Hans-Jörg Kreowski und Aaron Lye

Sicherheitsforschung: informationstechnische Aufrüstung der Polizei

Mit dem Schlagwort Digitalisierung wird heute oft ein Prozess bezeichnet, der schon seit einigen Jahrzehnten anhält, aber immer noch mehr Fahrt aufnimmt. Mit den Fortschritten in der Informations- und Kommunikationstechnik, in der Informatik und in jüngster Zeit insbesondere auch in der Künstlichen Intelligenz (KI) und Robotik ist eine allmähliche und fortschreitende Nutzung in nahezu allen gesellschaftlichen Bereichen verbunden. Das gilt auch für die Polizei. Dieser Beitrag zeigt die vielfältigen Auswirkungen von Sicherheitsforschung auf die Nutzung von Informationstechnik durch die Polizei.

Einleitung: Gewachsene Bedeutung der Sicherheitsforschung

Der Staat unternimmt erhebliche Anstrengungen, die Forschung im Bereich „ziviler Sicherheit“ voranzutreiben. Seit 2007 hat das Bundesministerium für Bildung und Forschung rund 650 Millionen Euro in die Förderung von praxisnahen Sicherheitslösungen gesteckt, bei deren Entwicklung Wirtschaft, Wissenschaft und Einrichtungen der inneren Sicherheit zusammenarbeiten. In dem aktuellen Programm Forschung für die zivile Sicherheit 2018 bis 2023 geht es um Nutzung von KI und insbesondere von Robotik. Des Weiteren laufen in dem EU-Forschungsförderprogramm Horizon 2020 (Projektlaufzeit: 2014-2020, Budget: rund 70 Mrd. Euro) zahlreiche Teilprojekte, in denen Informationstechnik- (IT) und Rüstungsunternehmen, Forschungseinrichtungen, Universitäten und nationale als auch europäische Strafverfolgungsbehörden zusammenarbeiten. Erwähnenswert ist außerdem die 2017 gegründete deutsche Behörde Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), welche die Aufgabe hat, Behörden des Bundes (Bundeskriminalamt (BKA), Bundespolizei und Bundesamt für Verfassungsschutz) mit Sicherheitsaufgaben im Hinblick auf informationstechnische Fähigkeiten zu unterstützen und zu beraten. Sie ist Forschungs- und Entwicklungsstelle mit den Aufgabenschwerpunkten digitale Forensik, Telekommunikationsüberwachung, Kryptoanalyse und *Big-Data*-Auswertung. Digitale Forensik umfasst die Entwicklung neuer softwaretechnische Methoden und spezielle Hardware zur Auswertung und Archivierung von Daten. Telekommunikationsüberwachung umfasst die

Erforschung und Entwicklung neuer Methoden und Strategien, um auf Telekommunikationsdaten zuzugreifen. Kryptoanalyse beschäftigt sich mit der Vorbereitung und Durchführung praktischer Angriffe auf unterschiedliche IT-Systeme und deren Verschlüsselung. *Big-Data*-Auswertung umfasst das Datamining (also das Durchsuchen großer unsortierte Datenbestände) als auch deren Analyse und Interpretation mittels Maschinellem Lernen.

In diesem Beitrag wollen wir an einzelnen typischen Beispielen zeigen, welche aktuellen technologischen Entwicklungen von der Polizei genutzt oder hinsichtlich zukünftiger Nutzung geprüft werden:

- Maschinelles Lernen
- Gesichtserkennung
- Kombinierte Datenbanken
- Predictive-Policing
- Social-Media und Open-Source-Intelligence
- Grenzüberwachung und Fluchtwegrekonstruktion
- Erweiterte DNA-Analyse.

Andere Bereiche wie Remote-Forensics/Trojaner, Robotik, Kryptoanalyse, Deanonymisierung und Quantencomputing sparen wir aus, weil sie sich neben den anderen Themen nicht kurz abhandeln lassen.

Maschinelles Lernen

Das aktuell wichtigste Teilgebiet der KI ist Maschinelles Lernen. Unter Verwendung statistischer Verfahren und Softwaretechniken wird ein Modell mit bekannten Daten trainiert, indem es Muster und Strukturen erkennt und anhand einer vorher definierten Logik daraus Schlussfolgerungen zieht, um dann für unbekannte Daten Vorhersagen zu treffen. Dabei erfolgt die Optimierung des Modells anhand einer einzigen Kennziffer, welche die Entwickler_innen festlegen (Schelling 2019). Die Einsatzgebiete sind vielfältig: So können beispielsweise Objekte, Gesichter, Basisemotionen und Laufwege in Fotos und Videos erkannt, Sprache erkannt und übersetzt, Spiele gespielt, oder Daten klassifiziert und Anomalien erkannt werden. Allerdings kann ein Modell nur trainiert werden, wenn genügend Daten und Rechenleistung vorhanden sind. Alle Daten über Menschen enthalten jedoch gesellschaftlich bedingte Verzerrungen. Deshalb macht es beispielsweise einen Unterschied, ob die Gesichtserkennung im Training eine gesellschaftsagnostische Gesamtgenauigkeit optimiert oder Genauigkeiten für Minderheiten mit verrechnet werden. Rassistische und sexistische Weltanschauungen werden hinter vermeintlich neutraler Mathematik versteckt (Schelling 2019). Da es sich um probabilistische Algorithmen handelt, besteht die Gefahr der fehlerhaften Vorhersage. Allerdings neigen Menschen dazu, einer Berechnung übermäßig zu vertrauen[1]. Nichtsdestotrotz bewerben Cloud-Anbieter[2], vor allem *Amazon Web Services,* ihre Dienste erfolgreich bei Strafverfolgungsbehörden in den USA[3].

