

# KI in der Kriminalitätsbekämpfung

Beim 12. internationalen Symposium „Neue Technologien“ am 5. und 6. November 2025 in Bern wurden der Einsatz künstlicher Intelligenz für polizeiliche Zwecke erörtert und Projekte vorgestellt.

Das Symposium befasste sich mit der Zukunft der Kriminalitätsbekämpfung aus dem Blickwinkel technischer Innovationen und gesellschaftlicher Herausforderungen. Es sei, so der stellvertretende Leiter der Direktion Fedpol, Simon Spörri, notwendig, mit der technischen Entwicklung Schritt zu halten bzw. ihr zuvorzukommen. Auch in den von der Digitalisierung neu erschlossenen Lebensbereichen müsse die Polizei vertreten sein.

Tobias Broser, Leiter Information-Management von Europol, zeigte auf, dass die Zahl der fast 1,6 Millionen Polizistinnen und Polizisten in der EU vergleichbar wäre mit der Zahl der Mitarbeiter größter weltweiter Privatunternehmen. Rechne man ein, dass im Durchschnitt der Bevölkerung etwa 2,3 Prozent hochqualifiziert seien, würde dies auf etwa 35.000 Angehörige dieser Berufsgruppe zutreffen. Seine Behörde habe eine Koordinierungsfunktion. Europol beobachte Entwicklungen, prüfe deren Relevanz für die Polizei und erstelle Berichte an die politische Ebene. Treten in einem Mitgliedsstaat auf polizeilicher Ebene Probleme auf, wird erfragt, ob diese auch bei anderen Staaten bekannt geworden sind und welche Abhilfe geschaffen wurde.

Falls das Problem neu ist, wird an einer Lösung gearbeitet. Bei der Entwicklung der KI für polizeiliche Zwecke sind spezielle Trainingsdaten erforderlich. Hierfür steht eine eigene Sandbox mit operativen Daten zur Verfügung, samt etwa 50 Tools. Der Zugriff ist über die *Europol Platform for Experts (EPE)* möglich. Für große Datenmengen wird die KI zur Schlüssel-Technologie.

**KI im Einsatz.** „80 bis 90 Prozent aller virtuellen Angriffe bauen auf öffentlich zugänglichen Daten auf“, berichtet Juan Vargas, *Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAQ*. Öffentlich zugängliche Daten stellen in Zeiten generativer KI, maschinellen Lernens (Mustererkennung zur Vorhersage



**Forschungsprojekt READY (Reading The Enemy): systematische Evaluierung eines Flughafens aus Täterperspektive**

künftigen Verhaltens), Bildanalyse und NLP (Sprache verstehen und generieren) Angriffsmöglichkeiten für Betrugshandlungen dar. Im *Lernlabor Cyber-Sicherheit Faktor Mensch* wurden Ransomware-Angriffe, etwa über USB-Sticks, E-Mail-Anhänge, Phishing-Websites, erläutert und gezeigt, wie einfach und schnell die Stimme eines Menschen geklont (*Voice Cloning*) und zu Voice Phishing (*Vishing*) eingesetzt werden kann.

Ferner können mit dem erlangten Datenmaterial gezielte Angriffe durchgeführt werden, bei denen Angreifer personalisierte E-Mails oder Nachrichten nutzen, um Personen oder Unternehmen zu täuschen (*Spear Phishing*). Der Schwerpunkt des Lernlabors liegt auf der Stärkung der Resilienz des Nutzers gegenüber derartigen Angriffen.

Die Open-Source-Dokumentensuchmaschine *LOOM* des Eidgenössischen Departments für Verteidigung, Bevölkerungsschutz und Sport ermöglicht das rasche Auffinden von Dokumenten samt zugehörigen Metadaten und in weiterer Folge die Suche nach bestimmten Begriffen. Demonstriert wurde dies an dem Winston Churchill zugeschriebenen Satz „no sports“, zu dem zahlreiche Fundstellen gefunden wurden. Das Programm bietet Übersetzungen unter anderem aus Hebräisch oder Hindi an sowie eine Verschlagwortung der Fundstellen und die KI-gestützte Erstellung einer Zusammenfassung.

