services durch Bundesbehörden.

Insbesondere gilt es, berechtigte, aber unspezifische Zweifel an der Qualität und Verlässlichkeit von Angeboten in einen objektivierbaren Rahmen überzuführen. Außerdem muss eine Erhöhung der Sicherheit beim Einsatz von Cloud-Services erfolgen. Zu diesem Zweck wurde in den vergangenen Jahren international bereits eine Reihe von Maßnahmen gestartet. Die wohl bedeutsamste wird die Einführung des Trusted-Cloud-Gütesiegels des Deutschen Bundesministeriums für Wirtschaft und Energie auf der CeBIT werden.

Bedarf und gewünschtes Ergebnis

Für Österreich besteht der dringende Bedarf, ebenfalls klare Rahmenbedingungen zu definieren, an denen sich Anbieter und Kunden von qualitativ hochwertigen und sicheren Cloud-Angeboten orientieren können. Dies gilt insbesondere dann, wenn Bundesstellen oder dem Bund nahestehende Organisationen Angebote selbst erstellen und anbieten bzw. hochwertige und sichere Cloud-Services einkaufen wollen. Die genannten Rahmenbedingungen (Gütekriterien) sollen so formuliert und flexibel einsetzbar sein, dass eine breite Unterstützung durch mehrere Ministerien möglich ist.

Eine Vorgangsweise ähnlich jener, die in Deutschland in Kürze eingeführt wird, könnte eine vergleichbare Referenz darstellen und müsste vernünftig auf etwaige österreichische Unterschiedlichkeiten angepasst werden.

Diese Studie dient dazu, rasch den Grundstein für ein hochwertiges Trusted-Cloud-Gütesiegel zu legen, das österreichische Rahmenbedingungen berücksichtigt und dennoch international kompatibel ist (was insbesondere für europaweite Ausschreibungen unerlässlich ist).

Auf diese Weise kann der Bund mit positivem Beispiel vorangehen, die Qualität des Cloud-Angebotes unmittelbar beeinflussen und vorzeigen, wie qualitativ hochwertige und sichere Cloud-Services leichter, kostengünstiger und rascher ausgeschrieben, verglichen und bewertet werden können. Außerdem wird mit einem solchen staatlich etablierten Cloud-Gütesiegel dargestellt, wie man als verantwortungsbewusster Cloud-Kunde – insbesondere mit spezifischen Anforderungsprofilen – sichere, vertrauenswürdige und qualitativ hochwertige Angebote von solchen unterscheidet, die diesen Anspruch nicht erfüllen.

Ziele des Projekts

Primäres Ziel des Projekts ist die Ausarbeitung von Qualitätssicherungsmaßnahmen und eines Kriterienkatalogs zur Unterstützung eines sicheren Einsatzes von Cloud in österreichischen Organisationen des privaten und öffentlichen Sektors. Im Rahmen des Projekts werden der Status Quo von Cloud Computing und mobilen Geräten in österreichischen Organisationen sowie Use Cases erfasst. In einem zweiten Schritt wird in enger Zusammenarbeit mit Bedarfsträgern ein Kriterienkatalog erarbeitet, der den Anforderungen bestmöglich entspricht. Zur Einbindung von Bedarfsträgern und Experten aus den Bereichen Cybersecurity, Cloud und Mobile wird u.a. ein Stakeholder-Workshop veranstaltet. Um die Praxistauglichkeit des Kriterienkataloges sicherzustellen, wird dieser gemeinsam mit potenziellen Bedarfsträgern validiert.

Inhalte des Projekts

- Erhebung des österreichischen Status Quo an Cloud-Nutzung, Cloud-Unternehmen (Kunden) und Beschäftigungseffekten, Vertrauensindex und Hemmnissen – immer jeweils im internationalen Vergleich. Damit soll sichergestellt werden, dass etwaige vorhandene österreichische Spezifika rechtzeitig berücksichtigt werden können.
- Übersicht über aktuelle Gütesiegel-Entwicklungen und Vergleich der Zugänge und inhaltlichen Qualitäten. Damit soll ein guter Marktüberblick als Basis für Entscheidungen vorliegen, und weitere Schritte sollen sich an „Best Practice" orientieren können.
- Definition eines österreichischen Trusted-Cloud-Labels auf Basis eines objektiven und transparenten Kriterienkatalogs inklusive Anforderungen, Gegenstand und Werteversprechen.
- Definition der Grundlagen und Merkmale einer österreichischen Trusted-Cloud-Plattform, die ein breites Informationsangebot, Transparenzkriterien sowie Entscheidungs- und Unterstützungsfunktionen bieten soll. Diese Plattform soll auch als Marktplatz von vertrauenswürdigen Angeboten fungieren und Orientierungs- und Entscheidungshilfen liefern.
- Definition der Trusted-Cloud-Plattform als Herausgeberin und Schirmherrin des österreichischen Trusted-Cloud-Gütesiegels und -Kriterienkatalogs.

Lieferobjekte des Projekts:

- Lieferung des Status Quo zum Thema Cloud in Österreich und im internationalen Vergleich.
- Lieferung eines Vorgangsleitfadens zur Schaffung eines österreichischen Cloud-Gütesiegels des Bundes.
- Lieferung eines Kriterienkatalogs auf Basis internationaler Referenzen.
- Einbeziehung österreichischer Ministerien zur Sicherung der spezifischen Interessenlage, insbesondere hinsichtlich Qualität und Sicherheit von Bundesstellen. Durchführung eines oder mehrerer Stakeholder-Workshops.
- Überprüfung der Inhalte und der Qualität des Anforderungskataloges anhand einer bestehenden behördlichen Cloud-Anwendung.
- Umsetzungsbeschreibung einer österreichischen Trusted-Cloud-Plattform und eines Labels.
- Vorschläge für die Ausgestaltung von Funktion, Prozessen und möglichen Organisationsformen für eine österreichische Trusted-Cloud-Plattform.