Gesichtserkennung

In den letzten rund 20 Jahren hat es auf dem Gebiet der Bilderkennung erhebliche Fortschritte gegeben. Das gilt insbesondere auch für die Gesichtserkennung, so dass sich Politik und Bundespolizei ermutigt fühlten, ein Pilotprojekt auf den Weg zu bringen. Nachdem frühere Versuche noch gescheitert waren, wird das Ergebnis des Pilotprojekts zur biometrischen Gesichtserkennung auf dem Bahnhof Berlin-Südkreuz nach einjähriger Erprobung von August 2017 bis Juli 2018 als großer Erfolg gefeiert.[4]

Der technische Versuchsaufbau sah grob skizziert so aus: An drei Stellen des Bahnhofs – ein Eingang, eine Rolltreppe und ein Ausgang – haben vorhandene Kameras Bilder aufgenommen und als Stream an die eingesetzten Gesichtserkennungssysteme gesendet. In allen drei getesteten Systemen (BioSurveillance von Herta Security, Morpho Video Investigator von IDEMIA und Anyvision vom gleichnamigen Unternehmen) wurden mit unterschiedlichen Algorithmen (die neben klassischen Bildanalyseverfahren alle drei auch mit künstlichen neuronalen Netzen arbeiten und damit mit sogenannten lernenden Systemen) die Gesichter auf den Bildern in Templates verwandelt, also nach bestimmten charakteristischen Merkmalen vereinfacht. Die Templates wurden dann automatisch mit den in einer Datenbank gespeicherten Gesichtstemplates der im ersten halben Jahr über 300 Versuchspersonen und im zweiten Halbjahr noch verbliebenen 200 verglichen. Diese hatten sich als regelmäßige Benutzer_innen des Bahnhofs freiwillig gemeldet. Ihre Zahl wurde so gewählt, dass die Auswahl statistisch gesehen repräsentativ war. Im ersten Halbjahr gab es nur ein Template pro Person nach einem guten Foto, im zweiten zwischen zwei und fünf nach Bildern, die mit den Überwachungskameras geschossen wurden. Außerdem wurde mit Hilfe von Transpondern, die die Testpersonen immer bei sich trugen, festgestellt, wer wann welche Beobachtungsstelle passiert hat. So ließ sich die Trefferrate ermitteln als Verhältnis der richtig erkannten Gesichter zu den insgesamt möglichen Erkennungen in Prozent. Als zweites „Güte"-Kriterium wurde die Falschakzeptanzrate gewählt, die in Prozent angibt, wie viele der Erkennungen falsch sind.

Durchschnittlich wurde eine Trefferrate von gut 80 Prozent erreicht, in günstigen Fällen über 90 Prozent. Die Falschakzeptanzrate lag deutlich unter einem Prozent. Das klingt gar nicht viel, bedeutet aber bei 10.000 Gesichtserkennungsvorgängen schon über 30 Personen, die fälschlich als gesucht erkannt werden. In dem Abschlussbericht des Bundespolizeipräsidiums 2018, dem noch viele weitere Details entnommen werden können, werden auch Faktoren genannt, die die Gesichtserkennung behindern und erschweren. Dazu gehören schlechte Lichtverhältnisse wie Gegenlicht oder starke Schattenbildung sowie ungünstige Kamerawinkel. Gute Ergebnisse werden insbesondere erzielt, wenn die Kamera senkrecht zur Gesichtsebene angebracht ist, was bei Ein- und Ausgängen praktisch unmöglich ist. Brillen, Schals und Makeup sollen die Erkennung nicht wesentlich beeinträchtigen. Aber es ist wohl nicht untersucht worden, wie häufig die Erkennung scheitert, weil die Zielperson nach unten, hinten oder zur Seite schaut, sich stark geschminkt hat, sich verkleidet hat oder das Gesicht verdeckt. Von anderen Bilderkennungsversuchen ist bekannt, dass schon kleinere Veränderungen an den zu erkennenden Objekten die Ergebnisse deutlich verschlechtern können. Bei der Beurteilung des Pilotprojekts muss auch beachtet werden, dass kein einzelnes

der getesteten Systeme aus Sicht der Polizei wirklich zufriedenstellende Ergebnisse erbracht hat, sondern erst eine Kombination zweier Systeme.[5]

Ungeachtet solcher technischer Bedenken muss befürchtet werden, dass Gesichtserkennungssysteme dieser Art im öffentlichen Raum bald Wirklichkeit werden. Das wirft viele weitere Fragen auf. Welche Datenbanken mit den Bildern welcher Zielpersonen werden verwendet? Werden (biometrische) Bilder von polizeilich gesuchten Tatverdächtigen und als Kriminelle eingestuften Personen verwendet, oder werden auch Menschen einbezogen, die als „Gefährder“[6] eingeschätzt werden, ohne dass ein konkreter Tatverdacht vorliegt? Es ist zu befürchten, dass Strafverfolgungsbehörden diese Überwachungstechnologie mit immer mehr Datenbanken vernetzen. Datenschützer_innen (des Bundes und der Länder) sind sich weitgehend einig, dass es sich um einen massiven und ungerechtfertigten Eingriff in die informationelle Selbstbestimmung von Menschen handelt. Die grundlegende Kritik an automatisierter und anlassloser Massenüberwachung ist klar. Menschen verhalten sich unfreier, wenn sie beobachtet werden. Weiter betreffen polizeiliche Maßnahmen und Überwachung überproportional viele Menschen, die Minderheiten angehören. Ist es also nur eine Frage der Zeit, bis solche Systeme eines Tages bei uns wie jetzt schon in China zur sozialen Überwachung und systematisch gegen Minderheiten (vgl. Reuter 2019) eingesetzt werden?

