

Übergriffe, Terror, Bomben: Neue Technik schützt vor Gefahren in der Öffentlichkeit

Auf dem Weihnachtsmarkt ein Glühwein? Am Brandenburger Tor Silvester feiern? Mit dem Zug durch Deutschland reisen? Was wir auch tun, wir wollen dabei vor Anschlägen und Gewaltkriminalität geschützt sein. Technologie kann Sicherheit erheblich steigern.

Am 29. Juli 2019 stößt ein psychisch gestörter Mann am Frankfurter Bahnhof eine Mutter und ihren achtjährigen Sohn vor einen einfahrenden ICE. Am 28. Juli 2017 sticht ein Asylbewerber in einem Hamburger Supermarkt mit einem Messer auf Kunden ein. Ein Mensch stirbt, fünf werden verletzt. Am 9. Oktober 2019, dem höchsten jüdischen Feiertag Jom Kippur, versucht ein Rechtsextremist, die Synagoge in

Halle zu stürmen und die versammelte Gemeinde anzugreifen. Als dies nicht gelingt, erschießt er eine Passantin und den Besucher eines türkischen Imbisses. Die Frage, die sich immer neu stellt: Wie lässt sich die Sicherheit vor Anschlägen und Gewaltkriminalität erhöhen?

So hilft Technik, Gewalt einzudämmen

Eine Technologie, die helfen kann, Gewaltkriminalität drastisch einzudämmen, bietet das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB mit der intelligenten Videoüberwachung. Während herkömmliche Videoüberwachung Probleme im Bereich Datenschutz hervorruft und in der Bevölkerung meist auf wenig Akzeptanz stößt, lässt sich der Datenschutz hier technisch erzwingen.

"Unser System unterscheidet selbstständig zwischen relevanten und irrelevanten Vorgängen bzw. Aktivitäten", sagt Dr. Markus Müller, Leiter der Abteilung Videoüberwachungssysteme am Fraunhofer IOSB. Schlendert jemand mit seiner Einkaufstüte über den überwachten Platz oder spielen dort ein paar Kinder, so sieht die Einsatzkraft vor den Rechnern nur einen schwarzen Bildschirm oder ein pixeliges Bild, auf dem kaum etwas zu erkennen ist. Bemerkt das System jedoch einen Tritt oder Schlag oder einen anderen tätlichen Übergriff, schaltet es den Monitor ein und zieht den menschlichen Entscheidungsträger hinzu.

"Das System agiert wie ein digitaler Schnüffelhund", erläutert Müller. "Ein Schnüffelhund ist auf einen ganz bestimmten Geruch trainiert – nur wenn er diesen wahrnimmt, schlägt er an. Ähnlich funktioniert unser System: Es meldet sich nur bei tätlichen Übergriffen, alle anderen Verhaltensweisen sind ihm unbekannt."

Eine Meldung des Systems ist also ähnlich zu werten wie ein Anruf unter der 110. Doch woher weiß das System eigentlich, wann ein Angriff vorliegt und wann nicht? Dies haben die Forscherinnen und Forscher ihm über Künstliche Intelligenz beigebracht und optimieren diesen Lernvorgang. Sprich: Sie haben das System mit verschiedenen Videoaufzeichnungen von Schlägen, Tritten und Co. "gefüttert", mit jedem Video wird das System sicherer.

Sicherheit am Bahnhof

Die Entscheidungen jedoch trifft nach wie vor der Mensch. Schaltet das System etwa wegen einer Tritthypothese um auf ein Klarbild, kann er den Hinweis verwerfen, da ggf. harmlos, oder aber Maßnahmen einleiten, etwa eine Streife hinschicken. "Den ersten Schlag verhindern wir nicht, der soll als solcher erkannt werden. Aber eine weitere Fortsetzung, die Eskalation, der versuchte Totschlag oder gar der Totschlag könnte durch unmittelbare Erkennung des Übergriffs sowie rasche Intervention verhindert werden", sagt Müller.