**KI-Projekte.** KI kann auf Bildern Gesichter finden (*Detektion*) und diese einer Person zuordnen (*Verifikation*). Die Erkennungsleistung liegt bei 97,3 Prozent und ist damit, wie IT-Experte Ganen Sethupathy ausführte, bereits auf nahezu menschlichem Niveau. Die Programme dazu (*OpenCV2*, *DeepFake*) sind Open Source, also frei erhältlich und können mit KI-gestützten Browsern direkt auf einer Bodycam, einem Smartphone oder einer Drohne verwendet werden. Sicherheitsrelevante Objekte (Waffen) und Szenen können erkannt werden

– auch beispielsweise Drohnenschwärme. Wird mit Hilfe von KI der menschliche Körper auf ein Skelett reduziert, können Körperhaltung, Gesten und Bewegungen erfasst und analysiert werden (*Rigging*). Das ermöglicht, Schläge oder Prügeleien, aber auch Stürze oder das Zusammenbrechen von Menschen in öffentlichen Bereichen zu erkennen. Damit kann eine automatische Detektion und Alarmierung von Einsatzkräften erfolgen. *Skeleton Detection* ermöglicht, auf Grund von Handgeschwindigkeit, Stoß- und Zielrichtung zu erkennen, ob Gewalt ausgeübt wird. Kausalzusammenhänge zwischen Stoß und Fall müssen allerdings an Hand der Umstände erschlossen werden, da bloßes Stolpern auch ohne Gewalteinwirkung erfolgen kann.

Raumtiefenerkennung ermöglicht, eine sich nähernde Person zu detektieren, was der Einsatzkraft durch ein akustisches Warnsignal angezeigt werden kann.

Durch das Sammeln von Einsatzdaten könnte Erfahrungswissen aufgebaut werden – als Hilfsmittel für Entscheidungen in ähnlichen Lagen. Ähnlichkeitsalgorithmen können aktuelle Lagen mit früheren Fällen vergleichen, bewerten und letztlich bei der höchsten Gesamthähnlichkeit Handlungsempfehlungen ableiten.

Robert Pelzer, TU Berlin, und Stefan Taing, *Munich Information Labs*, berichteten über das noch bis April 2026

laufende Projekt *RadiGaMe* (*radigame.de*), mit dem Lösungsansätze für eine verbesserte Strafverfolgung, Früherkennung und Prävention von sicherheitsgefährdender Radikalisierung entwickelt werden. Relevante Quellen (Gaming-nahe Plattformen und Messenger-Dienste) werden nach szenenspezifischen Begriffen und Wörtern durchsucht und gesammelt. In einem weiteren Schritt werden Videos und Worthäufigkeiten transkribiert, analysiert und letztlich zu einem Produkt verarbeitet, das zu prüfende Vorlagen (*Postings*) hinsichtlich ihrer strafrechtlichen oder gefahrenbezogenen Relevanz in einem einfachen Ampelsystem darstellt. Die KI hat sich vor allem bei der Verarbeitung, der Datenanalyse und bei der Strukturierung als hilfreich erwiesen, hat jedoch kein diagnostisches Sinnverständnis. Die Interpretation der Daten muss durch den Menschen erfolgen, einschließlich einer allfälligen Nachjustierung des Systems.

Moderne Ermittlungen bringen eine fragmentierte und unstrukturierte Datenflut mit sich (beschlagnahmte Mobiltelefone, Chatverläufe, E-Mails, soziale Medien, Bilder und Videos). Mit dem im Februar 2025 begonnenen und bis Jän-



**Spezialgerät zur Erfassung der Seriennummern von Banknoten**

ner 2027 laufenden, vom österreichischen Finanzministerium geförderten Forschungsprogramm *EVIDENZ (Effiziente Verarbeitung Digitaler Indizien)*, das die Projektleiterin, Mina Schütz des *Austrian Institute of Technology (AIT)*, vorstellte, sollen, KI-gestützt, irrelevante oder redundante Daten ausgefiltert werden, Inhalte nach Fallrelevanz priorisiert und Entitäten, Zeitstempel und Be-

weismitteltypen semantisch verknüpft werden. Ziel ist, Zusammenhänge zwischen digitalen Spuren transparent und nachvollziehbar darzustellen.