Kombinierte Datenbanken

Im EU-Projekt „Interoperabilität“ werden derzeit alle in EU-Datenbanken vorhandenen Gesichtsbilder und Fingerabdrücke mit Personendaten in einem durchsuchbaren „gemeinsamen Identitätsspeicher“ zusammengeführt (vgl. Monroy 2019a). Einige der Datenbanken bleiben in ihrer derzeitigen Form erhalten, andere werden um weitere biometrische Merkmale ergänzt. Die Daten werden zentral bei der Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA) verarbeitet. Darüber hinaus werden sie durch ein gemeinsames Interface parallel durchsuchbar. eu-LISA ist auch für die technische Verwaltung und die sichere Datenübertragung im Betrieb zuständig. 2020 beginnt die technische Umsetzung, bis 2023 soll das System fertiggestellt werden (vgl. Europäische Kommission 2017 COM(2017) 794 final). Integriert werden (1) das Schengener Informationssystem (SIS II), welches als größte Fahndungsdatenbank Europas Informationen zur Einreise- oder Aufenthaltsverweigerung und zur Verhaftung oder zur verdeckten Kontrolle von Verdächtigen enthält; (2) das *European-Dactyloscopy-System* (EURODAC), welches Fingerabdruckdaten von Asylbewerber_innen und Drittstaatsangehörigen speichert und abgleicht; (3) das Visa-Informationssystem (VIS), welches personenbezogene und biometrische Daten von Antragsteller_innen und Einlader_innen von Kurzaufenthaltsvisa speichert, (4) das neue Einreise-/Ausreisesystem (EES), in welchem personenbezogene und biometrische Daten sowie Zeitpunkt und Ort der Ein- und der Ausreise von Drittstaatsangehörigen, die für einen Kurzaufenthalt in den Schengen-Raum reisen, elektronisch erfasst werden; (5) das ab 2021 verwendete Europäische Reiseinformations- und -genehmigungssystem (ETIAS) , bei dem es sich um ein weitgehend automatisiertes System zur Erfassung und Über-

prüfung der Angaben handelt, die von der Visumpflicht befreite Drittstaatsangehörige vor ihrer Reise in den Schengen-Raum übermitteln; (6) das Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN), bei dem es sich um ein elektronisches System für den Austausch von Informationen über frühere Verurteilungen von Drittstaatsangehörigen durch Strafgerichte in der EU handelt; und (7) Datenbanken von Europol und Interpol. Als Schnittstelle für die ersten sechs wurde ein neues universelles Nachrichtenformat federführend vom BKA entwickelt.[7] Das System integriert auch einen „Detektor für Mehrfachidentitäten", der innerhalb der ersten sechs Datenbanken biometrischen Daten und ihnen zugeordneten Ausweisdokumenten abgleicht. Die existierenden Datenbanken verfügen bereits über ein solches Suchsystem für Fingerabdrücke (vgl. Monroy 2018a). Das Ganze findet unter dem Vorwand der Terrorismusbekämpfung statt. Tatsächlich geht es aber um den Aufbau einer Überwachungsinfrastruktur, um insbesondere Migration in die und innerhalb der EU zu erschweren.

Darüber hinaus ist das BKA auch federführend an dem EU-Projekt *Europäischer Kriminalaktennachweis – Automatisierung der Datenaustauschprozesse* (EPRIS-ADEP)[8] beteiligt, welches ein System entwickelt, um bestimmte biografische Daten, die in nationalen polizeilichen Informationssystemen enthalten sind, verfügbar zu machen und direkte EU-weite Abfragen ermöglichen soll. Hierzu wird die bereits existierende Infrastruktur von Europol[9] genutzt, insbesondere das *Europol-Operations-Network* und die Kommunikationsplattform *Secure-Information-Exchange-Network-Application*.

Predictive Policing

Predictive Policing[10], das mit voraussagende oder vorausschauende Polizeiarbeit übersetzt werden kann, ist im Wesentlichen eine Anwendung quantitativer Analysemethoden der angewandten Wahrscheinlichkeitstheorie und Statistik, um Orte und Zeiten mit hohem Kriminalitätsrisiko, mögliche Straftäter_innen einerseits und gefährdete Opfer andererseits vorherzusagen. Eine weitere Anwendung ist die Erstellung von Profilen, um die Identität von Straftäter_innen anhand der Tatcharakteristika und Tatortspuren einzugrenzen. Im Unterschied zur traditionellen Kriminalitätsanalyse, die ganz ähnliche Ziele verfolgt, erfordert *Predictive Policing* große Datenmengen und ist methodisch wesentlich komplexer. Die eingesetzten Methoden umfassen beispielsweise die systematische Kombination von verschiedenen Datenbanken bei Abfragen und Auswertung, *Datamining*, Regressions- und Klassifikationsanalyse, Clusterverfahren, *Near-Repeat*-Modellierung wahrscheinlicher Wiederholungstaten und Raumzeitanalyse. Ziel ist dabei nicht Genauigkeit, sondern Brauchbarkeit. Und man darf nicht glauben, dass die automatisierte Kriminalitätsanalyse die Kriminalitätsrate senkt. Vielmehr ist es als technokratische Antwort auf ein soziales Problem zu verstehen. Statt die Ursachen von Kriminalität zu beheben, wird die Identifikation von Gefährder_innen und Verdächtigen sowie die Repression optimiert. *Predictive Policing* ist kein Garant, dass sich das ändert oder verbessert. Im Gegenteil ist aufgrund struktureller und institutioneller rassistischer Polizeipraxis (KOP 2016, Sarbo 2019) die Gefahr groß, dass noch mehr Personen unschuldig in Verdacht geraten und dass Methoden

eingesetzt werden, die die grundgesetzlich geschützten Persönlichkeitsrechte einschließlich der informationellen Selbstbestimmung zuwiderlaufen.

