Teilnehmerinnen und Teilnehmer sowie Mitglieder des Organisationstems des Symposiums neue Technologien.

Fortschritt oder Risiko?

Moderne Technologien bieten bei polizeilichen Ermittlungen Chancen und neue Möglichkeiten. Dadurch werden auch die Ermittler zukünftig vor neue Herausforderungen gestellt.

Das Internet of Things“ (IoT) und die damit verbundenen Technologien schaffen neue Bedrohungen und ermöglichen Angriffe auf verschiedene digitale Bereiche. Darunter fallen Smart Homes, Industrie 4.0, Digital Citys und selbstfahrende Autos“, sagte der stellvertretende Direktor des Bundeskriminalamtes, Dr. Michael Fischer, beim neunten internationalen Symposium für neue Technologien. Sicherheitsorganisationen würden dadurch vor neue Aufgaben gestellt. „Die Entwicklungen auf diesem Gebiet schreiten unaufhaltsam voran, sowohl was die Chancen als auch die Herausforderungen betreffen. Die Kriminalpolizei ist deshalb ständig gefordert“, betonte Fischer.

Die Veranstaltung findet einmal jährlich statt und soll im Sinne einer länderübergreifenden Plattform dazu beitragen, die Vorteile neuer Technologien in Zukunft bestmöglich nutzen zu können. Die Fachvorträge sowie die Möglichkeit der Vernetzung der Teilnehmer untereinander sollen helfen, die Nachteile und Risiken der neuen Technologien frühzeitig zu erkennen. Ziel dieser Veranstaltungsreihe ist es, Technologieprojekte vorzustellen und Ergebnisse zu präsentieren. Darüber hinaus soll der Forschungsbedarf bei Ermittlungen in der Strafverfolgung und in der digitalen Forensik skizziert werden. Das Symposium fand am 5. und 6. November 2019 in der Landesverteidigungsakademie des Bundesheeres in Wien statt. Rund 200 Interessierte aus den Bereichen Polizei, Militär, Behörden, Wirtschaft und Forschung zählten zu den Teilnehmern.

Neue Technologien. Künstliche Intelligenz (KI), „Big Data“, „Smart Home“ und Industrie 4.0 werden erhebliche Veränderungen bringen, beispielsweise durch den Einsatz von Robotern in verschiedenen Bereichen, etwa der Produktion und dem Dienstleistungs-Sektor. Mehr und mehr Aufgaben werden durch „smarte“ Maschinen übernommen. Man denke an selbstfahrende Kraftfahrzeuge oder Kassensysteme in Supermärkten, die es den Kunden ermöglichen, ihren Einkauf selbst abzurechnen. Das Smartphone gehört zum Alltag, immer mehr Menschen entscheiden sich auch in den eigenen vier Wänden für den Einsatz smarter Technologien. Beispielsweise die Steuerung von Rollos und der Heizung per App, Überwachungsvideos auf dem Smartphone, Sprachassistenten wie „Alexa“, vernetzte Fernseher und Kühlschränke, die selbstständig online Lebensmittel nachbestellen.

Risikofaktoren. Je mehr Geräte in den Haushalten vernetzt und mit Hilfe von Smartphone-Apps oder online per Fernzugriff steuerbar sind, umso deutlicher werden die Risiken, die damit verbunden sind. Oft wird bei neuen Technologien die Sicherheit vernachlässigt. Internetverbindungen werden nicht verschlüsselt, Passwörter werden aus den Voreinstellungen des Herstellers übernommen, anstatt selbst ein starkes Passwort zu generieren, Kameras und Mikrofone sind dauernd aktiviert.

Für Cyber-Kriminelle bilden die im Trend liegenden Geräte ein beliebtes Einfallstor. Ein Krimineller kann die Kontrolle über das gesamte Heimnetzwerk und alle daran angeschlossenen Smart-Home-Anwendungen übernehmen. Die Manipulation von Geräten, wie das Ein- oder Ausschalten der Heizung bis hin zum Öffnen der Fenster, Türen oder des Einfahrtstores sind ebenso denkbar wie der Diebstahl oder Missbrauch sensibler persönlicher Daten. Kriminelle werden so in die Lage versetzt, die Opfer zu erpressen. Man denke an eine durch „Ransomware“ infizierte smarte Heizung, die erst wieder in Betrieb genommen werden kann, wenn das Opfer einen durch die Kriminellen festgesetzten Geldbetrag überweist – ähnlich der Systematik, die beim „Polizeitrojaner“ Anwendung findet.