Projektleitung
IDC Central Europe GmbH
Projektpartner
- Bundesministerium für Finanzen
- EuroCloud.Austria
- REPUCO Unternehmensberatung GmbH
- A-SIT Plus GmbH

Kontakt
Dr. Nick Tahamtan
IDC Central Europe GmbH
Parkring 10, 1010 Wien
Tel: +43 1 516 33 31 78
E-Mail: ntahamtan@idc.com
www.idc-austria.at

Secure EGov

Standardentwicklung zum Schutz kritischer E-Governments

Secure EGov war ein Forschungsvorhaben zur Entwicklung eines sicheren E-Government-Standards für Österreich. Forschung, Wirtschaft und Behörden formulierten in nur einem Jahr einen technisch anspruchsvollen und formell einenden Sicherheitsstandard für webbasierte E-Government-Anwendungen.

Mit diesem Standard ist ein anwendungsorientiertes, fachlich fundiertes und überprüfbares Grundlagenwerk entstanden, das die Sicherheit von E-Government-Webapplikationen und Webservices erhöht und in Folge aufrecht hält. Der Secure E-Government-Standard dient zur Festlegung und Überprüfung angemessener Informationssicherheitsanforderungen für E-Government-Webapplikationen und -services, die für Privatpersonen sowie Wirtschaftstreibende verfügbar sind, einschließlich der grundlegenden IT-Infrastruktur. Im Mittelpunkt des Standards stehen technische und organisatorische Sicherheitsanforderungen im Lebenszyklus von Webapplikationen und -services (Entwicklung bzw. Beschaffung, Inbetriebnahme, Betrieb und Außerbetriebnahme).

Inhaltlich wurden nach einschlägiger Recherche und Auswahl von adäquaten Standards u.a. folgende Themen abgedeckt:

- Verantwortlichkeiten
- Zugriffskontrolle
- Verschlüsselung
- Kryptografie
- Betriebssicherheit
- Sicherheit in der Kommunikation
- Sichere Softwareentwicklung
- Lieferantenbeziehungen
- Eskalationspfade und Meldepflichten
- Konformität

Zudem wurden – neben der Beschreibung und detaillierten Erläuterung des Themas – technische und organisatorische (Sicherheits-)Anforderungen formuliert, relevante Rechtsvorschriften angeführt und Empfehlungen abgegeben. In Vertretung für das gesamte Themenfeld werden hier „Verantwortlichkeiten" sowie „Datensicherung und Archivierung" aus dem Secure-EGov-Standard angeführt:

Verantwortlichkeiten

Beschreibung: Die Definition der wesentlichen Verantwortlichen, welche mit der Entwicklung und dem Betrieb von Webapplikationen und -services in Beziehung stehen, ist ein wesentlicher Faktor zur Aufrechterhaltung der Sicherheitsziele.

Anforderungen: Festlegung von Verantwortlichkeiten. Alle für die Entwicklung, den Betrieb und die Sicherheitseinhaltung wesentlichen Verantwortlichkeiten sind zu definieren. Dies inkludiert eine formelle Aufgabenbeschreibung und eine Zuweisung zu Personen.

- Etwaige Unvereinbarkeiten müssen berücksichtigt werden.
- Bei der Besetzung ist das Vertretungsprinzip zu berücksichtigen.

Rechtsvorschriften: § 14 Abs. 2 Z 2 DSG 2000 (Auftragsprinzip).

Weitere Informationen sind u.a. im Österreichischen Informationssicherheitshandbuch (Version 4) in Kapitel 12.1.4 „Festlegung von Verantwortlichkeiten" zu finden.

Datensicherung und Archivierung

Beschreibung: Ziel der Datensicherung und Archivierung ist das kurz- und langfristige Sichern von Daten bzw. Informationen sowie der Erhalt der Fähigkeit, diese zeitgerecht und korrekt wiederherstellen zu können. Es gilt, Einflussfaktoren zu erheben und Verfahrensweisen festzulegen.

Anforderungen:

1. Zur Vermeidung von Datenverlust sind Datensicherungs- und Wiederherstellungsverfahren festzulegen und umzusetzen. Folgende Punkte sind zumindest festzulegen:
   - Umfang (Geschäftsdaten, Konfigurationsdaten, Systemdaten, Protokolldaten und Software), Art und Häufigkeit
   - Zugriffsberechtigung und Schutz
   - Aufbewahrungsdauer
2. Vor Inbetriebnahme und bei wesentlichen Architekturänderungen sind Wiederherstellungstests durchzuführen und zu dokumentieren. Auch die Sicherungsmedien müssen regelmäßig auf ihre Funktionsfähigkeit getestet werden.

Rechtsvorschriften: § 14 Abs. 1 DSG 2000 (Ergreifen von Maßnahmen zum Schutz vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust).