Selbst technisch gesehen muss *Predictive Policing* auch dann noch lange nicht erfolgreich sein, weil die Vorhersagen vielleicht auf Daten minderer Qualität beruhen, weil die Analyseergebnisse missverstanden werden wegen der Unkenntnis zugrundeliegender Faktoren oder weil nicht genügend überprüft wird, ob verwendete Vorhersagen überhaupt effektiv waren.

In Deutschland lassen sich auf kriminalpolitischer Ebene vermehrt Implementierungsvorstöße und Pilotprojekte zu Predictive Policing verzeichnen. In mehrere Bundesländer werden unterschiedliche informationstechnische Werkzeuge bereits eingesetzt (vgl. Heitmüller 2019): Bayern und Baden-Württemberg nutzen die kommerzielle Prognosesoftware PRECOBS (*Pre Crime Observation System*) des Instituts für musterbasierte Prognosetechnik IfmPt; Nordrhein-Westfalen nutzt und entwickelt SKALA (System zur Kriminalitätsauswertung und Lageantizipation) auf der Grundlage von SPSS Modeler von IBM; Niedersachsen wiederum benutzt IBM Cognos in dem Projekt preMAP (*predictive Mobile Analytics for the police*); Berlin nutzt die Eigenentwicklung KrimPro (Kriminalitäts-Prognose) und Hessen nutzte die Eigenentwicklung KLB-operativ (Kriminalitätslagebild-operativ), welche kürzlich durch die Software Gotham von Palantin abgelöst wurde (vgl. Singelnstein 2019).

Social-Media und Open-Source-Intelligence

Durch die verbreitete Nutzung von *Social-Media* erfährt *Open-Source-Intelligence* (OSINT), also das Sammeln und Bewerten von öffentlichen Informationen, insbesondere in sozialen Medien eine gravierende Aufwertung für die Informationsgewinnung von Polizei und Geheimdiensten weltweit. Bereits im EU-Projekt CAPER[11] (*Collaborative information Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime*; Projektlaufzeit: 2011 – 2014, Budget: 7 Mio Euro) wurden informationstechnische Werkzeuge entwickelt, um Internetinhalte den Behörden systematisch zugänglich zu machen – einschließlich Bild-, Video-, Sprach- und biometrischer Analyse.[12] Auch in Deutschland gibt es entsprechende Vorhaben und Umsetzungen. Seit 2014 ist bekannt, dass das Zentrum Operative Kommunikation der Bundeswehr, der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz mit mehreren Analysetools Blogs, Foren und soziale Netzwerke systematisch beobachten und analysieren (vgl. Hunko 2014, Meister 2015). Mithilfe statistischer Verfahren sollen gesellschaftliche Stimmungen, Tendenzen, Trends und Auffälligkeiten erkannt werden. Diese sind nicht auf einzelne Personen bezogen, sondern sollen grundsätzliche Aussagen zur Dynamik von Informationsströmen und zur allgemeinen Lageentwicklung im In- und Ausland ermöglichen. Ziel ist die Beherrschbarkeit sozialer Phänomene und politischer Situationen, indem Prognosen berechnet und Gruppen gezielt manipuliert werden.

Jetzt soll die Polizei ebenfalls in sozialen Netzwerken aktiv werden. Das Projekt SENTINEL[13] (Sicherheit im Einsatz durch Open-Source-Intelligence (OSINT) in Einsatzleitstellen, Projektlaufzeit: Januar 2018 bis Juni 2019) verdeutlicht dieses. Es wurden

sogenannte *Intel-Officer* implementiert, die polizeieinsatzbegleitend OSINT-Recherchen durchführen. Oft stehen so den Behörden aktuelle Lichtbilder, Hinweise zum Aufenthaltsort, Informationen zu Hobbies oder Besonderheiten der Örtlichkeiten zur Verfügung. Das orientiert sich an den Niederlanden, wo in sogenannten *Real-Time-Intelligence-Centres* (RTIC), die in den Einsatzleitstellen untergebracht sind, Polizeivollzugsbeamte neben der Datenerhebung in polizeilichen Datensystemen standardmäßig OSINT-Recherchen zu eingehenden Einsätzen durchführen und den Einsatzkräften die Informationen mitteilen.

Neben der individuellen Recherche und Ausforschung stehen die Analyse von Bestrebungen und die Identifikation von Gruppen und Personen im Vordergrund aktueller Polizeiforschung. Hier sind beispielsweise die zwei Projekte RadigZ[14] (Radikalisierung im digitalen Zeitalter – Analyse von Aufrufen zu extremistischen Gewalthandlungen und Straftaten via Internet/Social Media, Projektlaufzeit: Februar 2017 bis Februar 2020) und X-SONAR[15] (Analyse extremistischer Bestrebungen in sozialen Netzwerken, Laufzeit: März 2017 bis Februar 2020) bemerkenswert. Neben einer vertieften Analyse der Wirkungen von Internet-basierter Informationsverbreitung und Propaganda (im Sinne der behördenüblichen, extremismustheoretischen Einstufung als islamistisch, rechtsextremistisch, linksextremistisch) sowie der Identifikation von Gruppen und Personen, die entsprechende Informationen wahrnehmen, ist die Entwicklung zielgruppenspezifischer Gegenmaßnahmen zentrales Anliegen des Projekts. Durch die Analyse von sozialen Netzwerken, Blogs und Foren und die Identifizierung von gruppenspezifischen und individuellen Radikalisierungsmustern sollen Indikatoren zur Früherkennung und Risikoeinschätzung radikaler Tendenzen erarbeitet werden. Zusammen mit den beteiligten Landeskriminalämtern und Behörden wird Software für die Erkennung von Netzwerkstrukturen und zur dynamischen Risikoeinschätzung entwickelt.

