Falsche Rufnummern: Die Täter geben sich als Mitarbeiter der Polizei aus und verlangen Geld für die Einstellung eines angeblichen Ermittlungsverfahrens.

Stimmen, Bilder, Texte

Fachleute aus der Polizei, Wissenschaft und Forschung referierten bei einer Tagung in Wien über neue technische Methoden zur Verbrechensbekämpfung.

Kooperationspartner des Symposiums „Smart World – Smart Media – Smart Police“ am 24. und 25. November 2015 in Wien waren die Bundeskriminalämter Österreich und Deutschland, das Bayerische Landeskriminalamt, das Landeskriminalamt Baden-Württemberg und das schweizerische Bundesamt für Polizei (Fedpol).

An der zweitägigen Veranstaltung, die in der Landesverteidigungsakademie des Bundesheeres stattfand, beteiligten sich mehr als 200 Teilnehmer aus 14 Staaten. Es gab unter anderem Vorträge über die forensische Suche in Videoarchiven, den Umgang mit Videomassendaten und Metadaten, Textanalyse, die Analyse von Kurznachrichten in der polizeilichen Fallarbeit, die Aufbereitung von Massendaten und die automatische Sprecheridentifizierung.

Sprechererkennung. Dr. Stefan Gfrörer vom Bundeskriminalamt Wiesbaden, Fachbereich für Sprechererkennung, Tonträgerauswertung und Autorenerkennung, stellte das von der EU finanzierte Forschungsprojekt „Privacy Enhanced Speaker Identification at Global Reach“ vor, ein Projekt zum Aufbau einer biometrischen Stimmendatenbank.

Stimmen sollen gespeichert und mit bereits gespeicherten Stimmen abgeglichen werden. Ähnlich, wie es mit anderen biometrischen Merkmalen eines Menschen, etwa der DNA, Fingerabdrücken oder Gesichtern der Fall ist. Die Stimme eines Unbekannten in Telefongesprächen, auf Internetplattformen oder in sozialen Medien soll identifiziert und mit anderen Stimmprofilen verglichen werden können. Damit sollen vor allem Terrorverdächtige und Mitglieder von kriminellen Organisationen ausgeforscht werden können. An dem Forschungsprojekt sind 19 Partner aus Polizei, Wissenschaft und Industrie beteiligt. Es läuft bis 2018.

Polizei und Mobilität. Stefan H. Ruscher, MSc von der Firma *SYNYO GmbH* präsentierte das Kiras-Projekt „IMOPOL+ – iMobility und Polizei. Das Projekt verfolgt das Ziel, Mobilitätskonzepte und deren Auswirkungen im polizeilichen Umfeld zu untersuchen. Mit dem Projekt sollen Vorschläge für Maßnahmen erarbeitet werden, die die Effizienz von Einsatzorganisationen und den Schutz von kritischer Infrastruktur steigern. Zum Themenfeld *iMobility* gehören etwa neue Assistenzsysteme (wie Adaptive Cruise Control, Spurhalteassistenten, Sensoren zur Umfeldüberwachung), selbst-

FOTO: FOTOLIA/GAJ RUDOLF

Symposium „Neue Technologien“: 200 Teilnehmer aus 14 Staaten.

fahrende Fahrzeuge, Fahrzeugidentifikation in komplexen Verkehrssituationen und Cybersecurity von integrierten Komponenten. Die sich daraus ergebenden Herausforderungen liegen unter anderem in der Verhinderung des Missbrauchs von IT-Technologien in Pkws, dem Schutz von Persönlichkeitsrechten und in den Risiken der Sammlung von Daten. Die Chancen neuer Konzepte und Technologien bestehen vor allem in der verbesserten Koordination des Verkehrs, der erhöhten Sicherheit durch Assistenzsysteme und Kommunikation, im umfassenderen Schutz von kritischer Infrastruktur und in der Kriminalitätsprävention.

Durch die Einbeziehung des Bundesministeriums für Inneres als Hauptbedarfsträger sowie des *Kuratoriums für Verkehrssicherheit (KFV)* und des *Österreichischen Automobil-, Motorrad- und Touringclubs (ÖAMTC)* soll relevantes Wissen genutzt werden, um praxisnahe Analysen durchzuführen und um zukünftige Einsatzszenarien und -strategien abzuleiten.

Gemeinsam mit dem *Virtual Vehicle Research Center (VIF)* führt die *SYNYO GmbH* neben den fachlichen Analysen auch verstärkt Vernetzungsaktivitäten mit internationalen Experten und Anbietern im Bereich iMobility durch, um IMOPOL+, das erste Projekt zum Thema „iMobility im polizeilichen Umfeld“, auch auf europäischer Ebene zu positionieren.