Die Verbindlichkeit bzw. Relevanz der im Standard angeführten Anforderungen sind abhängig vom Schutzbedarf der verarbeiteten Informationen, der Angemessenheit der umzusetzenden Sicherheitsmaßnahmen sowie der Compliance, d. h. der zutreffenden Rechtsvorschriften. Die Anforderungen wurden auszugsweise laut Sicherheitshandbuch 2013 dargestellt und klassifiziert, zum Beispiel:

Anforderungen	Schutzbedarf[1]		
	Normal	Hoch	Sehr hoch
2.1 Verantwortlichkeiten			
1 Festlegung von Verantwortlichkeiten	●	●	●
2.2 Zugriffskontrolle			
2.2.1 Berechtigungskonzept und Berechtigungsmanagement			
1 Erstellung eines Berechtigungskonzepts	●	●	●
2 Sicherstellung einer Mandantentrennung	●	●	●
3 Management von Berechtigungen	●	●	●
4 Prüfung von administrativen Berechtigungen	●	●	●
2.2.2 Authentifizierung			
1 Einsatz von Authentifizierungsverfahren	●	●	●
2 Einsatz von Session Timeouts	●	●	●
3 Protokollierung von Verwendungsvorgängen	●	●	●
4 Einsatz von sicheren Passwörtern	●	●	●
5 Einsatz von Sperrmechanismen	●	●	●
6 Einsatz von Provisionierungsverfahren	●	●	●
2.3 Kryptografie			
1 Einsatz von kryptografischen Verfahren bei der Datenspeicherung			●
2 Einsatz von kryptografischen Verfahren bei der Datenübermittlung	●	●	●
3 Erstellung eines Kryptografiekonzepts	●	●	●
4 Eignungsprüfung von kryptografischen Verfahren	●	●	●
2.4 Betriebssicherheit			
2.4.1 Dokumentation			

Auszug zu den Verbindlichkeiten der Anforderungen laut Sicherheitshandbuch (2013)

Projektleitung
Michael Stephanitsch

Projektpartner
- Bundesministerium für Inneres
- Bundesministerium für Finanzen
- Bundeskanzleramt
- Universität Wien, Institut für Europarecht, Internationales Recht und Rechtsvergleichung
- Zentrum für sichere Informationstechnologien Austria A-SIT
- REPUCO Unternehmensberatung GmbH

Kontakt
Mag. Michael Stephanitsch
SBA Research gGmbH
Favoritenstraße 16, 1040 Wien
Tel: +43 1 505 36 88
E-Mail: MStephanitsch@sba-research.org
www.sba-research.org

Dank der effizienten Kooperation von Bedarfsträgern und Projektpartnern gelang es, einen schlanken, klar strukturierten und dadurch nutzerfreundlichen E-Government-Standard aus Österreich für Österreich zu entwickeln. Im Falle einer Umsetzung kann dieser Standard zu einer Referenz sowohl für Sicherheitsverantwortliche als auch für Privatpersonen werden; eine entsprechende Zertifizierungsmöglichkeit ist der nächste anzustrebende Schritt. Mit einer sicheren E-Government-Infrastruktur können Hemmnisse zwischen Staat und BürgerInnen effizient und effektiv beseitigt werden.

SI-ALT

Polizei und Alter: Stärkung der subjektiven Sicherheit älterer und hochaltriger Frauen und Männer im öffentlichen Raum

Das Projekt SI-ALT beschäftigt sich mit neuen Herausforderungen, die durch den demographischen Wandel und die wachsende Alterung der Gesellschaft auf PolizistInnen (und andere SicherheitsakteurInnen) in den nächsten Jahrzehnten zukommen werden. In Österreich liegt der Anteil an Menschen im Alter von 50 Jahren oder älter bei 38,3 %, der Anteil der Menschen im Alter von 65 Jahren oder älter bei 18,3 %. Diese Anteile werden bis 2030 voraussichtlich auf 43,4 % (50+) bzw. 23,6 % (65+) steigen (Statistik Austria, 2014).

Bei „den" älteren und hochaltrigen Frauen und Männern handelt es sich aber nicht um eine homogene Zielgruppe, an die sich PolizistInnen mit einer einheitlichen Präventions- und Kommunikationsstrategie im öffentlichen Raum wenden können, sondern um eine intern sehr stark differenzierte Gruppe von Menschen, die zwar gewisse Charakteristika miteinander teilen, sich jedoch in ihren Bedürfnissen, in ihren Lebensstilen und schlussendlich in ihrem subjektiven Sicherheitsempfinden stark unterscheiden.

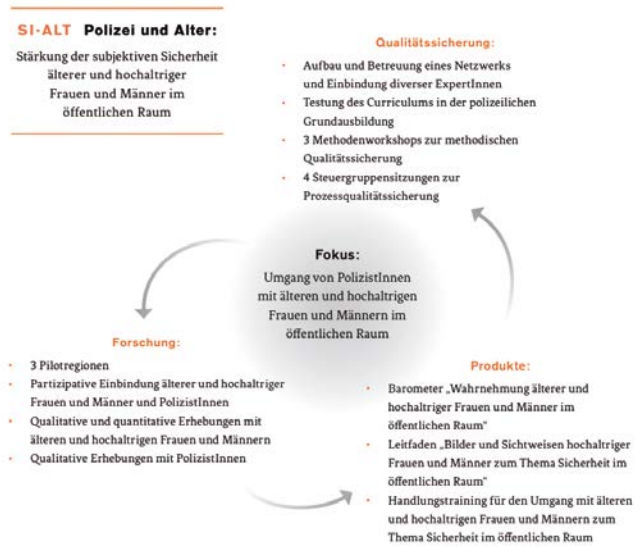
Obwohl die objektive Sicherheit im Sinne des Rückgangs von Straftaten steigt, spiegeln sich diese Entwicklungen nicht immer in der subjektiven Einschätzung der Bevölkerung wider. Obwohl in Österreich mehrere (nationale und internationale) Befragungen, die sich mit dem subjektiven Sicherheitsgefühl der Bevölkerung beschäftigen, durchgeführt wurden und werden, ist wenig darüber bekannt, wie sich die subjektive Sicherheitswahrnehmung älterer und hochaltriger Frauen und Männer im Detail darstellt und wie diese Bevölkerungsgruppen in der Polizeiarbeit bestmöglich berücksichtigt werden können. Insbesondere berücksichtigen bisherige Studien weder methodisch noch in der Auswertung der Daten die große Heterogenität innerhalb der Gruppe der älteren Frauen und Männer.