Die Daten müssen zunächst automatisiert, minimiert und gefiltert sowie priorisiert werden. Bilder können Dokumente (Rechnungen, Belege, Verträge) enthalten, die herausgefiltert werden müssen. Manipulierte oder generierte Bilder (*Deepfakes*) in Videos sollen erkannt werden. Die integrierte Media Intelligence Plattform (*mi*) ermöglicht auch eine Geolokalisierung. Herausforderungen liegen in der Einhaltung rechtlicher und ethischer Standards.

Im Projekt *LODI (Local Obfuscation of Device Identities)* der Schweizer zentralen Stelle für Informationstechnik im Sicherheitsbereich geht es darum, die „Fingerprints“ von Geräten der Consumer-Funktechnologie (WLAN, Bluetooth, Mobilfunk u. a.) an Hand ihrer funktechnisch hinterlassenen Spuren zu erfassen und auf dieser Basis beispielsweise den Weg eines Einbrechers durch ein Gebäude nachzuverfolgen.

Referenten des deutschen Bundeskriminalamtes und des LKA Nordrhein-Westfalen befassten sich mit dem auto-

matischen Auffinden von Hand- und Fingerabbildungen in Massendaten und in weiterer Folge mit der Erkennung der für Identifikationszwecke relevanten Bereiche auf Fingerkuppen und Handinnenflächen. Für das Projekt werden Partner gesucht, die Trainingsdaten zur Verfügung stellen, damit neue Modelle trainiert und validiert werden können.

Das deutsche Bundesland Baden-Württemberg hat Grenzen zu Frankreich, der Schweiz und Österreich. Unterschiedliche Funkstandards und Sprachen erschweren die, zunächst nur über die jeweiligen Leitstellen mögliche, Kommunikation der Einsatzorganisationen (BOS) untereinander. 2010 wurde zwischen den Einsatzorganisationen als direkte Funkverbindung eine solche im oberen Kurzwellenbereich (CB-Funk) eingerichtet, was, wie von der Polizei Baden-Württemberg berichtet wurde, in weiterer Folge zu einer erfolgreichen grenzüberschreitenden Zusammenarbeit im Bereich Deutschland, Schweiz, Österreich und Liechtenstein (D-CH-AT-LI) geführt hat. Seit Jänner 2024 läuft das Projekt *Total Cross Border Communication (TCBC)* mit dem Ziel, eine nahtlose, automatisierte Kommunikation zwischen mehreren Staaten herbeizuführen. Für Sprachübersetzung in Echtzeit sollen KI und maschinelles Lernen eingesetzt werden. Was dabei an KI-Komponenten entwickelt wird, soll europaweit verwendet werden können (*build once – deploy many*). Herausforderungen stellen Fachsprachen im BOS-Bereich dar sowie Lücken in den rechtlichen Grundlagen (DSGVO, AI-Act).

**Erfahrungsberichte.** Die Kantonspolizei Zürich, die für die Sicherheit am Flughafen Zürich zuständig ist, hat mit Beginn Jänner 2023 im Rahmen des Forschungsprojekts *READY (Reading The Enemy)* mit einer systematischen Evaluation des Gesamtsystems Flughafen aus Täterperspektive begonnen. In Form von Red-Teams wurden Perspektive und Taktiken potenzieller Angreifer simuliert. Wie reale Täter hatten die aus dem eigenen Personalstand gebildeten Teams die Aufgabe, sich zur Erfüllung eines Auftrags Informationen über Sicherheitsmaßnahmen zu verschaffen, die Tat zu planen und letztlich simuliert durchzuführen. Aufgaben waren Schmuggel, Platzierung einer Bombe, Verursachung hohen Schadens, Vermeidung von Entdeckung. Ziel war es, Einsicht in die Vorgangsweise potenzieller