Ein anderer Aspekt der Social-Media-Offensive ist die interaktive Propaganda. Das Projekt PräDiSiKo[16] (Präventive digitale Sicherheitskommunikation – ein innovativer Ansatz für Kriminalprävention in sozialen Online-Medien, Projektlaufzeit: November 2016 bis Oktober 2019) behandelt die Erforschung und softwaretechnischen Umsetzung eines neuen Systems, das der Polizei ermöglicht, interaktiv Botschaften über ein soziales Netzwerk an die Bevölkerung zu kommunizieren. Insbesondere sollen spezifische Personengruppen adressiert werden, wobei die Art der Kommunikation und Botschaft von der jeweiligen Gruppe abhängt.

Darüber hinaus arbeiten europäische Polizeibehörden zusammen mit Rüstungsfirmen im Horizon-2020-Programm an diversen Projekten in diesem Bereich. Im Sicherheitsforschungsprojekt „TENSOR“[17] wird eine „Plattform für Terrorismusaufklärung“ im Internet entwickelt. Sie soll automatisierte und teil-automatisierte Werkzeuge kombinieren, um Inhalte in mehreren Sprachen und aus unterschiedlichen Formaten (Text, Bilder, Filme, Tonaufzeichnungen) zur „Förderung von Gewalt“ und „Radikalisierung“ aufzuspüren und automatisch zu erkennen. Die Software soll auch „dialoggestützte Bots“ mit KI nutzen. Gefundene Inhalte werden anschließend kategorisiert und interpretiert, damit sie von Strafverfolgungsbehörden genutzt werden können (Monroy 2019b). Des Weiteren laufen die EU-Projekte TRIVALENT[18] und PROPHETS[19] (je ca. 3 Mio. Euro, Projektlaufzeit TRIVALENT: Mai 2017 – April 2020, Projektlaufzeit

PROPHETS: Mai 2018 – April 2021) in dem unter anderem auch Analysesoftware für OSINT entwickelt werden soll, um Radikalisierungen zu erkennen. Neben der Analyse sind Synthese und Gegenstrategien Projektziele. Einen Schritt weiter geht das aktuelles Projekt Red Alert[20], bei dem die Erkennung und Klassifizierung von Internetinhalten in Echtzeit erprobt wird. Auch hier kommen natürliche Sprachverarbeitung, Analyse sozialer Netzwerke und KI-Methoden zum Einsatz.

Grenzüberwachung und Fluchtwegrekonstruktion

Neben der Identifikation von Menschen anhand biometrischer Merkmale ist die Beobachtung und Vorhersage von Fluchtrouten sowie die interorganisationale[21] und transnationale Zusammenarbeit zwischen Polizei, Behörden, Hilfsorganisationen und anderen involvierten Akteuren Bestandteil der Polizeipraxis im Kontext der Grenzüberwachung.

Zentral ist das Grenzüberwachungssystem Eurosur (*European Border Surveillance*), welches vom europäischen Grenzschutz Frontex betrieben wird und Aufklärungsdaten von Satelliten, Flugzeugen, Drohnen und Fesselballons zusammenführt. Kern des EUROSUR-Systems ist die Satellitenaufklärung. Die Bilder stammen von kommerziellen Satellitendiensten (wie etwa von Airbus, das Bilder seiner Radarsatelliten TerraSar-X und TanDEM-X verkauft) sowie von optischen und radarbasierten Satelliten des EU-Erdbeobachtungsprogramms Copernicus und werden vom Satellitenzentrum der Europäischen Union SatCen erhoben und aufbereitet (vgl. Monroy 2018b). 2018 wurde der Ausbau der technischen Fähigkeiten von Copernicus von der EU-Kommission beschlossen[22]. Das System soll mittels KI „Unregelmäßigkeiten im Schiffsverhalten" detektieren und Informationen zum Standort, der Schiffsbezeichnung und zum abweichenden Verhalten melden. Seit 2017 werden von Flugzeugen (und seit 2018 zusätzlich von Aufklärungsdrohnen) über dem Mittelmeer aufgenommene Videos in ein Lagezentrum der EUROSUR-Zentrale nach Warschau gestreamt, um sie dort in Echtzeit auszuwerten[23]. Im Rahmen des Projekts *FRONTEX Compatible Operational Image* wird die Verbesserung dieser Echtzeit-Übertragung ins Hauptquartier erforscht. Dies betrifft neben Flugzeugen und Drohnen auch Schiffe und Fahrzeuge an Land (vgl. Monroy 2018b). 2019 wurden die Überwachungsfähigkeiten weiter ausgeweitet, sodass mittels Maschinellem Lernen Personen und Objekte auf von Drohnen aufgenommenen Bildern automatisch klassifiziert werden können (vgl. Monroy 2019c).

Aber das ist nur ein Aspekt. 2015 hat der EU-Rat die Kooperation von Europol mit Facebook und Twitter beschlossen (vgl. Krempl 2015). In der Europol-Meldestelle für Internetinhalte wurden zusätzliche Stellen geschaffen, die soziale Medien nach Fluchtaktivitäten durchsuchen und Inhalte (z.B. von Menschen, die bei der Flucht unterstützen) zu löschen. Darüber hinaus wurde der direkte Zugriff auf Tracking-Daten von Facebook beschlossen, wobei die im vorherigen Abschnitt erwähnten Systeme zur Analyse sozialer Medien für diese Zwecke benutzt werden können.

Als letzter Aspekt sei die Auswertung von Smartphones erwähnt. Im deutsch-österreichischen Projekt SmartIdentifikation[24] (Projektlaufzeit: April 2018 – März 2020) forscht die Bundespolizei zur schnellen Auswertung von Dokumenten und der Mobil-

telefone von Geflüchteten. Durch die Analyse unterschiedlicher Daten, wie Ländercodes angerufener Telefonnummern, Kontakte, Top-Level-Domains aufgerufener Websites, Geodaten und der in Textnachrichten verwendete Sprache, sollen Fluchtwege (automatisiert oder teil-automatisiert) rekonstruiert werden.