Um den mit dem demographischen Wandel einhergehenden Herausforderungen gerecht zu werden, adressiert SI-ALT folgende Fragestellungen:

- Wie unterscheiden sich die subjektiven Sicherheitswahrnehmungen innerhalb der Gruppe der älteren Menschen und welche Bedürfnisse resultieren daraus für verschiedene Lebenslagen im Alter?
- Mit welchen Irritationen und Verunsicherungen älterer und hochaltriger Personen sind PolizistInnen konfrontiert?
- Wie können diese Erkenntnisse für die Entwicklung von zielgruppenadäquaten Strategien und Maßnahmen im öffentlichen Raum genutzt werden?
- Wie kann das generierte Wissen zur Unterstützung in der Handlungssicherheit für PolizistInnen didaktisch und methodisch nutzbar gemacht werden?
- Wie können Forschungen zu einer heterogenen Zielgruppe dazu beitragen, dass in der polizeilichen Praxis vorherrschende Rollenbilder reflektiert und durch aktuelle Bilder des Alters erweitert werden?

Diesen Fragestellungen will SI-ALT gerecht werden, indem durch quantitative und qualitative Erhebungen in drei Pilotregionen mit unterschiedlicher Besiedelungsdichte (Wien, Bruck a.d. Mur und Tamsweg) die Sichtweisen älterer und hochaltriger Frauen und Männer sowie jene von PolizistInnen zum Thema Sicherheit im öffentlichen Raum erhoben werden.

Auf Basis der partizipativen Erhebungen werden im Projekt SI-ALT folgende Produkte entwickelt, die einen wertvollen Beitrag zur Präventions- und Kommunikationsarbeit und zum Umgang von PolizistInnen mit älteren und hochaltrigen Menschen leisten:



Projektskizze SI-ALT

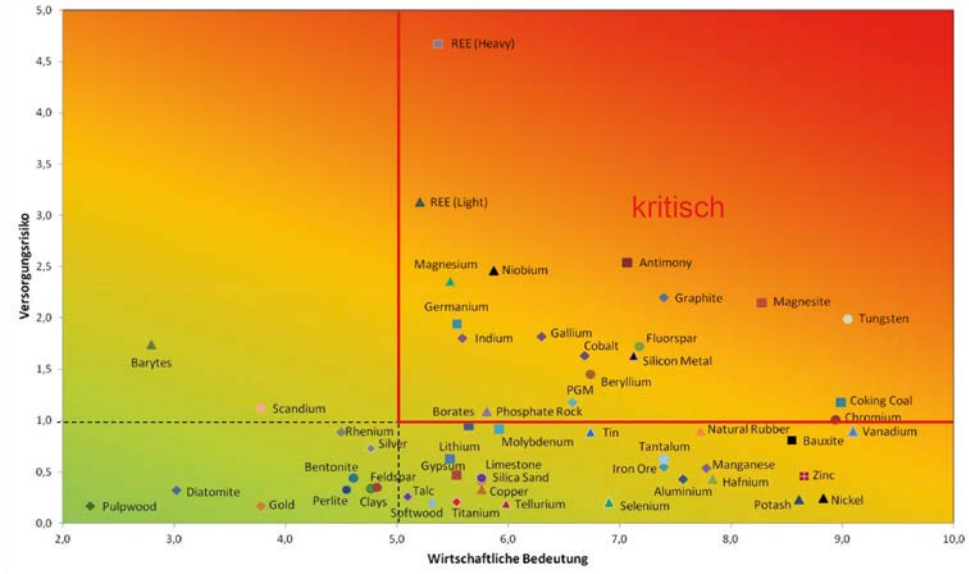
- Ein Barometer zur Darstellung der objektiven Sicherheitslage und der subjektiven Sicherheitswahrnehmung älterer und hochaltriger Frauen und Männer,
- ein Leitfaden zur Sensibilisierung von PolizistInnen für neue Bilder des Alter(n)s und zur Darstellung der Bedürfnisse, Risiken und Irritationen einer heterogenen Zielgruppe im öffentlichen Raum und
- ein Curriculum für die polizeiliche Aus- und Fortbildung zur Stärkung der Präventions- und Kommunikationsarbeit für den polizeilichen Alltag, das PolizistInnen in ihrer Handlungssicherheit im Umgang mit älteren und hochaltrigen Frauen und Männern unterstützen soll.

