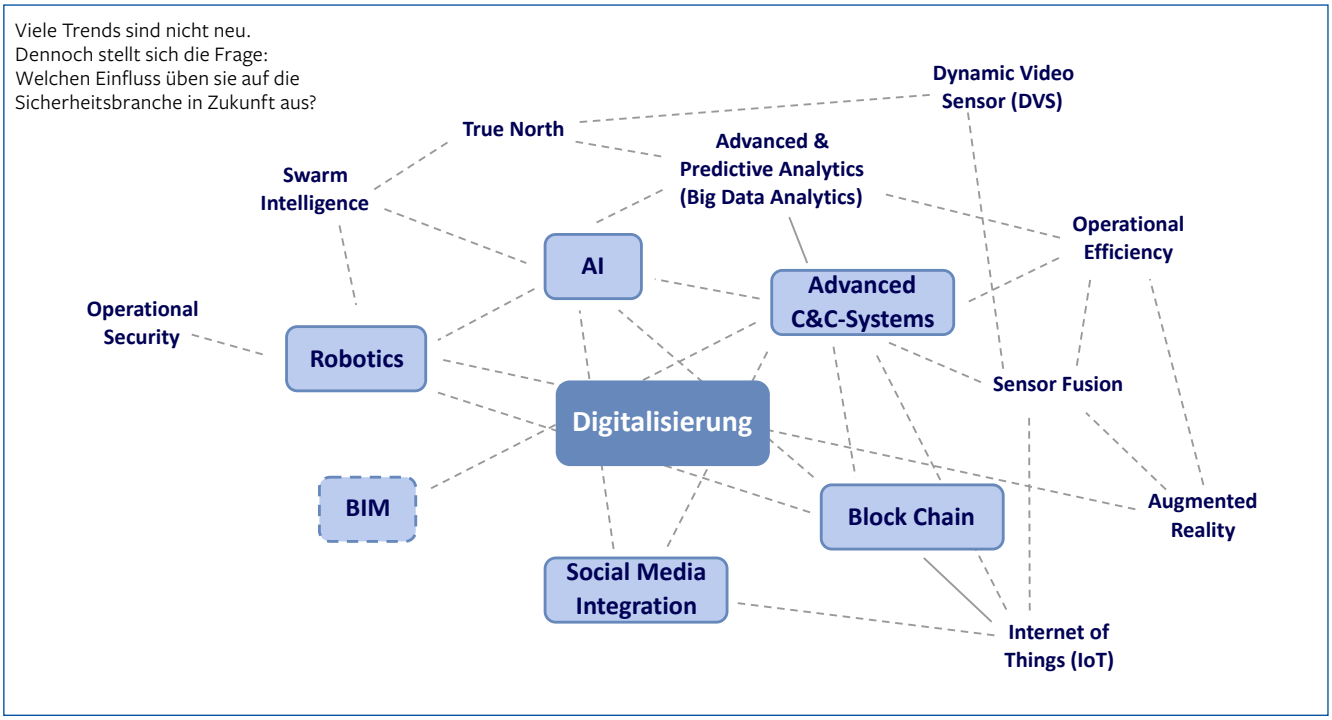

Trends in der Sicherheitstechnik

Was bringt die Zukunft bis 2026?

Dr. Peter Fey

Die Geschwindigkeit des technischen Fortschritts in Verbindung mit steigender Komplexität und teils völlig neuen Technologien fordern von der Sicherheitstechnik immer wieder eines: Sich den Auswirkungen zentraler Trends zu stellen und Handlungsoptionen für zukünftige Szenarien abzuleiten. Doch was sind eigentlich die einflussreichsten technischen Trends in den nächsten drei bis acht Jahren?