**Das Symposium „Neue Technologien“ wird jährlich abwechselnd von den Landeskriminalämtern Bayern und Baden-Württemberg, dem österreichischen Bundeskriminalamt und der Schweizer Bundespolizei (Fedpol) veranstaltet.**

Täter zu gewinnen, die vorhandenen Sicherheitsmaßnahmen zu evaluieren und zu verbessern. Den Red-Teams standen die Blue-Teams der tatsächlichen Einsatzkräfte gegenüber. Gesteuert wurde über die Spielleitung. Gezeigt hat sich, dass durch das gegnerorientierte Denken blinde Flecken im System aufgedeckt werden konnten.

Über Erfahrungen und Herausforderungen bei der forensischen Sicherstellung verschlüsselter Speichersysteme berichtete Harald Wenisch, Fachhochschule Wiener Neustadt. Er wies darauf hin, dass die am Gehäuse eines Datenträgers angegebene Seriennummer nicht mit der des eigentlichen Datenträgers übereinstimmen müsse und berichtete über Möglichkeiten, für forensische Zwecke Daten im Live-Betrieb sicherzustellen.

Am Beispiel eines illegalen Chemie-Labors, in dem Suchtgift hergestellt wurde, beleuchtete Jürgen Bügler vom bayerischen Landeskriminalamt die Wichtigkeit der Ausbildung von Ersteinsatzkräften. Diese müssten, wie auch bei illegaler Herstellung von Sprengstoffen, darin geschult werden, die Ausgangsstoffe zu erkennen, also beispielsweise was auf Kanistern etikettiert ist. An technischer Ausrüstung steht für CBRN(E)-Lagen eine apparative Vor-Ort-Messtechnik (massenselektive Verfahren, Spektralanalysegeräte) zur Verfügung. Der Referent berichtete über eine diesbezügliche Übung mit der analytischen Taskforce (ATF) München, die auch Probenentnahmen und deren Weiterleitung an Speziallabore zur kriminaltechnischen Untersuchung umfasst hat.

Über Probleme, die sich beim Einsatz von IMSI-Catchern im 5G-Netz ergeben, berichtete ein Mitarbeiter des

Dienstes Überwachung Post- und Fernmeldeverkehr der Schweiz.

**Bargeldscanner.** Die unverwechselbare DNA eines Bargeldscheins ist seine Seriennummer. Mit dieser könnten, wie Gerrit Stehle, *Elephant&Castle Capital GmbH*, ausführte, physische Geldströme verfolgt werden. Die vorherige Erfassung der Seriennummern wäre etwa bei Überfällen auf Bargeldtransporte, Bankomatsprengungen, Lösegelderpressungen oder Geldwäsche (Einzahlung von Bargeld bei Money-Transfer-Services) ein Erkenntnisgewinn für Ermittlungsbehörden, wenn die Scheine wieder in Umlauf kommen. Geldzählmaschinen könnten mit Lesegeräten zur Erfassung der Serien-Nummern von Geldscheinen ausgestattet werden. Dass dies bisher noch nicht der Fall war, wurde mit mittlerweile gelösten technischen Schwierigkeiten bei der Zeichenerfassung (OCR-Technik) erklärt.

Ein derartiges Gerät ist transportabel und kann auch über einen Akku betrieben werden. Ausschlaggebend für diese Zusatzausrüstung war, dass bei der Aufnahme der Seriennummern sichergestellt Geldscheine im sechsstelligen Wertbereich der Besitzer sich weigerte, elektrischen Strom für das Zähl- und Erfassungsgerät zur Verfügung zu stellen. Die Nummern mussten damals händisch erfasst werden.

**Das Symposium neue Technologien** wird jährlich abwechselnd von den Landeskriminalämtern Bayern und Baden-Württemberg, dem österreichischen Bundeskriminalamt und der Schweizer Bundespolizei Fedpol veranstaltet. Tagungsort für das 13. Symposium wird Wien sein. *Kurt Hickisch*