Projektleitung
queraum. kultur- und sozialforschung
Projektpartner
- Bundesministerium für Inneres
- Universität Wien, Institut für Soziologie
- WU Wien, Kompetenzzentrum für empirische Forschungsmethoden

Kontakt
Mag. Michael Stadler-Vida
queraum. kultur- und sozialforschung
Obere Donaustraße 59/7a, 1020 Wien
Tel.: +43 1 958 09 11
E-Mail: stadler.vida@queraum.org
www.queraum.org

SRA

Entwurf eines indikatorbasierten Frühwarnsystems für kritische strategische Rohstoffe der Energie- und Kommunikationstechnologie



Kritische Rohstoffe 2014, DI Reichl (Bundesministerium für Wissenschaft, Forschung und Wirtschaft)

Ausgangslage

Die Versorgung der österreichischen und der europäischen Industrie mit nicht-energetischen Rohstoffen darf nicht mehr in jedem Falle als gesichert betrachtet werden. Im Hinblick auf eine Reihe von Rohstoffen ist die EU zur Gänze (z. B. Antimon, Kobalt, Molybdän, Niob, Tantal, Seltenerdmetalle) oder großteils (Eisenerz 85 %, Wolfram 75 %, Bauxit 95 %) von Importen abhängig.

Die Empfindlichkeit österreichischer High-Tech-Industrien ist dort besonders groß, wo die Möglichkeit fehlt, knappe und teure Rohstoffe zu substituieren. Frühwarnsysteme können helfen, die damit verbundenen Risiken zu minimieren. SRA (Strategisches Lagezentrum für Ressource-Analysis) setzte sich zur Aufgabe, ein sogenanntes Lagezentrum als Frühwarnsystem zu designen, das Entwicklungen bei kritischen Rohstoffen rechtzeitig erkennen kann.

Projektinhalte und -schritte

Im **Arbeitspaket 1** wurde eine Ist-Analyse zu Stakeholdern und Faktenlage durchgeführt.

- Identifikation nationaler und internationaler Stakeholder sowie eine europaweite Recherche über die Bedeutung kritischer Rohstoffe in den nationalen Energieagenturen über das European Energy Network.

- Darstellung der Bedeutung der Sozialen Netzwerkanalyse für ein Lagezentrum inklusive Erstellung einer Recherche- und Formatvorlage als Grundlage für die Netzwerkanalysen eines Lagezentrums. Exemplarische Durchführung einer konkreten Netzwerkanalyse (Datenbankabfrage in der Unternehmensdatenbank ORBIS und Patentabfrage zu 18 kritischen Rohstoffen).
- Interviews mit folgenden ExpertInnen: Univ. Prof. Dr. Leopold Weber (IOC der Weltbergbaukongresse), Mag. Dr. Robert Holnsteiner, (BMWFW), DI Christian Reichl, (BMWFW), Dr. Martin Brunkhorst (Europäische Investitionsbank), Mag. DI Dr. Alfred Maier (Montanuniversität Leoben).

Die Analysen lassen den Schluss zu, dass starker Bedarf nach einem Lagezentrum für Ressourcen-Analysen gegeben ist. Dieses muss sich für eine wirtschaftliche Tragfähigkeit idealerweise international ausrichten und Dienstleistungen anbieten, welche über jene von anderen Anbietern wie z. B. der Deutschen Rohstoffagentur (DERA) hinausgehen. Das heißt, es müssen Dienstleistungen definiert werden, die für potenzielle Käufer einen Mehrwert darstellen (wie z. B. Lagebild, Risikolagebild, Netzwerkanalyse, Forecast, Foresight, kombinierter Forecast/Foresight, Horizon Scanning, Stoffflussanalysen, Analyse dynamischer Systeme, Szenarioanalyse, Supply Chain-Analyse). Eine mögliche Dienstleistung können Soziale Netzwerkanalysen sein.

Im **Arbeitspaket 2** wurden Designvorschläge zur Aufbau- und Ablauforganisation des Strategischen Lagezentrums beschrieben. Dieser Teil beinhaltet neben einer umfassenden Darstellung aller für das Lagezentrum in Frage kommenden Methoden auch die Abschätzung der notwendigen Kapazitäten sowie Vorschläge zum Aufbau eines Executive Information Systems (EIS). Hier wird dargelegt, mit welchen Herausforderungen ein Strategisches Lagezentrum konfrontiert sein wird. Es wird jene Informationslogistik skizziert, die für die Gewinnung, Verarbeitung, Analyse und Kategorisierung erforderlich sein wird. Zusätzlich werden infrastrukturelle Fragen behandelt.

Für die **Use Cases** wurden zwei Rohstoffe ausgewählt: „Seltene Erden" als Beispiel für eine kritische Rohstoffgruppe für die Herstellung von Produkten der Informations- und Telekommunikationstechnologie sowie „Palladium", dessen Einsatz in zukunftsträchtigen Technologien vielfältig ist (Katalysatoren, miniaturisierte Kondensatoren, Meerwasserentsalzung, Elektrodenmaterial in Brennstoffzellen, Speichermaterial für Wasserstoff in Wasserstoffautos).

Für diese beiden hochkritischen Rohstoffe erfolgt die Darstellung der Wechselwirkungen bzw. Abhängigkeiten zwischen Rohstoffen, Akteuren, hauptbetroffenen Wirtschaftssektoren sowie Technologieentwicklung. Die Praktikabilität bzw. Funktionalität des erarbeiteten Konzepts für ein strategisches Lagezentrum wird so evaluiert.

In **Arbeitspaket 4** wurden die konkreten Anforderungen an ein Lagezentrum beschrieben, so dass im **Arbeitspaket 5** ein Betriebsführungskonzept erstellt werden konnte. Zuerst wurde das Qualifikationsprofil der MitarbeiterInnen und der Arbeitsaufwand in Personenmonaten abgeleitet. Außerdem erfolgte die Spezifizierung der notwendigen Betriebsmittel bzw. der Büroinfrastruktur, um Investitionskosten für die Errichtung und Gemeinkosten für den laufenden Betrieb berechnen zu können. Abschließend erfolgte die Kalkulation der Gesamtkosten für ein Lagezentrum.