Erweiterte DNA-Analyse

In einem Konsortium mit dem Namen „*VISible Attributes through GEnomics*" mit dem Akronym „VISAGE" (Projektlaufzeit: 1.5.2017 - 30 April 2021) haben sich mehrere europäische Universitäten sowie Strafverfolgungsbehörden, unter anderem auch das BKA, für die weitere Erforschung der erweiterten DNA-Analyse zusammengeschlossen.[25] Das Projekt wird von der Europäischen Union mit fünf Millionen Euro unterstützt. Das übergeordnete Ziel von VISAGE ist, die Einschränkung der derzeitigen forensischen Nutzung von DNA zu überwinden, indem es sie erweitert und zusammengesetzte Skizzen unbekannter Spender aus so vielen biologischen Spuren und Quellen wie möglich und so schnell wie möglich konstruiert.[26] Das derzeit verwendete standardisierte forensische DNA-Profil ist nur dann erfolgreich, wenn ein gesuchtes DNA-Profil mit dem einer Person übereinstimmt, die entweder direkt über die polizeiliche Untersuchung oder durch die Suche in polizeilichen DNA-Datenbanken auf nationaler oder europäischer Ebene verfügbar ist. VISAGE zielt darauf ab, aus DNA, die sich nicht zuordnen lässt, Rückschlüsse auf Augen-, Haar- und Hautfarbe sowie das biologische Alter mit genomischen Mitteln zu führen. Durch die Kombination dieser sichtbaren Attribute wird eine zusammengesetzte Skizze des unbekannten Spenders konstruiert und auf eine Personengruppe reduziert. Darüber hinaus ermöglichen Alters- und teilweise biogeographische Abstammungsinformationen zusätzlich die Suche in Registern. Als Ergebnis des Projekts formulierte das Konsortium die Entwicklung und forensische Evaluation von Prototypenwerkzeugen auf der Grundlage von massiv paralleler Sequenzierung zur gleichzeitigen Analyse der identifizierten DNA-Prädiktoren für Aussehen, Alter und Abstammung und die Entwicklung eines integrierten Interpretations-Frameworks mit einer Prototyp-Software zur kombinierten statistischen Berücksichtigung des Aussehens, des Alters und der Abstammung von DNA-Informationen, die in die routinemäßigen forensischen DNA-Serviceumgebung integriert werden kann.

Die Kritik ist vielfältig. Es bestehen „*rechtliche, ethische und soziale Risiken*"[27] aber auch technische Probleme. Vor allem ermöglichen Erweiterte DNA-Analysen eine weitere Stigmatisierung von Menschen, die sich ohnehin täglich mit Rassismus konfrontiert sehen (dazu mehr in Novago, Leydenberg 2019). Manche DNA-Fragmente kommen in bestimmten Regionen häufiger vor. Dies sagt aber „absolut nichts" über das Aussehen des Täters aus (vgl. Schultz, Bartram 2017). Die Software basiert aber auf probabilistischen Methoden (*probabilistic genotype matching*), sodass die Auswertung einer Interpretation bedarf, die stark durch den Automation-Bias und rassistische Vorurteile beeinflusst ist. Darüber hinaus sind die Methoden wissenschaftlich umstritten; Unternehmen wie Parabon Nanolabs und Identitas versprechen den Behörden mehr als sie wirklich können (vgl. May 2018). Trotzdem halten europäische Straf-

verfolgungsbehörden an dem Vorhaben fest, diese Methoden in der Praxis einzusetzen.

Fazit

In dem Artikel haben wir anhand eines Spektrums an Beispielen aufgezeigt, dass die informationstechnische Aufrüstung der Polizei massiv vorangetrieben wird. Erhebliche Mittel fließen in die Polizeiforschung beziehungsweise in die Forschung und Entwicklung zur zivilen Sicherheit, wobei KI-Methoden – insbesondere Maschinelles Lernen – in immer mehr Bereichen der Polizei zur Anwendung kommen. Politik und Polizei versprechen sich davon, mit immer mehr Daten und lernenden Algorithmen die Aufgaben der Polizei besser lösen zu können. Probleme der Technik und insbesondere die gesellschaftlichen Implikationen werden überwiegend ignoriert. Es scheint keine großangelegten wissenschaftlichen Projekte zu geben, die untersuchen, ob einerseits die technologischen Instrumente der Polizei überhaupt wirksam sind und andererseits welche Eingriffe in die Persönlichkeits- und Freiheitsrechte wie die informationelle Selbstbestimmung mit dem Einsatz der neuen Technologien verbunden sind oder wie sie vermieden werden können. Es ist also dringend geboten, dass ein ausreichender Teil der Forschungsmillionen für eine kritische Evaluation ausgegeben wird. Weiter braucht es eine kritische Öffentlichkeit, die sich gegen diese Algorithmisierung und Roboterisierung der Polizei in der jetzigen Form zur Wehr setzt.

PROF. DR. HANS-JÖRG KREOWSKI (1949) ist Professor (i.R.) für Theoretische Informatik an der Universität Bremen. Er ist außerdem im Vorstand des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) und der Zeitschrift Wissenschaft und Frieden. Er ist Mitglied der Leibniz-Sozietät der Wissenschaften zu Berlin und seit 2019 Mitherausgeber des Grundrechte-Reports. Neuere Veröffentlichung: Stefan Hügel, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht: Cyberwar and Cyberpeace. In Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos (Hrsg.) 2018:editors, *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, Heidelberg: Springer,S. 885-909.