Viele aktuelle Trends (siehe Grafik) sind zwar nicht neu. Dennoch stellt sich die Frage: Welchen Einfluss haben sie auf die Sicherheitsbranche? Wie sehen die besten strategischen Antworten auf immer dynamischere Veränderungen aus? Erst mit einer zielorientierten strategischen Antizipation wird es den Unternehmen, die am meisten von diesen Trends betroffen sind, auch gelingen, dem Wettbewerb einen entscheidenden Schritt voraus zu sein. Haupttreiber für alle in der Grafik benannten Haupt- und für einen Großteil der Sub-Trends ist die Digitalisierung. Zentral werden vor allem die folgenden technologischen Trends sein, da sie das Zeug haben, der Branche nicht nur neue Werkzeuge an die Hand zu geben, sondern grundsätzlich neue Leistungsoptionen zu ermöglichen:

Artificial Intelligence (AI): Intelligente Algorithmen sind heute schon in eine Vielzahl sicherheitstechnischer Anwendungen integriert. Mit ihnen sollen beispielsweise Videodaten nach auffälligen Ereignissen analysiert werden. Das funktioniert teilweise schon ganz gut. Doch Künstliche Intelligenz, oder Artificial Intelligence, stellt die nächste Stufe in der Entwicklung hin zu Advanced Analytics dar. Hierunter wird in der Regel ein Computerprogramm verstanden, dass vergleichbar zum menschlichen Gehirn dazu in der Lage ist, zum Beispiel Sprache und Verhaltensweisen zu erkennen und sich über die gemachten Erfahrungen selbständig weiter zu entwickeln. Im Großen zeigen das kognitive, lernbasiertes System „Watson“ von IBM und Googles „AlphaGo“ wohin die Reise geht. Die Sicherheitstechnik dürfte für ihre Anwendungen vor allem von Produkten wie dem ebenfalls von IBM entwickelten Chip „TrueNorth“ profitieren, der als neuromorpher Computer zukünftig viele Anwendungen leistungsfähiger und im wahrsten Sinne des Wortes intelligenter unterstützen kann.

Advanced Command & Control Systems: Ein sicherheitstechnischer Leitstand, zum Beispiel eines Gebäudekomplexes integriert mehr und mehr unterschiedliche Gewerke wie Videoüberwachung, Einbruch- und Brandmeldung sowie Zutrittsmanagement. Häufig werden diese Systeme unter dem Schlagwort „PSIM“ (Physical Security Information Management) zusammengefasst. Wenn aber ein größerer Rahmen aufgespannt wird, dann hilft ein integriertes, aber dennoch singuläres System nicht immer weiter. Die Herausforderung wird daher sein, Überwachung, intelligente Analyse, Planung und die sogenannten First Responders in einem integrierten Metasystem zusammen zu bringen. Hier kann sich die Branche unter anderem an den Entwicklungen rund um die „C4ISR-Architekturen“ (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) aus dem (para-) militärischen Umfeld inspirieren lassen. Ziele sind unter anderem schnelle Gefahrenerkennung und Entscheidungen sowie zügige Gefahrenabwehr in komplexen, mehrdimensionalen Situationen.

Robotics: Gerade im öffentlichen Raum, in schwer zu überwachenden beziehungsweise zugänglichen Gebieten, oder im Falle höchster Gefahr für die Sicherheitskräfte werden für die Zukunft immer mehr Roboter, wie UGVs (Unmanned Ground Vehicles) oder UAVs (Unmanned Aerial Vehicles) zum Einsatz kommen. Gerade Drohnen sind bestens geeignet, das Sicherheitspersonal bei der Überprüfung von kritischen Situationen zu unterstützen. Einige Autoren gehen sogar soweit, die Drohnen als eine neue Art der Augmented Reality zu beschreiben. Zur Zeit sind Entwicklungen zu beobachten, die darauf hinauslaufen, die Drohnen über Machine Learning in der Datensammlung zu unterstützen beziehungsweise – wie etwa Shield AI zeigt – Machine Learning zu nutzen, um Drohnen zu befähigen, andere Drohnen anzuleiten und durch gemeinsame Interaktion schneller die gewünschten Ergebnisse zu liefern (Swarm Intelligence).

