Sobald die 5G-Technologie breiter einsetzbar wird, wird es zu einer engen Vernetzung von Unternehmensprozessen und Produktionsanlagentechnologien kommen.

KI, Cloud, 5G

In einer Studie des Kuratoriums für Verkehrssicherheit werden die Chancen und Herausforderungen neuer Technologien und ihre Auswirkungen auf die Eigentumskriminalität analysiert.

Die Covid-19-Pandemie hat die Digitalisierung beschleunigt. Neue Technologien fanden Eintritt in alle Bereiche des täglichen Lebens. Dies bringt Chancen, aber bietet Cyber-Kriminellen Angriffsmöglichkeiten. Das *Kuratorium für Verkehrssicherheit (KFV)* hat im November 2020 eine Studie zum Thema „Kriminalität der Zukunft – Herausforderungen, Chancen, Innovation" herausgebracht. In dieser Studie setzen sich die Autoren mit verschiedenen Technologiebereichen auseinander, die Auswirkungen auf die Eigentumskriminalität und Bedeutung für die Strafverfolgungsbehörden haben werden. Sie geben in verschiedenen Bereichen neuer Technologien Anregungen zum richtigen Umgang mit diesen Technologien. Fünf Themenbereiche sollen hervorgehoben werden: Cyber-Sicherheit von Unternehmen, die 5G-Technologie, Cloud-Computing, Quantencomputer und künstliche Intelligenz.

Cyber-Sicherheit. Die Digitalisierung unserer Wirtschaft bringt eine erhöhte Anforderung an die Cyber-Sicherheit. Mehr und mehr Unternehmen und deren Mitarbeiter werden digital miteinander vernetzt. Eine Cyber-Sicherheitsstrategie ist notwendig. Das *KFV* plädiert dafür, dass ein Schutz vor Cyber-Kriminellen ein Unternehmen stärkt, vor allem, weil anzunehmen ist, dass die Gefahr, die von den Tätern ausgeht, weiter steigen wird. Die Europäische Kommission (EK) stellte Mitte Dezember 2020 die EU-Cyber-Sicherheitsstrategie für das digitale Jahrzehnt vor. Diese soll Europas Abwehrfähigkeit gegen Cyber-Bedrohungen stärken und dazu beitragen, dass alle Personen und Unternehmen die Vorzüge der Digitalisierung nutzen können. Die EK präsentierte zwei neue Vorschläge, mit denen die Widerstandsfähigkeit kritischer, digitaler und physischer Infrastruktur erhöht werden soll, die Netz- und Informationssystemsicherheit-2-Richtlinie (NIS 2-RL), mit der die NIS-RL 2016 ersetzt wird, und eine Richtlinie zur Widerstandsfähigkeit kritischer Einrichtungen (RKE-RL).

5G-Technologie. Sobald die 5G-Technologie breiter einsetzbar wird, wird es zu einer engen Vernetzung von Unternehmensprozessen und Produktionsanlagentechnologien kommen. Dank dieser Technologie können größere Datenmengen schneller transportiert werden. Dies ist auch für Privatpersonen eine gute Neuigkeit, da Geräte, die über das Internet miteinander verbunden sind, auch in Haushalten immer mehr Einzug halten. Das *KFV* geht davon aus, dass diese Entwicklung dazu führen wird, dass Cyber-Kriminelle Schwachstellen im System suchen werden. Dies gilt sowohl für staatliche als auch nicht staatliche Akteure im Cyber-Bereich. Die EU ist sich diesem Umstand bewusst. Daher wurden unter der deutschen Ratspräsidentschaft im

FOTO: THODONAL/STOCK.ADOBE.COM

Dezember 2020 Schlussfolgerungen zu den neuen Risiken für die Privatsphäre und die Informations- und Cyber-Sicherheit von IoT-Geräten angenommen. Weiters warnt das *KFV* in seiner Studie davor, dass durch die ansteigende Zahl von Geräten, die im Mobilfunknetz operieren werden, auch die Gefahren einer Übernahme dieser Geräte durch Kriminelle steigt. Das Thema Datensicherheit wird noch aktiver behandelt werden müssen, in Unternehmen sowie im privaten und öffentlichen Bereich. Das *World Economic Forum* geht in seinem globalen Risikobericht 2021 davon aus, dass sich die Generierung von Daten bis 2025 vervierfachen wird. Das *KFV* warnt davor, dass Phishing und DDoS-Attacken durch 5G erleichtert werden.

Cloud-Dienste. Drittens nimmt die Nutzung von Cloud-Diensten im privaten und im gewerblichen Bereich stark zu. Unter Cloud-Computing versteht man das internetbasierte Bereitstellen von Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung. Die EU-Mitgliedsstaaten haben im Oktober 2020 eine Deklaration unterzeichnet, mit der sie den Weg zu einer europäischen Cloud bahnen wollen. ENISA, die Agentur der Europäischen Union für Cyber-Sicherheit, wurde beauftragt, ein europäisches Zertifizierungsschema für Cloud-Dienste auszuarbeiten. Auch in der Studie des *KFV* wird darauf verwiesen, dass die Cyber-Sicherheit und Kontinuität der Anbieter umso wichtiger werden, je mehr Unternehmen Privatpersonen oder öffentliche

Die Gewährleistung von Datenschutz und Cyber-Sicherheit sind wichtige Punkte für die Auslagerung von Informationen in Cloud-Dienste.