AARON LYE (1989) promoviert in theoretischer Informatik an der Universität Bremen zum Thema Hypergraphtransformation. Er engagiert sich außerdem im FIfF. Neuere Veröffentlichung:Aaron Lye 2017: Techniken und Möglichkeiten digitaler Kriegsführung am Beispiel Stuxnet. *FIfF-Kommunikation*(2),71-74.

Literaturverzeichnis

Armbrost, Andreas 2014: Polizeitechnologie: Predictive-Policing, Criminologia, https://criminologia.de/2014/03/polizeitechnologie-predictive-policing/ gepostet am 14.03.2014

Bundesministerium des Innern, für Bau und Heimat 2018: Projekt zur Gesichtserkennung erfolgreich, Pressemitteilung vom 11.10.2018, https://www.bmi.bund.de/DE/ministerium/ministerium-node.html, aufgerufen am 28.08.2019

Bundespolizeipräsidium 2018:. Abschlussbericht zum Teilprojekt 1 „Biometrische Gesichtserkennung“ am Bahnhof Berlin Südkreuz, Stand 18.09.2018, https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile aufgerufen am 28.08.2019

Europäische Kommission 2017: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) COM(2017) 794 final.

Greis, Friedhelm 2018: Pilotprojekt Südkreuz ausgewertet: Flächendeckende Gesichtserkennung rückt näher, golem, 12.10.2018, https://www.golem.de/news/pilotprojekt-suedkreuz-ausgewertet-flaechendeckende-gesichtserkennung-rueckt-naeher-1810-137080.html, aufgerufen am 28.08.2019

Heitmüller, Ulrike 2017: Predictive-Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report, heise.de,. https://www.heise.de/newsticker/meldung/Predictive-Policing-Die-deutsche-Polizei-zwischen-Cyber-CSI-und-Minority-Report-3685873.html aufgerufen am 25.08.2019

Heitmüller, Ulrike 2019: Missing Link: Predictive-Policing – die Kunst, Verbrechen vorherzusagen. Heise.de, https://www.heise.de/newsticker/meldung/Missing-Link-Predictive-Policing-die-Kunst-Verbrechen-vorherzusagen-4425204.html aufgerufen am 25.08.2019

Hunko, Andrej 2014: Wie der Bundesnachrichtendienst und die Bundeswehr das Internet ausspähen wollen. http://andrej-hunko.de/component/content/article/7-beitrag/2152-wie-der-bundesnachrichtendienst-und-die-bundeswehr-das-internet-ausspaehen-wollen aufgerufen am 20.07.2019

Kampagne für Opfer rassistischer Polizeigewalt (KOP) (Hrsg.). Alltäglicher Ausnahmezustand: Institutioneller Rassismus in deutschen Strafverfolgungsbehörden. kritik_praxis. 2016

Krempl, Stefan 2015: Internetüberwachung: Europol will an Daten von Facebook und Twitter. Heise.de, https://www.heise.de/newsticker/meldung/Internetueberwachung-Europol-will-an-Daten-von-Facebook-und-Twitter-2913746.html aufgerufen am 23.08.2019

May, Mary 2018: Next Generation Forensics: Changing the role DNA plays in the justice system. http://sitn.hms.harvard.edu/flash/2018/next-generation-forensics-changing-role-dna-plays-justice-system/ aufgerufen am 23.08.2019

Meister, Andre 2015: Geheimer Geldregen: Verfassungsschutz arbeitet an „Massendatenauswertung von Internetinhalten". Netzpolitik.org, https://netzpolitik.org/2015/geheimer-geldregen-verfassungsschutz-arbeitet-an-massendatenauswertung-von-internetinhalten/ aufgerufen am 23.08.2019

Monroy, Matthias 2017: Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit. CILIP 113, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/ aufgerufen am 23.08.2019

Monroy, Matthias 2018a: Neues EU-System zur Identifizierung mit Fingerabdrücken freigeschaltet. Cilip, https://www.cilip.de/2018/03/07/neues-eu-system-zur-identifizierung-mit-fingerabdruecken-freigeschaltet/ aufgerufen am 04.08.2019

Monroy, Matthias 2018b: Der europäische Grenzgeheimdienst. Netzpolitik.org, https://netzpolitik.org/2018/der-europaeische-grenzgeheimdienst aufgerufen am 04.08.2019

Monroy, Matthias 2019a: EU legt biometrische Datentöpfe zusammen. Netzpolitik.org, https://netzpolitik.org/2019/eu-legt-biometrische-datentoepfe-zusammen-jetzt-droht-der-abfrage-tsunami/ aufgerufen am 06.02.2019

Monroy, Matthias 2019b: „Crawlen, Überwachen und Sammeln": EU forscht an Suchmaschine für kriminelle Internetinhalte. Netzpolitik.org, https://netzpolitik.org/2019/crawlen-ueberwachen-und-sammeln-eu-forscht-an-suchmaschine-fuer-kriminelle-internetinhalte/ aufgerufen am 11.02.2019

Monroy, Matthias 2019c: An Land, zu Wasser und in der Luft: EU-Mitgliedstaaten testen Drohnen zur Grenzüberwachung. Netzpolitik.org, https://netzpolitik.org/2019/an-land-zu-wasser-und-in-der-luft-eu-mitgliedstaaten-testen-drohnen-zur-grenzueberwachung aufgerufen am 21.08.2019

Novago, Emilia und Leydenberg, Anton 2019: Die Mär vom genetischen Phantombild: Die „Erweiterten DNA-Analysen" auf dem Vormarsch. RHZ (2).