Metadaten aus Videoaufzeichnungen. Walter Kuhn, *PKE Electronics AG* und Johannes Traxler, *TBT GmbH,* stellten das Forschungsprojekt „AVA Search – Forensische Suche in Videoarchiven“ vor. Videoüberwachungssysteme verfügen über große Datenspeicher für Bild- und Metadaten. Die Suche nach Personen entspricht oft der Suche nach der Stecknadel im Heuhaufen. „Forensische Suchsysteme“ sollen

FOTO: BK/GERD THURNER

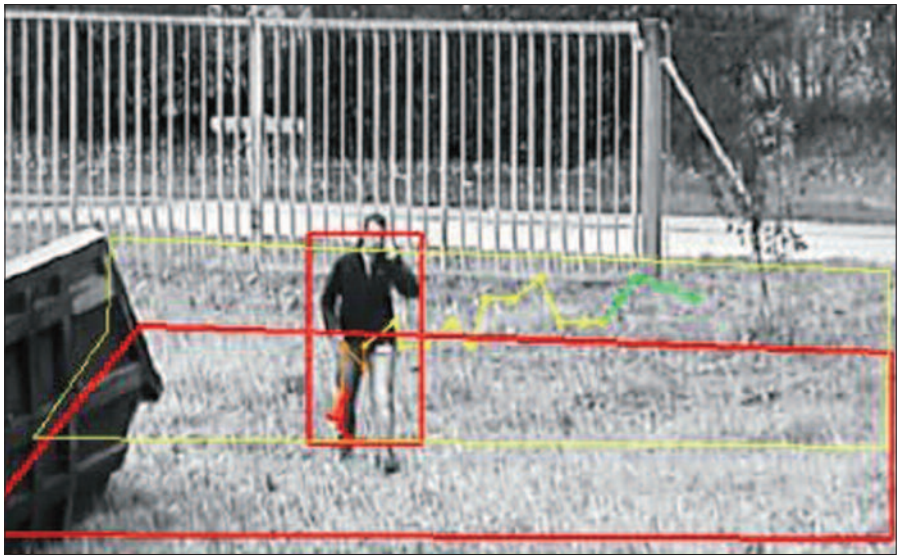
Kurznachrichten können beweiserhebliche Informationen enthalten.

die zielgerichtete Suche erleichtern und beschleunigen. Das *AVASYS-Managementsystem* von *PKE Electronics AG (www.pke.at)* ermöglicht es, beinahe beliebige Objekteigenschaften aus dem Videobild extrahieren zu können und sie mit anderen Informationen etwa von Zutritts- und Gebäudemanagement bis hin zu Brandmeldesystemen zu kombinieren. Die Herausforderung im Forschungsprojekt „AVA Search“ ist es, eine Lösung zu entwickeln, die algorithmisch und visuell den Benutzer möglichst rasch zu seinem gewünschten Suchereignis innerhalb der Video- und Metadaten führt. Dabei sollen die Daten durch eine Art „forensische Lupe“ immer mehr auf den eigentlichen Suchkreis eingeschränkt werden.

Personentracking. Man sucht zum Beispiel eine bestimmte Person, von der bekannt ist, dass sie eine gewisse Größe hat, einen roten Pullover trägt, sich zu einer gewissen Zeit durch eine Tür bewegt hat und fluchtartig das Gebäude verlassen hat. Das Ziel von forensischen Systemen ist es, durch die Kombination von Türkontaktgebern mit Personentracking, Farbraumsegmentierung, Ultraschall- Geschwindigkeitssensoren oder People-Counting-Systemen diese Person von den vielen anderen herauszufiltern. Der Benutzer erhält nach der Eingabe der Eigenschaften erste Vorschläge in Form von Bildern, die er dann durch Selektieren immer weiter einschränkt und damit den „Suchradius“ in dem Raster verringert. Er erhält immer ein Suchergebnis grafisch dargestellt.

Damit dies funktioniert, müssen der Eigenschaftsraum bzw. die Objekteigenschaftsvektoren dynamisch gewählt und soweit wie möglich normiert werden, sodass es zu keiner Übergewichtung von Eigenschaften kommt. Das Projekt „AVAsearch“ wird von der *Österreichischen Forschungsförde-*

Foto: Fotolia/Africa Studio



Personentracking: Forensische Suchsysteme sollen die zielgerichtete Suche nach Personen erleichtern und beschleunigen.

rungsgesellschaft mbH (FFG) im Rahmen des Schwerpunktes „Frontrunner – Förderung von Vorhaben im Feld der technologischen Spitzenposition" gefördert.

Caller-ID-Spoofing. Manuela Schmidt vom bayerischen Landeskriminalamt erklärte unter anderem das Vorgehen von Kriminellen, die mit gefälschten Telefonnummern Menschen anrufen und vorgaukeln, sie seien zum Beispiel von einer Polizei- oder Justizdienststelle. Diese Methode wird „Caller-ID-Spoofing" genannt.

