Bilder: Securitas

Im Securitas Operation Center (SOC) laufen alle eingehenden Daten zusammen.

Künstliche Intelligenz

Motor oder Konkurrenz?

Manfred Buhl

Künstliche Intelligenz (KI) ist 2017 ein Trendthema, in Fortsetzung der Megathemen Industrie 4.0 und Internet der Dinge. Für das Sicherheitsgewerbe stellt sich dabei die Frage: Wird KI zum Motor oder zur Konkurrenz?

Künstliche Intelligenzen, autonome Systeme, Drohnen und Roboter – die Digitalisierung verändert in spektakulärer Geschwindigkeit Wirtschaft und Gesellschaft. Welche Potenziale ergeben sich in der digitalen Transformation in Verbindung mit künstlicher Intelligenz für die Sicherheitsbranche?

Definition von KI

Künstliche Intelligenz bezeichnet die Fähigkeit einer Maschine oder eines Systems, die menschliche Intelligenz in ihrer Vielfalt von Wahrnehmung und Analyse, Bewertung, Entscheidung und Handlung künstlich nachzubilden. Geschaffen wird KI durch Algorithmen als Handlungsanweisung für Rechenoperationen oder andere logische Regeln zur eindeutigen Problemlösung. Man spricht von „starker KI“, wenn sie in der Lage ist, menschliche Intelligenz zu ersetzen, und von „schwacher KI“, wenn sie zumindest menschliche Intelligenz in ihrer Anwendung erleichtert und verbessert. Beide Formen KI haben zunehmende Bedeutung auch für die Sicherheitstechnik und für die Leistungsfähigkeit des Sicherheitsgewerbes.

KI in der Sicherheitstechnik

Roboter, Drohnen & Co.

Roboter, die mit künstlicher Intelligenz ausgestattet werden, sind bereits in der Lage, überschaubare Dienstleistungen zu erbringen und mit Menschen zu interagieren (zum Beispiel digitale Pförtner). Längst übernehmen moderne Roboter dank KI immer mehr Routinetätigkeiten – nicht nur in Produktionsprozessen.

Roboter können so programmiert werden, dass sie Streifengänge im Objektschutz oder in der Sicherheitskontrolle von Betriebsprozessen und Gefahrstofflagern durchführen. Sie könnten auch dort zum Einsatz kommen, wo gefährliche unbekannte Gegenstände zu erkunden sind, um dann aufgrund vorgegebener Kriterien Alarm auszulösen oder selbständig bestimmte Reaktionen durchzuführen. Die Entwicklungsstufe einer „starken KI“ ist erreicht, wenn solche Roboter aufgrund einer Programmierung und eigener Lernerfahrungen Reaktionskriterien selbstständig beurteilen, etwa die Streifenrichtung ändern oder aufgrund einer erkannten und bewerteten Gefahrensituation alarmieren.

Auch Drohnen unterstützen den Menschen bereits in unterschiedlichen Einsatzfeldern. In der Kombination mit umfassenden „Big Data“-Analysen und weiteren digitalen Technologien ergeben sich erhebliche Potenziale für Drohnen, die ähnlich wie Roboter antrainierte Lernerfahrungen umsetzen. Ihre Intelligenz können Drohnen insbesondere im Brandschutz- und Safety-Bereich beweisen, zum Beispiel bei der thermografischen Statusüberprüfung von Wärme- und Gasleitungen und der Suche nach Leckagen, bei der Brandherdbestimmung mittels Thermokamera, beim Detektieren und Kartieren der Schadstoffausbreitung bei großen Stofffreisetzungen und bei der Live-Bildübertragung auch schwer zugänglicher Örtlichkeiten an den Krisenstab. Securitas Deutschland hat

beispielsweise zusammen mit der Aidrones GmbH für den Einsatzbereich Fire & Safety eine hochspezialisierte Drohne mit Alleinstellungsmerkmalen entwickelt (explosionsgeschützt für den Einsatz in Zone 2, Multi-Gas-Sensorik, HD-Kamera sowie Wärmebildkamera). Wenn die örtlichen Rahmenbedingungen der Gebietsvermessung geschaffen sind, kann die Drohne auch aufgrund empfangener GPS-Daten, die mit dem Alarm gesendet werden, automatisch aufsteigen und Bilder vom Ereignisort an die Leitzentrale übermitteln, noch bevor die Feuerwehr oder andere Interventionskräfte dort eingetroffen sind.