Blockchain: Laut dem Weltwirtschaftsforum zählt die Technologie zu den sechs Megatrends, welche die Gesellschaft in den kommenden Jahren nachhaltig beeinflussen werden. Der Grundgedanke der Blockchain-Technologie geht in seinem Wesen zurück auf dezentral geführte Kontobücher (Distributed-Ledger-Technologie). Im Prinzip kann die Blockchain auch als verteiltes Datenbankmanagementsystem bezeichnet werden, das auf einer kontinuierlich erweiterbaren Liste von miteinander verketteten Datensätzen besteht. Dabei bestehen die Vorteile der Technologie darin, dass sie eine digitale Verbriefung von Werten beziehungsweise Daten ermöglicht, die im Ergebnis dazu beiträgt, Kosten einer Transaktion zu sparen (Wegfall des „Man-in-the-Middle“), eine höhere Prozesseffizienz zu erreichen (Wegfall von Medienbrüchen) und gleichzeitig die Sicherheit zu steigern. So setzt zum Beispiel auch Porsche für das Öffnen und Schließen seiner Autos via App auf diese Technologie, was sicherlich auch die Hersteller von Zutrittstechnologie inspirieren dürfte.

Social Media Integration: Immer mehr Unternehmen und Behörden beginnen, soziale Medien als Kommunikationsinstrument in Krisensituationen zu nutzen. Das hat unter anderem die Reaktion der Bayrischen Polizei auf den Amoklauf in München 2016 gezeigt. Umgekehrt können soziale Medien aber auch dazu eingesetzt werden, über Social Listening-Plattformen und sogenannte Social-Intelligence-Methoden Gefahren und Bedrohungen zu erkennen und auf solche aufmerksam zu machen. So zeigte das Beispiel eines in London ansässigen Unternehmens, dass das dortige Security-Management mehr und raschere Informationen über risikorelevante Vorfälle in der Nähe des Firmenstandorts über Twitter als über die Polizei erfahren hat. Zentral ist, dass mit Hilfe der Social Intelligence in Echtzeit wichtige Informationen über die Sicherheit eines Objekts oder einer Person gewonnen werden können.

Building Information Modeling (BIM): Zugegeben, BIM ist in Deutschland noch nicht so verbreitet, wie in anderen europäischen Ländern. Dennoch wird BIM in Zukunft gerade bei Großprojekten eine immer größere Rolle spielen. Hierauf müssen sich die Player der Branche einstellen. So bietet zum Beispiel Bosch seit Ende 2016 BIM-Modelle für seine Produkte an. Wichtig ist jedoch, dass BIM nicht nur die Planungsphase eines Bauvorhabens unterstützt. Auch die Errichtungsphase soll durch den Einsatz von BIM effizienter und koordinierter vonstattengehen. Da BIM auch Auswirkungen auf die Betriebsphase eines Gebäudes und damit auf die Verknüpfung aller technischen und betriebsrelevanten Daten haben wird, sind auch Hersteller von sicherheitstechnischen Leitständen beziehungsweise PSIM-Systemen mit diesem Trend konfrontiert.

Zu vielen der in diesem Artikel beschriebenen Trends lassen sich noch eine Vielzahl interessanter Informationen für die Sicherheitstechnik anführen. Einer Artikelserie, die 2019 exklusiv in PROTECTOR & WIK erscheint, wird auf die interessantesten Trends detaillierter eingehen, um weitere Ideen und Impulse für die Geschäftsentwicklung zu geben.

Dr. Peter Fey, ist Mitglied der Geschäftsleitung der Münchner Unternehmensberatung Dr. Wieselhuber & Partner.

Bild: Dr. Wieselhuber & Partner GmbH

Dr, Peter Fey, Mitglied der Geschäftsleitung der Dr. Wieselhuber & Partner GmbH, www.wieselhuber.de