Perry, Walter L., McInnis, Brian, Price, Carter C., Smith, Susan C. und Hollywood, John S. 2013: Predictive-Policing - The Role of Crime Forecasting in Law Enforcement Operations, RAND Corporation, https://www.rand.org/pubs/research_reports/RR233.html, aufgerufen am 28.08.2019

Reuter, Markus 2019: Gesichtserkennung: Automatisierter Rassismus gegen uigurische Minderheit in China. Netzpolitik.org, https://netzpolitik.org/2019/gesichtserkennung-automatisierter-rassismus-gegen-uigurische-minderheit-in-china/ aufgerufen am 15.04.2019

Sarbo, Bafta 2019: Racial Profiling in Deutschland: Keine Frage individuellen Fehlverhaltens. CILIP 118-119, http://www.cilip.de/2019/06/18/racial-profiling-in-deutschland-keine-frage-individuellen-fehlverhaltens/ aufgerufen am 24.08.2019

Singelnstein, Tobias 2019: Big Data bei der Polizei: Hessen sucht mit US-Software nach Gefährdern. In: B. Bartolucci et al (Hrsg.), Grundrechte-Report 2019. S. 27-30.

Schelling, Arkadi 2019: Künstliche Intelligenz als Cloud Service: Folgen für Gesellschaft, Geheimdienst und Militär. IMI-Analyse 2019/16.

Schultz, Susanne und Bartram, Isabelle 2017: Erweiterte DNA-Analysen: Technische Aufrüstung mit rassistischen Verwicklungen. CILIP 113, https://www.cilip.de/2017/09/08/erweiterte-dna-analysen-technische-aufruestung-mit-rassistischen-verwicklungen/ aufgerufen am 24.08.2019

Anmerkungen

1 Dieser psychologische Effekt ist als Automation-Bias bekannt.
2 Cloud Services bieten Dienste eines Rechenzentrums über das Internet an, von Festplattenspeicher über virtuelle Server bis hin zu höheren Softwarefunktionen.
3 Mit einer App können Bilder gegen eine Datenbank von ehemaligen Gefängnisinsassen abgleichen werden. Mobile und stationäre Überwachungskameras können ebenfalls mit Amazons System verbunden werden (vgl. Schelling 2019).
4 Siehe dazu die Pressemitteilung des Bundesministeriums des Innern, für Bau und Heimat vom 11.10.2018 und den Abschlussbericht des Bundespolizeipräsidiums vom September 2018 sowie den Kommentar von Greis 2018.
5 Dabei liefert eine ODER-Verknüpfung, bei der ein Treffer vorliegt, wenn nur eins der zwei System das Gesicht erkennt, eine hohe Trefferrate, gleichzeitig aber auch eine hohe Falschakzeptanzrate. Bei einer UND-Verknüpfung, bei der beide Systeme ein Gesicht erkennen müssen, erreicht man die kleinste Falschakzeptanzrate, jedoch auch eine nur ziemlich kleine Trefferquote.
6 Der Begriff Gefährder ist neu im Rechtssystem und unklar definiert. Klar ist nur, dass Menschen betroffen sind, denen Polizei oder Geheimdienste zutrauen, dass sie in der Zukunft Straftaten begehen könnten.
7 Die Abfragen bei Europol erfolgen ebenfalls über ein neues Protokoll („Querying Europol Systems“, QUEST) (vgl. Monroy 2019a).
8 S. https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/Polizei2020/EPRIS_ADEP/EPRIS.html
9 S. https://www.europol.europa.eu/activities-services/services-support/information-exchange.
10 Synonyme Bezeichnungen für Predictive-Policing sind „Smart Policing“, „Crime Forecasting“ und „Predictive Crime Mapping“. In Deutschland hat sich der Begriff Predictive-Policing durchgesetzt. Wer mehr zu diesem Thema erfahren möchte, ist auf Perry et al. 2013, Armbrost 2014, Monroy 2017, Heitmüller 2017, Heitmüller 2019 und Singelnstein 2019 verwiesen.
11 S. Projektwebsite: http://www.fp7-caper.eu/.
12 S. https://cordis.europa.eu/project/rcn/188358/factsheet/en.
13 S. Projektwebsite: https://www.dhpol.de/departements/departement_II/FG_II.1/projekt-sentinel.php.
14 S. Projektwebsite: https://www.dhpol.de/departements/departement_III/FG_III.1/projekte/radigz.php.
15 S. Projektwebsite: https://www.dhpol.de/departements/departement_II/FG_II.5/x_sonar.php.
16 S. Projektwebsite: https://www.dhpol.de/departements/departement_III/FG_III.1/projekte/praedisiko.php.
17 S. https://tensor-project.eu/overview/aims-and-objectives.
18 S. Projektwebsite: http://trivalent-project.eu.
19 S. Projektwebsite: https://www.prophets-h2020.eu.
20 S. Projektwebsite: http://redalertproject.eu.
21 Die Deutsche Hochschule der Polizei (DHPol) untersucht beispielsweise im Rahmen des Projekts

Human+ (Projektdauer: April 2018 bis März 2020) die Anforderungen deutscher Polizeibehörden an ein interorganisationales Echtzeit-Lagebild für „effizientes Migrationsmanagement“.

22 S. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018D0620.

23 S. https://www.esteri.it/mae/resource/endtemp/2017/10/job_profile_maritime_surveil_exp_16 nota.pdf.

24 S. Projektumriss: https://www.sifo.de/files/Projektumriss_SmartIdentifikation.pdf.

25 S. https://cordis.europa.eu/project/rcn/210214/factsheet/en.

26 S. Projektwebsite: http://www.visage-h2020.eu.

27 Offener Brief zum kritischen Umgang mit Erweiterten DNA-Analysen in der FOrensik von Wissenschaftler_innen des Lehrstuhls für Wissenschaftsforschung am University College der Albert-Ludwigs-Universität Freiburg, 8. Dezember 2016, http://stsfreiburg.wordpress.com/offener-brief aufgerufen am 03.09.2019