Biometrie

Die Anwendung der Biometrie zur Identifizierung von Personen, ihrer Authentifizierung oder der Gültigkeitsprüfung von Dokumenten und Unterschriften beruht auf KI. Dass die Gesichtserkennung bisher zu sehr von der Körperhaltung der von der Videokamera aufgenommenen Person und den Lichtverhältnissen abhängt, widerspricht der KI nicht. Seit dem „gescheiterten“ Pilotversuch des BKA auf Treppen und Rolltreppen im Mainzer Hauptbahnhof 2007, bei dem nur eine Treffergenauigkeit von 60 Prozent bei sehr guten Lichtverhältnissen erreicht wurde, ist die Technologie vorangeschritten, vor allem die Leistungsfähigkeit der einzusetzenden Videokameras. Ob die Gesichtserkennung inzwischen eine für Fahndungszwecke ausreichende Leistungsfähigkeit erreicht hat, soll in einem weiteren Pilotversuch des BMI zusammen mit der Bundespolizei, dem BKA und der Deutschen Bahn getestet werden. Ein Zwischenschritt der Entwicklung wäre ein erfolgreicher Einsatz in Verbindung mit Vereinzelungssystemen der Zutrittskontrolle, die automatisch Frontalaufnahmen ermöglichen.

Vom teilweise schlechten Ruf biometrischer Identifikationssysteme – sie seien zu teuer, zu langsam und mit einer hohen fehlerbehafteten Rückweisungsrate belastet – kann heute keine Rede mehr sein. Dank Leistungssteigerung und größerer Effizienz im Hard- und Softwarebereich sind die meisten biometrischen Identifikationssysteme ausgereift und wirtschaftlich attraktiv. Die zuvor skizzierte automatische Gesichtserkennung ist dabei die vielversprechendste Möglichkeit biometrischer KI.

Analysesoftware in Videokameras

Intelligente Analysesoftware ist KI. Sie ist in der Lage, Personen von Tieren, menschliche Bewegungen von im Wind bewegten Baumästen zu unterscheiden, Bewegungsrichtungen, körperliche Auseinandersetzungen in einer Personengruppe oder das Fehlen eines Trägers neben dem abgestellten Koffer zu detektieren. Die ständige, ermüdende und dadurch lückenhafte Beobachtung der Monitore durch den Operator in der Leitstelle wird durch eine intelligente Software im Kamerasystem ersetzt. Sie befähigt die Videoüberwachung, vordefinierte Bewegungen automatisch zu detektieren, die Beobachtung der sich fortbewegenden Person auf andere Kameras zu transferieren und nach vorgegebenen Kriterien Alarm auszulösen.

KI unterstützt Planung und Strategie

Ein intelligent geführtes Unternehmen plant seine Einsätze ebenso wie seine geschäftliche Weiterentwicklung. Und dabei kann KI das Management unterstützen. Gerade im Geschäftsumfeld gibt es vielseitige Einsatzfelder für KI, etwa in der effizienteren Auswertung vorhandener Daten. Auch dafür einige Beispiele:

Data Mining

Data-Mining-Software durchsucht automatisch „Big Data“ mit komplexen Datensätzen, um entscheidungsrelevante Muster und Beziehungen aufzuspüren. So könnte zum Beispiel die Datenbank eines Sicherheitskonzerns, in der alle im Unternehmen entwickelten Sicherheitslösungen mit ihren spezifischen Voraussetzungen, Rahmenbedingungen und Realisierungserfahrungen eingegeben sind, für die Erstellung neuer Sicherheitslösungen genutzt werden. Die Basis vielfältiger Erfahrungswerte macht die neue Sicherheitskonzeption wertvoller und gibt dem Anbieter größere Verhandlungschancen.