Projektleitung
Österreichische Energieagentur,
Austrian Energy Agency (AEA)
Projektpartner
- Zentrum für Risiko- und Krisenmanagement (ZRK)
- Universität für Bodenkultur, Department für Wirtschafts- und Sozialwissenschaften, Institut für Produktionswirtschaft und Logistik
- AIT – Austrian Institute of Technology GmbH

Kontakt
Prof. Herbert Lechner
Österreichische Energieagentur,
Austrian Energy Agency (AEA)
Mariahilfer Straße 136, 1150 Wien
Tel: +43 1 5861524-0
E-Mail: office@energyagency.at
www.energyagency.at

VR Training

Virtual Reality Training für ABC-Abwehr und Sicherheits-Einsatzkräfte

Österreichs ABC-Abwehrkräfte trainieren Schutz- und Abwehrmaßnahmen gegen die Wirkung von atomaren, biologischen und chemischen Kampfmitteln, zum Schutz kritischer Infrastruktur und aller Bürger des Landes. Ziel des Projekts Virtual Reality Training für ABC-Abwehr und Sicherheits-Einsatzkräfte war die Erstellung einer Studie, die sich mit der qualitativen Verbesserung, Kostenreduktion und Effizienzsteigerung von ABC-Abwehr-Trainingsmaßnahmen mit Hilfe von Virtual Reality (VR)-Technologien befasst.

Im Rahmen des Projekts wurden in einem ersten Schritt international sich im Einsatz befindliche VR-Trainingssysteme von der TU Wien analysiert sowie die Anforderungen der beiden involvierten Bedarfsorganisationen – Bundesministerium für Landesverteidigung und Sport und Rotes Kreuz Innsbruck – erhoben. Auf Basis der Ergebnisse dieser beiden Studien wurden aktuelle Virtual Reality Hard- und Softwaresysteme sowie Systeme zur kosteneffizienten Erstellung von Trainingsszenarien von der TU Wien mit der Zielsetzung untersucht, die Anforderungen der Bedarfsträger abzudecken. Da keines der am Markt befindlichen Systeme alle Anforderungen abdecken kann, wurde von der TU Wien ein neuartiges und innovatives Konzept zum Training von mehreren Benutzern in einer immersiven virtuellen Umgebung beschrieben. Im Detail wurden für dieses zukünftige Trainingssystem die dafür notwendigen Hard- und Softwarekomponenten aufgeführt, sowie erläutert, welche Forschungs- und Entwicklungsmaßnahmen zur Umsetzung notwendig sind. Basierend auf diesem vorgeschlagenen Konzept wurden die für die Evaluierung von Trainingsergebnissen notwendigen Evaluierungsmaße von der TU Wien wie auch vom BMLVS erhoben und beschrieben, wie diese technisch erfasst und ausgewertet werden können. Abschließend wurde für das zukünftige immersive Trainingssystem eine Architektur zur Gewährleistung der organisatorischen und technischen Sicherheit entwickelt (AIT, XYLEM Technologies).

Die durchgeführte Studie führte zu einer Reihe von neuen Erkenntnissen und Forschungstätigkeiten, die im Rahmen von zwei wissenschaftlichen Aufsätzen international veröffentlicht wurden. Auf Basis des beschriebenen zukünftigen immersiven VR-Trainingssystems, gekoppelt mit der entwickelten Sicherheitsarchitektur und den Trainingsszenarien, kann ein innovatives System entwickelt werden. Dessen Alleinstellungsmerkmale sind:

- ein voll-immersives Training für mehrere Probanden
- ein mobiles und transportables Setup, das in beliebigen Seminarräumen rasch mit einer geringen Menge an Hardware aufgebaut werden kann
- die Möglichkeit, die virtuelle Welt durch natürliches Gehen zu erkunden, so dass Stress und Erschöpfung realistisch simuliert werden können

Die Studie hat den Bedarf eines solchen immersiven VR-Trainingssystems aufgezeigt, um in Zukunft Trainingsszenarien zu

ABC-Training mit Aufklärungsfahrzeug und abgesessener Aufklärungseinheit

Einsatzkräfte des Österreichischen Bundesheeres bei einer Übung in Österreich

Einsatzkräfte des Österreichischen Bundesheeres bei einem Erdbeben in der Türkei

ermöglichen, die mit derzeitigen Mitteln nicht umsetzbar sind, entweder aufgrund von möglichen realen Gefahren oder auf der hohen Kosten, wie beispielhaft in den Bildern illustriert.

Außerdem hat die Analyse existierender VR-Trainingssysteme ergeben, dass das Training mit Hilfe von nicht-immersiven 3D-Simulationen bereits von vielen militärischen und zivilen Bedarfsträgern weltweit eingesetzt wird. Aufgrund der exzellenten Zusammenarbeit von TU Wien und BMLVS ist die Fortsetzung der Kooperation hin zu einer ersten technischen Umsetzung des methodisch erarbeiteten Systems geplant.

Weiterführende Informationen:

- Mossel, Peer, Göllner, Kaufmann. Requirements Analysis On A Virtual Reality Training System For CBRN Crisis Preparedness. 59th Annual Meeting of the International Society for the Systems Sciences (ISSS), Berlin, 2015.
- Mossel, Peer, Göllner, Kaufmann. Towards An Immersive Virtual Reality Training System For CBRN Disaster Preparedness, International Defense and Homeland Security Simulation Workshop (DHSS). 12th International Multidisciplinary Modeling & Simulation Multiconference (I3M), Bergeggi, 2015.