In Mannheim setzt die Polizei das System im Rahmen eines Pilotprojekts für Experimente bereits ein – dort werden bestimmte Kriminalitäts-Hotspots mit insgesamt rund 70 Kameras überwacht, ihre Bilder sollen vom System parallel und in Echtzeit ausgewertet werden. Die Akzeptanz der Bevölkerung ist enorm: 80 bis 85 Prozent der Menschen befürworten das System. "Die Kriminalitätsrate sinkt, im Durchschnitt dauert es in den überwachten Gebieten nicht einmal zwei Minuten, bis die Einsatzkräfte an Ort und Stelle sind", weiß Müller.

An Bahnhöfen und Co. könnte das dortige Sicherheitspersonal sogar innerhalb von Sekunden eingreifen. Wird der Wachdienst dort verständigt, dass jemand angegriffen wird, kann er über Lautsprecher direkt den Täter ansprechen: "Sie werden beobachtet, die Streife ist unterwegs. Unterlassen Sie die Angriffe!" Keine Frage: Vorfälle wie in Frankfurt lassen sich auch durch dieses System nicht verhindern, selbst direkt daneben stehende Polizisten hätten das Unglück wohl kaum abwenden können.

Bei vielen anderen Situationen kann das System jedoch für deutlich mehr Sicherheit sorgen. "Es gab einmal eine Situation nachts in einer U-Bahn-Station, in der verschiedene Täter einen Mann auf die Gleise gestoßen haben und ihn minutenlang nicht wieder hoch ließen. In einem solchen Fall könnten Einsatzkräfte mithilfe der intelligenten Videoüberwachung schnell eingreifen und die Fortsetzung von Straftaten verhindern", ist sich Müller sicher.

"Wir sehen uns im Dienste der Gesellschaft: Wir wollen mit unserer Technik solche Schrecklichkeiten verhindern – oder zumindest die Eskalation des Schreckens", sagt Müller. So könnte das System, trainiert mit den passenden Daten, auch Posen und Körperhaltungen erkennen, die für das Bereithalten oder Zielen mit einer Waffe typisch sind. Denn diese Körperhaltungen entscheiden sich genügend von "normalen" Körperpositionen. "Wir sind der Meinung, dass man besonders gefährdete Einrichtungen wie Synagogen bundesweit mit intelligenter Videoauswertung überwachen sollte. In Halle hätte man so, noch bevor der erste Schuss fiel, Einsatzkräfte losschicken können", meint Müller. "Vielleicht hätte es dann keine Toten gegeben."

Schutz vor schmutzigen Bomben

Der Gefahr schmutziger Bomben mit radioaktiven Stoffen begegnen Forscherinnen und Forscher des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE mit einer Technologie, die sie im Projekt REHSTRAIN, kurz für "REsilience of the Franco-German High Speed TRAIIn Network", entwickelt haben. "Unser Assistenzsystem ermöglicht es, radiologische Quellen im Menschenstrom zu erkennen und das Sicherheitspersonal zu alarmieren", sagt Dr. Felix Govaers, stellvertretender Leiter der Abteilung "Sensordatenfusion" am Fraunhofer FKIE.

Das System besteht aus mehreren Komponenten. Gammaskpektrometer, die in Böden oder Mauern des Bahnhofsgebäudes verbaut werden können, erfassen die radioaktive Strahlung und können sogar bestimmen, um welche Isotope es sich handelt. Da ein einziger Sensor nur analysieren kann, ob Strahlung vorhanden ist, setzen die Forscher ein Netz von Sensoren

sowie handelsübliche Kinect-Kameras ein. Diese Kinect-Kameras liefern neben Bildern auch Entfernungsinformationen. Über eine Software zur Datenfusion koppeln sie die Daten miteinander und können die Strahlungsquelle auf diese Weise lokalisieren und einer bestimmten Person zuordnen.

An neuralgischen Punkten angebracht – also in Eingangsbereichen, Auf- und Abgängen von Bahnhöfen, Flughäfen oder anderen öffentlichen Gebäuden –, könnten solche Assistenzsysteme künftig Informationen über radiologische Gefährder an die Überwachungssysteme etwa der Verkehrsbetriebe übertragen. Elementar dabei: Ob ein Zugriff erfolgt, entscheidet weiterhin der Mensch. Die Forscher des Fraunhofer FKIE sind derzeit im Gespräch mit der Düsseldorfer Firma innoRIID, die das System vermarkten möchte.