Sicherheitsvorkehrungen treffen. Bei der Errichtung eines „Smart Homes“ können die Nutzer selbst dazu beitragen, ihre Geräte sicherer zu machen

FOTO: ANDREAS MITAK

und dem Risiko eines Hackerangriffs entgegenwirken. Maßnahmen wie die regelmäßige Aktualisierung der Software von Geräten – wenn neue Sicherheitsupdates verfügbar sind – die Änderung voreingestellter Standardpasswörter, die Aktivierung der Firewall des Routers oder die Aktivierung der Verschlüsselung der Kommunikation der IoT-Geräte, sind nur einige Beispiele. Darüber hinaus sollten IoT-Geräte nur dann mit dem Internet verbunden sein, wenn ein Fernzugriff notwendig ist. Ansonsten ist es ratsam, die Verbindung beim Verlassen des Eigenheims zu unterbrechen.

Datenschutz. Thematisiert wurde auch, dass dem Datenschutz durch die Industrie bei der Software- und Hardwareentwicklung in der Vergangenheit zu wenig Aufmerksamkeit geschenkt wurde. Die Datensicherheit bei der Verarbeitung von personenbezogenen Daten soll in Zukunft durch Maßnahmen wie „Pseudonymisierung“ und Verschlüsselung personenbezogener Daten (z. B. Passwortsicherung von Dateien) noch effektiver gestaltet werden. „Pseudonymisierung“ bedeutet das Ersetzen des Namens und anderer Identifikationsmerkmale einer Person durch ein Kennzeichen, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Der wissenschaftliche Leiter des Zentrums für digitale Menschenrechte in Wien, Dr. Christof Tschohl, erläuterte in diesem Zusammenhang die Begriffe „Privacy by Design“ und „Privacy by Default“. Übersetzt bedeuten sie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Rechtliche Grundlage ist die EU-Datenschutz-Grundverordnung (EU-DSGVO), die in Österreich unmittelbar angewendet wird.

„Privacy by Design“ heißt, dass der Datenschutz bereits bei der Konzipierung und Entwicklung von Soft- und Hardware zur Datenverarbeitung berücksichtigt wird. „Privacy by Default“ setzt voraus, dass die Werkseinstellungen, beispielsweise bei einer smarten Heizung, datenschutzfreundlich auszugestalten sind. Es sollen somit speziell jene Nutzer geschützt werden, die weniger technisch versiert und dadurch nicht in der Lage sind, bei einem Gerät die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.

Hersteller in die Pflicht nehmen. Durch die geltenden Regelungen sind Unternehmen nun gefordert – in puncto Datenvermeidung und Datensparsamkeit. Bei bestimmten Verstößen können die Aufsichtsbehörden Geldbußen bis zu 20 Millionen Euro – im Fall eines Unternehmens bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres – verhängen, je nachdem, welcher Betrag höher ist. Zum Beispiel bei Verletzung der Betroffenenrechte (z. B. Recht auf Löschung und auf „Vergessenwerden“).

Biometrische Gesichtserkennung. „Gespeicherte Lichtbilder haben dann einen Sinn, wenn die Gesichtserkennung zur Auswertung dieser Bilder verwendet wird“, betonte Bernhard Egger vom bayerischen Landeskriminalamt. Der leitende Kriminaldirektor und Experte für Gesichtserkennung brachte zum Ausdruck, dass die Flut an zur Verfügung stehendem Bildmaterial, das noch dazu im Internet für jedermann zugänglich ist, ein neues Feld für die polizeilichen Ermittlungen eröffnet.

Egger zeigt sich davon überzeugt, dass sich die digitale Bilderkennung neben der Auswertung von Fingerabdrücken und DNA-Spuren zur dritten Säule im Erkennungsdienst etablieren werde.

Erhöhtes Bildaufkommen. Bilder, speziell von Gesichtern, haben in den vergangenen Jahren sowohl als Spur und Beweismittel als auch für die Fahndung wesentlich an Bedeutung gewonnen. Das liegt zum einem daran, dass sich das Bildaufkommen in den vergangenen Jahren immens erhöht hat, beispielsweise durch Smartphone-Fotos, den Ausbau der Videoüberwachung und die rasante Verbreitung von Bildern über das Internet und in sozialen Netzwerken. Zum anderen haben sich die technischen Möglichkeiten zur Auswertung und Nutzung dieser Bilder erheblich weiterentwickelt.