Predictive Analytics

Die Möglichkeit, durch Auswahl geeigneter Software vorhandene Daten so zu analysieren, dass belastbare und treffsichere Prognosen abgeleitet werden können, ist eine der Entwicklungen, die die Sicherheitsbranche positiv beeinflussen wird. Denn Erkenntnisse aus komplexen Datensätzen bieten enorme Möglichkeiten für Prozesssteigerungen und Ressourcenplanungen und sind die Grundlage für verbesserte Sicherheitsleistungen, besseren Service und höhere Kundenzufriedenheit.

Die Möglichkeit der systematischen Vorhersage des Täterverhaltens ist im Zusammenhang mit der räumlichen Planung von

polizeilichen Präventionsmaßnahmen gegen Wohnungseinbrüche bekannt geworden. Dazu werden Daten von Wohnungseinbrüchen erhoben, wie Zeitraum, Tatbereich, Tatgelegenheits-Strukturdaten, Tatumstände und Täterverhalten. Algorithmen der mit diesen Daten entwickelten Software errechnen die Wahrscheinlichkeit, dass und unter welchen Umständen in dem definierten Ortsbereich erneut Wohnungseinbrüche begangen werden. Die Polizei kann sich in ihrer Ressourcenplanung, Streifenhäufigkeit und Streifendichte nach dieser Vorhersage richten. Berichtet wird sowohl über gute Erfahrungen mit solchen Prognosen mit Hilfe von KI wie auch über kritische Bewertungen der Verlässlichkeit solcher Berechnungen.

Anwendbar ist ein derartiges intelligentes Prognosesystem grundsätzlich auch in der Einsatz- und Ressourcenplanung eines Sicherheitsunternehmens. Wie könnte hier ein Wandel aussehen? In der Vergangenheit wurden mittels Dienstbücher, Werkschutzmeldungen, Checklisten oder über Reports Sachverhalte belegt, „was vor Ort geschehen ist“. Mittlerweile werden diese Daten digital erfasst, und es kommen diagnostizierende Analysen hinzu, die uns sagen, „warum etwas geschehen ist“. In der Zukunft reden wir über vorausschauende Analysen, die uns Vorhersagen ermöglichen und die Frage beantworten, „was geschehen wird“. Durch intelligente Steuerung und empfehlende Analysen werden wir wissen, „was getan werden muss“. Um das zu erreichen, wird der Guard im Securitas-Konzern mit mobilen Endgeräten zur Datenerfassung und -auswertung ausgestattet.

Sicherheitsmarktprognose

Zukunftsplanung ist für jede Unternehmensführung unverzichtbar. Sicherheitsunternehmen müssen sich rechtzeitig auf Veränderungen im Sicherheitsmarkt einstellen. Der ist von vielfältigen Einflussfaktoren abhängig. Deren Entwicklung lässt sich mit einer Trendanalyse grob prognostizieren. Unter Anwendung KI methodisch abgesichert ist die „Szenariomethode“. Nach ihr werden Einflussfaktoren auf die Entwicklung des Sicherheitsmarktes nach Wichtigkeit und Ungewissheit ausgewählt, beschrieben und auf mögliche unterschiedliche Ausprägungen in der Zukunft untersucht. Für jede Ausprägung wird die Eintrittswahrscheinlichkeit bestimmt und zu den unterschiedlichen Ausprägungen aller anderen ausgewählten Deskriptoren in Beziehung gesetzt. Mit Hilfe einer speziellen Software werden

Mobilecams sind sehr flexibel einsetzbar. Die Bilder werden in die Sicherheitszentrale übertragen.