Abwehr von Gefahren aus der Luft

Eine Drohne nähert sich einer Großveranstaltung – beispielsweise der Silvesterfeier am Brandenburger Tor in Berlin. Ist sie ein harmloses Flugobjekt? Oder ist sie eine von Terroristen gesteuerte Waffe, die Sprengstoff oder – viel wahrscheinlicher – Brandbeschleuniger in die Menschenmenge trägt? Es sind dringend verlässliche Detektions- und Abwehrsysteme für Drohnen gefragt. Ein solches haben zwölf Partner aus Industrie, Forschung und Lehre im BMBF-geförderten Projekt "Abwehr von unbemannten Flugobjekten für Behörden und Organisationen mit Sicherheitsaufgaben" – kurz AMBOS – entwickelt. Die Koordination lag beim Fraunhofer FKIE.

Ein Radargerät, mehrere Kameras, ein Funkaufklärungssensor, der das Funksignal der Fernbedienung analysiert, und akustische Sensoren, die die Geräusche anfliegender Drohnen erkennen, überwachen das Gelände. Jeder Sensor hat seine Vorteile: Der Radar kann beispielsweise einige Kilometer weit schauen, jedoch brauchen die Kameras und das Radar eine "Line of Sight", also Sichtkontakt. Funkaufklärung und akustische Sensoren dagegen brauchen dies nicht, allerdings haben akustische Sensoren lediglich eine Reichweite von einigen hundert Metern.

"Der Segen liegt in der Multimodalität", sagt Hans Peter Stuch, Forschungsgruppenleiter und Verbundkoordinator AMBOS am Fraunhofer FKIE. "Insbesondere in der Sensordatenfusion: Sie koppelt nicht nur die Daten der unterschiedlichen Sensoren miteinander, sondern überprüft auch gleich die Qualität der Daten jedes einzelnen Sensors."

Den Einsatzkräften, die beispielsweise am Silvesterabend in Berlin für Sicherheit sorgen sollen, erleichtert das System, die Situation einzuschätzen und entsprechend zu reagieren. Nähert sich eine Drohne dem Festgelände, sehen sie deren aktuelle Position auf einer digitalen Karte; zudem werden die Flughöhe, die Fluggeschwindigkeit und die Flugrichtung angezeigt. Doch stellt das Flugobjekt tatsächlich eine Gefahr dar? Auch bei dieser Frage unterstützt das System: Anhand der Daten schätzt es die Gefahrenlage ein und schlägt mögliche Gegenmaßnahmen vor. Entscheidet sich der Einsatzleiter daraufhin für eine Aktion, kann er sie ganz einfach per Knopfdruck starten.

Die erste Option liegt darin, ein Störsignal auszusenden: Die Drohne kann das Signal ihrer Fernbedienung in dem Wirrwarr nicht mehr hören. Abgesehen von autonom fliegenden Drohnen bleibt die betroffene Drohne entsprechend ihrer Konfiguration daraufhin stehen, landet oder fliegt zum Startpunkt zurück. Eine zweite mögliche Abwehrmaßnahme ist ein elektromagnetischer Hochenergiepuls. Dieser bringt den Flug-Controller der Drohne

durcheinander, der unter anderem die Rotoren ansteuert – die Drohne fällt wie ein Stein zu Boden. Als dritte Option steht ein Netzwerfer bereit, der die Drohne mechanisch zum Absturz bringt.

Ende Juni 2019 haben die Forscher das Projekt erfolgreich abgeschlossen – mit einer Evaluierung in Mosbach. Dort flogen Drohnen in verschiedenen Flugszenarien auf die zu schützende Liegenschaft zu. Das System erkannte die Gefahrenlage und leitete, auf Knopfdruck des Personals, erfolgreich entsprechende Gegenmaßnahmen ein. "Bezüglich dieses Kernsystems, das aus Sensordatenfusion, Lagedarstellung und Entscheidungsunterstützung besteht und an welches beliebige Sensoren und Abwehrmaßnahmen gekoppelt werden können, sind wir unter anderem im Gespräch mit einigen Polizeibehörden und der deutschen Flugsicherung", erläutert Stuch. Vielleicht lässt sich künftig die Zahl der Horrormeldungen durch solche Technologien reduzieren.