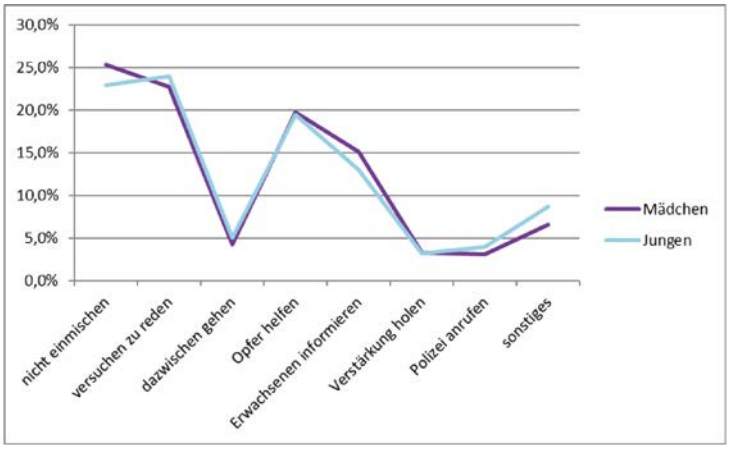
Projektleitung
TU Wien, Institut für Softwaretechnik und Interaktive Systeme

Projektpartner
- Bundesministerium für Landesverteidigung und Sport
- AIT – Austrian Institute of Technology
- Xylem – Science and Technology Management GmbH
- Rotes Kreuz Stadt Innsbruck (RK)

Kontakt
Priv.-Doz. Dr. Hannes Kaufmann,
DI Dr. Annette Mossel
TU Wien, Institut für Softwaretechnik und Interaktive Systeme
Favoritenstr. 9-11/188/2, 1040 Wien
Tel.: +43 1 58801 18893
E-Mail: mossel@ims.tuwien.ac.at

Zivilcourage 2.0

Mechanismen und Wirkungsweisen zivilcouragierter Interventionen durch Jugendliche im Umgang mit wahrgenommener Gewalt im Internet



Projekt „Peer Violence"-Sparkling Science (BMWFW). Eigene Darstellung.

Jugendliche sind besonders häufig mit virtuellen Übergriffen in Form von Beschimpfungen, Belästigungen, Mobbing, Erpressungen bis hin zu körperlichen Gewaltandrohungen und -ausübungen konfrontiert. Darüber hinaus sind die Online- und Offline-Lebenswelten Jugendlicher zunehmend komplex vernetzt: Cyber-Opfer sind auch im realen Leben Opfer, Übergriffe finden in beiden Handlungskontexten statt.

Übergriffe im Web 2.0 werden von Jugendlichen als besonders schwerwiegend erlebt. Eine bereits abgeschlossene Studie des Projektteams zur Wahrnehmung von Gewalt unter 12- bis 15-jährigen weiblichen und männlichen Jugendlichen zeigte, dass Übergriffe und Beschimpfungen im Internet als nahezu ebenso gravierend eingestuft werden wie reale Gewaltübergriffe. Die Gründe dafür liegen vermutlich darin, dass Übergriffe im Internet zum Teil noch massiver ausfallen als im realen Alltag, da virtuelle Distanz und Anonymität häufig zu einer Enthemmung der TäterInnen führen. Oft ist Jugendlichen die emotionale Tragweite ihrer Handlungen gar nicht bewusst. Zudem potenzieren sich Übergriffe zusätzlich durch die vielfältigen medialen Möglichkeiten. Die Bandbreite reicht von Beschimpfungen, Provokationen, Beleidigungen, Verleumdungen, Verbreitung von Gerüchten, Bloßstellungen, sexuellen Übergriffen (z. B. Versenden von Nacktbildern, „Sexting", Aufforderung zu sexuellen Handlungen vor der Webcam), Veröffentlichung entwürdigender Fotos und Videos, Cybermobbing, Verfolgung, Konfrontation mit gewalttätigen Videos bis hin zu konkreter Androhung körperlicher Gewalt.

Davon betroffene Jugendliche erfahren Übergriffe meist allein vor dem Computer oder Smartphone, oft ist es ihnen nicht möglich, in der unmittelbar erlebten, emotional belastenden Situation überhaupt handlungsfähig zu sein. Das Einbeziehen Erwachsener ist in der Regel nicht erwünscht, am ehesten werden FreundInnen zu Rate gezogen.

Belastend ist aber vor allem, dass die Übergriffe vor einem großen Kreis unbeteiligter Dritter (sog. Online-Bystander) öffentlich zur Schau gestellt werden: Neben VoyeurInnen, die an der Demütigung der betroffenen Person Gefallen finden und häufig für die weitere Verbreitung von Bildern oder Videos sorgen, gibt es auch MitläuferInnen, die sich dem Gruppendruck beugen, Desinteressierte, die sich heraushalten, überforderte Personen, die nicht wissen, was sie dagegen tun könnten bzw. aus Angst, selbst zum Opfer zu werden, lieber nicht eingreifen, und schließlich einen kleinen Anteil an Personen, die für das betroffene Opfer Partei ergreifen. Obwohl gerade diese vielfältige Öffentlichkeit hohes Interventionspotenzial hat, scheint Zivilcourage im Web 2.0 in der Forschung kaum Thema zu sein.