Eintrittswahrscheinlichkeiten für einzelne Szenarien berechnet. Das Ergebnis besteht also in der Darstellung von Entwicklungsszenarien mit unterschiedlichen Eintrittswahrscheinlichkeiten. Mit dieser Methode hat zum Beispiel die Kölner Polizei die Entwicklung der Sicherheitslage in ihrem Zuständigkeitsbereich prognostiziert. Und das Unternehmen Bosch Sicherheitssysteme hat so mögliche Szenarien für die Entwicklung des Sicherheitsmarktes erarbeitet.

KI – Motor oder Konkurrenz?

Das Sicherheitsgewerbe braucht die fortschreitende Anwendung der KI nicht zu fürchten. Zwar kann KI Streifengänge teilweise durch maschinelle Überwachungen, Analysen, Alarmierungen und andere Reaktionen ersetzen. Dies wird aber nur in geringem Maße zum Verlust von Arbeitsplätzen im Sicherheitsgewerbe führen. Nach einer Abfrage des von der ARD initiierten Datenbanksystems „Job-Futoromat“ können Tätigkeiten in folgenden Sparten des Sicherheitsgewerbes entweder derzeit gar nicht oder nur zu einem geringen Prozentsatz von Maschinen übernommen werden:

• Sicherheitsmanager	10 %
• Sicherheitsbeauftragte im Werkschutz	0 %
• Fachkraft für Schutz und Sicherheit	0 %
• Servicekraft für Schutz und Sicherheit	11 %
• NSL	0 %

Die in immer kürzeren Innovationszyklen fortschreitende Intelligenzfähigkeit der Sicherheitstechnik ermöglicht es Sicherheitsunternehmen, immer leistungsfähigere und im Vergleich mit personellen Dienstleistungen kostengünstigere Sicherheitslösungen anzubieten: in der Sensortechnologie, in der Bildanalyse, in der Biometrie und in der intelligenten Auswertung von „Big Data“.

Sicherheitsforschung

Damit KI im Sicherheitsbereich noch stärker als bisher genutzt werden kann, ist die Förderung der Sicherheitsforschung von großer Bedeutung. Dies wird bereits in Deutschland von bedeutenden Unternehmen mit Forschungskapazitäten, ebenso wie von Forschungsinstituten – insbesondere dem Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung und dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie – sowie spezialisierten Behörden wie dem BKA und dem BSI, vorangetrieben. Seither wurden für Forschungsprojekte rund 400 Millionen Euro Fördermittel zur Verfügung gestellt, und die Industrie hat ungefähr 100 Millionen Euro an Eigenmitteln investiert. Auf Initiative des Bundesministeriums für Bildung und Forschung (BMBF) hat die Bundesregierung 2007 ein erstes Rahmenprogramm „Forschung für die zivile Sicherheit“ aufgelegt. Seit September 2016 läuft das vom BMBF mit 1,4 Millionen Euro unterstützte Sicherheitsforschungsprogramm Osima (Ordnung des Sicherheitsmarktes). Rahmenprogramme für Sicherheitsforschung existieren seit 2007 auch in der EU. Für die europäische Sicherheitsforschung werden von 2014 bis 2020 insgesamt 1,7 Milliarden Euro zur Verfügung gestellt.

Als Fazit bleibt zu unterstreichen, dass KI Märkte und Geschäftsmodelle verändern wird. Diese KI frühzeitig zu erkennen und zu nutzen, um so den Erfolg der digitalen Transformation des eigenen Unternehmens sicherzustellen, setzt einen Meilenstein und bietet eine enorme Bandbreite an Einsatzfeldern mit unterschiedlichen Sicherheits- und Schutzanforderungen.

Manfred Buhl, CEO Securitas Deutschland, Vizepräsident BDSW, www.securitas.de