Soziale Netzwerke für mehr Sicherheit

Hilfreich bei der Vermeidung von Attentaten sind auch Medien, die die Extremisten vorab nutzen und über die sie sich absprechen oder ihre Vorhaben ankündigen. Um Verdächtige weiter einzukreisen und ihre Tweets und Äußerungen in sozialen Netzwerken schnell auf Schlagworte zu durchsuchen, können Sicherheitskräfte künftig auf eine Technologie aus dem Fraunhofer FKIE setzen. Sie kombiniert eine Telefonüberwachung mit einer Suchmaschine für soziale Netzwerke. Ist eine Person verdächtig und hat ein Richter die Telefonüberwachung genehmigt, lassen sich zunächst die Telefonate analysieren. Dies erfolgt in drei Stufen. In der ersten Stufe wird untersucht, an welchen Stellen des Telefonats überhaupt gesprochen wird oder wo im Gegensatz dazu etwa nur Hintergrundgeräusche zu hören sind.

In einem zweiten Schritt vergleicht das System die Sprachstellen mit hinterlegten Sprachproben und ermittelt auf diese Weise die Identität der sprechenden Personen, die bei der Nutzung von Pre-Paid-Handys ansonsten kaum aufzudecken wäre. Und in einem dritten Schritt sucht es nach dem Vorkommen von Schlagworten, die von den Ordnungskräften vorab eingegeben wurden. Haben die Einsatzkräfte auf diese Weise einen vagen Anfangsverdacht erhärtet, können sie mit dem System NewsHawk analysieren, was die entsprechenden Personen auf sozialen Netzwerken wie Twitter posten.

Auch im Nachgang von Anschlägen kann die Technologie hilfreich sein – etwa um über das Netzwerk des Täters weitere Drahtzieher ausfindig zu machen und so wiederum weitere Anschläge zu vermeiden. "NewHawk fungiert dabei wie eine Suchmaschine über Twitter", sagt Prof. Dr. Ulrich Schade, Forschungsgruppenleiter "Informationssysteme" am Fraunhofer FKIE. Zunächst einmal erstellt das Tool eine Art Karte, in der die unter dem Suchwort – etwa dem Hashtag #Halle0910 – am häufigsten sonst vorkommenden Begriffe in Kreisen entsprechender Größe dargestellt werden. Klickt der Ermittler auf den Kreis zu einem dieser Begriffe, zeigt das System ihm alle Tweets an, die auch diesen Begriff enthalten. Dabei kann er priorisieren und Regeln angeben, beispielsweise: Suche alles, wo das Wort XY enthalten ist, aber nicht das Wort Z.

In einem zweiten Schritt untersucht ein Analysetool, das die Forscher via Machine Learning an die Aufgabe angepasst haben, die Textfiles auf die Gefühle, die darin zum Ausdruck gebracht werden. Befürwortet ein Nutzer in seinem Tweet einen Anschlag, ruft er zu weiteren Gewalttaten auf, oder verurteilt er sie? "Dabei gilt es, die jeweilige Sprache einer radikalen Gruppe zu berücksichtigen. Denn ein Islamist verwendet andere Ausdrücke als ein Rechtsradikaler", erläutert Schade.

In einem dritten Schritt analysiert das Programm die Metadaten: Welcher Befürworter hat etwa welche Follower? Auf diese Weise konstruiert das Tool eine Netzwerkkarte – ausgehend vom Täter eines Anschlags. "Wirft ein geübter Polizeianalyst einen kurzen Blick auf eine solche Netzwerkkarte, sieht er sofort, wo sich ein problematischer Knoten befindet", so Schade.

Der Text wurde zur Verfügung gestellt von der Fraunhofer-Gesellschaft. Fraunhofer ist führend als Organisation für anwendungsorientierte Forschung mit 74 Instituten in Europa