Die Täter verschaffen sich Zugang zu internetbasierten Telefonnetzwerken und manipulieren die Rufnummernanzeige. Sie simulieren bei ihrem Anruf zum Beispiel die Nummer dieser Dienststelle. Sie sagen den Betroffenen zum Beispiel, dass gegen sie ein Strafverfahren laufe, das gegen die Zahlung von mehreren Tausend Euro eingestellt werden würde. Die Täter benutzen ein „Voice-over-IP-Programm", das die tatsächliche Rufnummer unterdrückt und eine beliebige andere Nummer – etwa der Polizei – beim Angerufenen aufscheinen lässt. Rufen Betroffene die angezeigte Nummer zurück, landen sie bei der Polizei.

„Spoofing-Dienste" machen das Ändern der Anruferkennung möglich. Die mitgesendete Telefonnummer lässt sich beliebig auswählen. Diese Möglichkeit besteht in unregulierten Kommunikationsnetzen (z. B. Internet), ist aber in regulierten öffentlichen Netzen verboten – ob VoIP- oder klassische Telekommunikationsnetze, die den jeweiligen Telekommunikationsgesetzen unterliegen. In Österreich sind der Polizei bislang keine Schadensfälle bekannt.

Manuela Schmidt erläuterte auch, wie „Verkehrsdaten" entstehen und wo sie gespeichert werden. „Verkehrsdaten" sind Daten, die bei der Nutzung von Telekommunikations-Diensten durch den Erbringer der Dienste erhoben, verarbeitet oder genutzt werden (z. B. Telefonnummern und Verbindungszeiten, Standortdaten von Mobiltelefonen, IP-Adressen und Zeitraum der Zuweisung zu einem Anschluss bei der Nutzung von Computern).

Analyse von Kurznachrichten. Michael Spranger, Florian Heinke und Prof. Dr. Dirk Labudde befassten sich in einer Studie an der Hochschule für angewandte Wissenschaften in Mittweida in Deutschland mit der Analyse von Kurznachrichten in der polizeilichen Fallarbeit.

Die Ermittlungen umfassen immer mehr auch die Analyse und Auswertung moderner Kommunikationsmittel. Da die Speicherkapazitäten der Geräte größer werden, werden Kurznachrichten oder Messenger-Logs selten gelöscht. Für Ermittler ist das von Vorteil, weil beweiserhebliche Informationen nicht verlorengehen. Die Analyse dieser Daten ist zeitaufwendig. 15.000 gespeicherte Kurznachrichten eines Handys oder Smartphones sind nicht ungewöhnlich. Das wären ausgedruckt etwa 600 DIN A4-Seiten. Hinzu kommen Nachrichten von Messengern, wie Whats-App, deren Menge schnell das Zehnfache dieser Anzahl erreichen kann. In Fällen von organisierter Kriminalität wächst der Suchraum mit jedem Mitglied und jedem verwendeten Gerät. Die Suche fallrelevanter Informationen in diesen Daten erfolgt noch weitgehend manuell.

Kurznachrichten fehlen in der Regel korrekte grammatikalische Strukturen und sie weisen neben unregelmäßig fehlendem Kontext Tippfehler und syntaktische Fehler auf. Das Vokabular orientiert sich kaum an Sprachkonventionen und ist geprägt von Deliktsart sowie Bildungsstand und sozialem Umfeld des Schreibers. Dazu kommen Fehler durch die Autokorrekturfunktion und die Verwendung atypischer Emoticons und Abkürzungen sowie zusätzlich eingefügte Zeichen, um Gefühlslagen auszudrücken (z. B. „Haaaallo", „seeeehr"). Eine Herausforderung stellen Dialekte und die Verwendung von gruppenspezifischem Vokabular dar. Häufig anzutreffen ist diese Form der Kommunikation, im Zusammenhang mit der Verwendung „versteckter Semantik", vor allem im Drogenmilieu. „Versteckte Semantik" verweist auf eine Art steganografischer Codes. Steganografie ist die verborgene Speicherung oder Übermittlung von Informationen.

Eine automatisierte Analyse dieser Daten ist technisch noch nicht möglich. Spranger, Heinke und Labudde haben ein forensisches Analysewerkzeug für Kurznachrichten (Mobile Network Analyzer – MoNA) entwickelt, das den Aufwand für die manuelle Analyse und Entscheidung über die Beweiserheblichkeit einzelner Textpassagen erheblich verringert, indem der Suchraum drastisch eingeschränkt wird.

Ziel der Entwicklung ist, den manuellen Aufwand so zu verkürzen, dass diese Art der Analyse zum Standardvorgehen wird und die monotone manuelle Tätigkeit ablöst. Die Effektivität der verwendeten Algorithmen hängt von der Qualität der verwendeten Fachwörterbücher ab. Eine Reduzierung des Suchraums ist in jedem Fall gewährleistet und führt zu einer Zeitersparnis bei der Analyse.

Das internationale Symposium „Neue Technologien" fand 2015 zum fünften Mal statt. Es gilt als wichtiger Impulsgeber und bedeutende Plattform für die Sicherheitsforschung aus Sicht der Sicherheitsbehörden. 2016 wird das Symposium in Baden-Württemberg abgehalten. *Siegbert Lattacher*

FOTO: PKE ELECTRONICS