Nach Information des bayerischen Landeskriminalamtes sind in Deutschland bis dato 3,5 Millionen Personen erkennungsdienstlich erfasst worden. Das entspricht einer Auswahl von 5,5 Millionen Bildern. In Bayern sollen künftig mehr Tatverdächtige durch biometrische Gesichtserkennung identifiziert werden. „Die Gesichtserkennung ist elementar, um bereits gespeicherte Bilder mit Bildern von unbekannten Tätern abzugleichen“, erläutert Egger.

Mannheim: Intelligente Videoüberwachung erkennt Verhaltensmuster.

Bayern hat ein landesweites Gesichtserkennungssystem im Einsatz.

Recherche im Gesichtserkennungssystem. Zur Identifizierung von Personen wird Bildmaterial von Überwachungskameras, gefälschten, verlorenen oder weggeworfenen Ausweisen, von Aufnahmen mit Handys (Videos und Bilder) oder aus dem Internet herangezogen. Es erfolgt ein Abgleich der gesuchten Person mit allen in „INPOL-Zentral“ einliegenden erkennungsdienstlichen Bildern und aktuellen Fahndungsfotos. Das polizeiliche Informationssystem „INPOL“ ist ein elektronischer Datenverbund zwischen Bund und Ländern in Deutschland und wird beim Bundeskriminalamt (BKA) betrieben. „Vereinfacht erklärt, werden bei der Gesichtserkennung Gesichtszüge vermessen und in Daten umgewandelt“, erläuterte Egger. Als Ergebnis liefert die Gesichtserkennungssoftware beispielsweise eine Auswahl von 200 Gesichtern mit den ähnlichsten Übereinstimmungen. Jedes Gesicht besteht aus einer Vielzahl individueller anatomischer Merkmale. Das sind Merkmale, die unveränderlich sind. Zum Beispiel die Abstände der Augen oder der Wangenknochen. Anhand solcher Merkmale vergleichen ausgebildete Lichtbildexperten das Suchbild mit den Bildern von bereits bekannten Straftätern.

Bayern nützt seit 2019 ein eigenes landesweites Gesichtserkennungssystem. Dieses System soll die automatische Suche, das automatische Clustern und Erkennen von Gesichtern in Videos ermöglichen. „Verwendet ein Krimineller für seine Tat einen gefälschten Reisepass, bietet oftmals nur das Bild einen Anhaltspunkt für weitere Ermittlungen“, sagte Egger und hob damit die Bedeutung der Gesichtserkennung für die Polizeiarbeit nochmals hervor.

Intelligente Videoüberwachung. Im Dezember 2018 wurde in der Stadt Mannheim am Hauptbahnhof eine intelligente, algorithmusbasierte Videoüberwachung in Betrieb genommen. Es handelt sich um ein gemeinsames Projekt mit dem *Frauenhofer Institut* und soll zur Bekämpfung der Straßenkriminalität beitragen. Zur Umsetzung des Projektes musste das baden-württembergische Polizeigesetz geändert werden. Das System erkennt in einem ersten Schritt Personen und Objekte. Im zweiten Schritt analysiert die intelligente Videoüberwachung Körperhaltungen und Bewegungsabläufe. Gewaltsame Übergriffe durch Schläge oder Tritte sollen erkannt werden. Die intelligente Videoauswertung informiert in einem weiteren Schritt einen Videobeobachter der Polizei. Zu diesem Zweck wird ein geografisch referenzierter Hinweis in eine Lagekarte eingezeichnet. Dieser Hinweis wird vom Polizisten überprüft, der aufgrund seiner Wahrnehmung entscheidet und gegebenenfalls weitere Maßnahmen trifft – eine automatische Alarmierung der Einsatzkräfte durch das System erfolgt nicht.

Ziel ist es, die Arbeit der Polizisten vor den Überwachungsmonitoren zu erleichtern und effizienter zu gestalten. „Bei der intelligenten Videoüberwachung geht es um das Erkennen polizeilich relevanter Bewegungsabläufe mithilfe automatischer Bildauswertung, nicht um eine Gesichtserkennung oder sonstige Methoden zur Identifikation von Menschen“, erklärte Polizeidirektor Klaus Pietsch vom Polizeipräsidium Mannheim.

Weitere Themen der Veranstaltung waren „Audiovisuelle Methoden zur Erkennung von manipuliertem Bild-, Video- und Audiomaterial, „Intelligente Unterstützungssysteme – Schichtwechsel mit Predective Planning – User Storys zur agilen Einsatzplanung“ oder „Fahrzeugautomatisierung – Neue Herausforderungen für polizeiliche Tätigkeiten und Maßnahmen.

Gernot Burkert

FOTOS: FRAUNHOFER IOSB, GOODPICS/STOCK.ADOBE.COM