In der oben erwähnten Studie des Projektteams wurden Jugendliche auch dazu befragt, ob und wie sie bei verschiedenen typischen Gewaltszenarien im Alltag jugendlicher Peers intervenieren würden. Die Analysen zeigten ein überraschendes Ergebnis, wie aus der Grafik zu entnehmen ist: Zum Thema „Mobbing in Facebook", bei dem eine Gruppe Jugendlicher dargestellt wurde, die diffamierende und herabwürdigende Inhalte über eine dritte Person aus dem eigenen Peer-Umfeld postet, gaben auffallend viele der befragten Jugendlichen an, sich in einem solchen Fall nicht einmischen zu wollen.

Dieser Befund und die Erkenntnis, dass es kaum Studien gibt, die sich gezielt mit Zivilcourage im Web 2.0 beschäftigen, haben das Forschungsteam dazu veranlasst, das bislang in der Sicherheitsforschung und -praxis kaum berücksichtigte hohe Präventionspotenzial jugendlicher Online-Bystander in den Mittelpunkt zu rücken.

Projektziel ist es, jene zugrundeliegenden Faktoren, Mechanismen und Wirkungsweisen zu identifizieren, die zivilcouragiertes Handeln Jugendlicher in Online-Kontexten fördern oder hemmen. Untersucht wird außerdem, welche unterschiedlichen Rollen und Funktionen nicht direkt beteiligte Dritte in Online-Kontexten annehmen.

Das Forschungsvorhaben fokussiert damit also nicht klassische Täter-/Opferkonstellationen, sondern geht der Frage nach, was Jugendliche als unbeteiligte Dritte dazu bewegt, spezifische Rollen und Funktionen einzunehmen.

Die Studie startet mit einer explorativen Phase und eruiert mittels Gruppendiskussionen mit Jugendlichen und ExpertInneninterviews typische Szenarien, in denen zivilcouragiertes Verhalten Jugendlicher in Online-Kontexten gefragt ist. Wir fragen, unter welchen Bedingungen hier Zivilcourage gelingen kann und welche Handlungsmodelle dafür geeignet sind. Die Gruppendiskussionen werden nach Alter (Zielgruppe: 14 bis 18 Jahre) und Geschlecht variiert (jüngere bzw. ältere, gleich- bzw. gemischtgeschlechtliche Gruppen).

Im quantitativen Teil wird eine Vignettenstudie unter 14- bis 18-jährigen SchülerInnen durchgeführt. Vignetten sind kurze Situationsbeschreibungen, die systematisch variiert und im Rahmen einer Fragebogenerhebung eingesetzt werden. Dabei werden die im qualitativen Teil eruierten Bedingungen und Handlungsoptionen in unterschiedliche Online Zivilcourage-Settings umgesetzt, die typische Situationen repräsentieren, in denen zivilcouragiertes Verhalten von Online-Bystandern gefragt ist. Die konkrete inhaltliche Gestaltung erfolgt mit Unterstützung von Jugendlichen, da diese die Erfahrungswelt ihrer Peer-Gruppe kennen und so wichtige jugendadäquate Darstellungselemente (z. B. visuelle Gestaltung, angemessene Wortwahl) berücksichtigt werden können. Befragt werden ca. 1.600 SchülerInnen in Wien, die Auswahl erfolgt über eine geschichtete Zufallsauswahl mit Berücksichtigung unterschiedlicher Schultypen.

Aufbauend auf den Ergebnissen wird in Zusammenarbeit mit den Projektpartnern ein jugendgerechtes Interventionsrepertoire sowie ein umfassendes Informations-, Schulungs- und Trainingsangebot ausgearbeitet, um Zivilcourage von Jugendlichen auch im Internet nachhaltig zu fördern.

Projektleitung
Universität Wien, Institut für Soziologie
Projektpartner
- Mag.ª Dr.in Ingrid Kromer, Kirchliche Pädagogische Hochschule Wien/Krems
- Bundeskriminalamt
- Österreichisches Institut für angewandte Telekommunikation
- Mauthausen Komitee Österreich

Kontakt
Ass. Prof.in Mag.a Dr.in Ulrike Zartler
Mag.a Dr.in Christiane Atzmüller
Universität Wien, Institut für Soziologie
Rooseveltplatz 2, 1090 Wien
Tel.: +43 1 4277-48244
E-Mail: ulrike.zartler@univie.ac.at;
christiane.atzmueller@univie.ac.at
www.soz.univie.ac.at

Kontakte

Programmverantwortung

Bundesministerium für Verkehr, Innovation und Technologie (bmvit)
Sektion III – Innovation und Telekommunikation
Stabsstelle für Technologietransfer und Sicherheitsforschung
1030 Wien, Radetzkystraße 2
Web: www.bmvit.gv.at
www.kiras.at

Kontaktpersonen

Dr. Ralph Hammer
Tel.: +43/1/711 62-65 2109
E-Mail: ralph.hammer@bmvit.gv.at

Mag. Lukas Siebeneicher
Tel.: +43/1/711 62-65 3125
E-Mail: lukas.siebeneicher@bmvit.gv.at

Programmmanagement

Österreichische Forschungsförderungsgesellschaft mbH (FFG)
1090 Wien, Sensengasse 1

Kontaktpersonen

DI Johannes Scheer
Tel.: +43/5/7755-5070
E-Mail: johannes.scheer@ffg.at

Christian Brüggemann
Tel.: +43/5/7755-5071
E-Mail: christian.brueggemann@ffg.at

Impressum

Herausgeber
Stabsstelle für Technologietransfer und Sicherheitsforschung,
Bundesministerium für Verkehr, Innovation und Technologie,
MR Dr. Gernot Grimm

www.kiras.at
www.ffg.at/programme/kiras
www.bmvit.gv.at

Gestaltung
beyond.ag

Produktion
Lindenau Productions

Juli 2017