Stellen Cloud-Services in Anspruch nehmen. Aus Datenschutzgründen wäre es zu befürworten, wenn sowohl private als auch Unternehmensdaten in Europa blieben, wo sie der Datenschutzgrundverordnung unterworfen sind. Im privaten Bereich wird in der Studie des *KFV* vor allem darauf hingewiesen, dass Fotos und kritische Dokumente in Clouds besser geschützt werden sollen, da die Gefahr steigt, Opfer von Erpressung zu werden.

Quantentechnologie. An vierter Stelle müssen die Entwicklungen in der Quantentechnologie beobachtet werden. Die Geschwindigkeit von Computern wird immer mehr zur Herausforderung. Die Quantentechnologie bringt neue Chancen, vor allem hinsichtlich

STUDIE

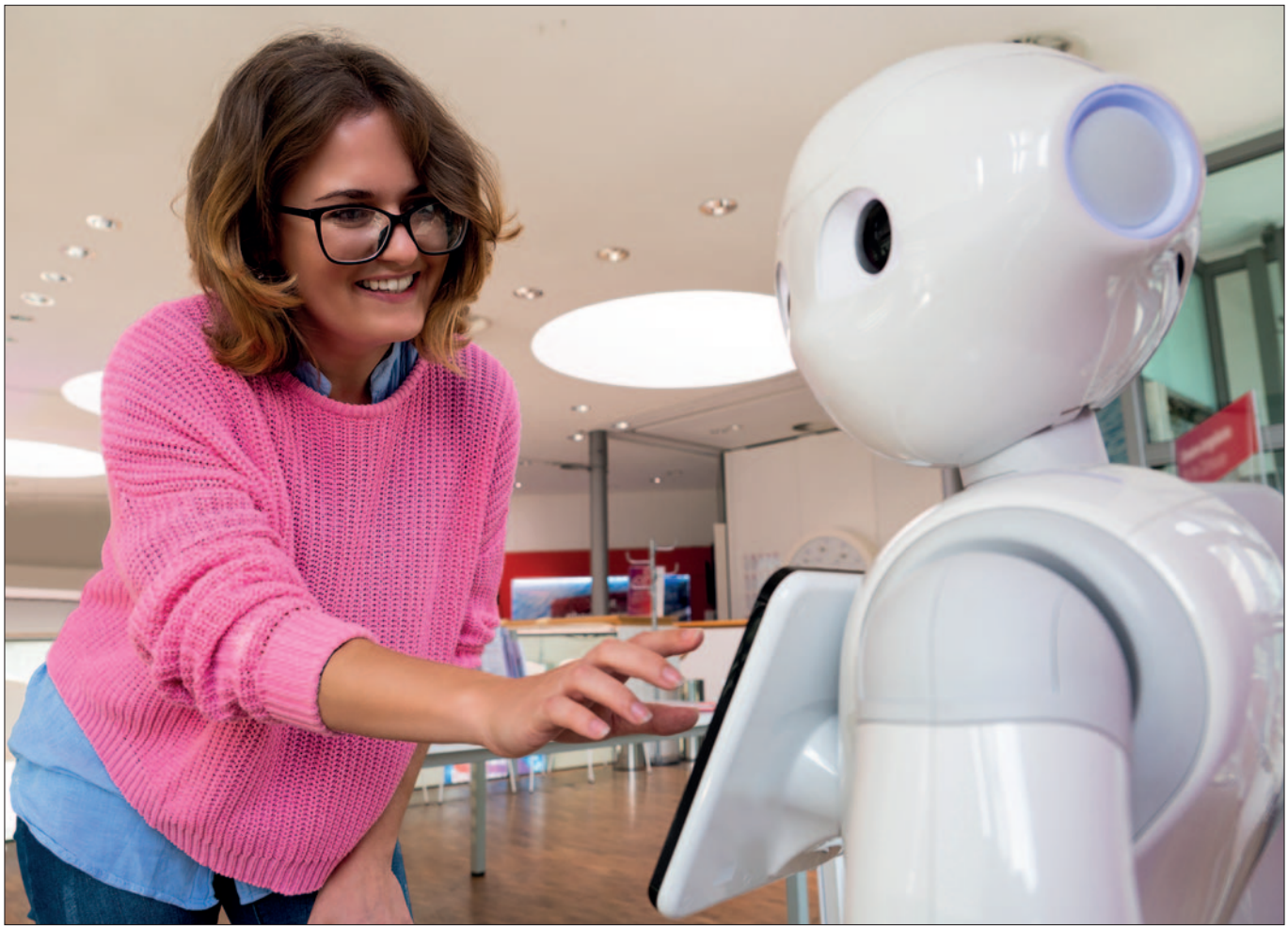
Verlagerung der Einbruchskriminalität

Maßnahmen zur Eindämmung der Covid-19-Pandemie im Frühjahr 2020 führten zur Verlagerung von Einbrüchen. Eine Studie aus den USA belegt, wie es in Detroit innerhalb weniger Tage zu einer Verlagerung von Einbrüchen von Wohngegenden in Stadtviertel mit mehr gewerblicher Nutzung kam.

Die Wissenschaftler analysierten 360 Einbrüche, die im Kriminalitätsbericht der Polizei in Detroit im März 2020 erfasst wurden. Dafür wurde der März in drei Phasen geteilt, in denen es keine Covid-19-Maßnahmen gab (Anfang bis 10. März), sie eingeführt wurden (bis 24. März) und danach streng umgesetzt wurden (bis Ende März). Durch die Covid-19-Maßnahmen kam es zu einem Rückgang der Zahl an Einbrüchen und einer Verlagerung der Einbruchsorte.

Im letzten Monatsdrittel kam es zu einem Anstieg der Zahl an Einbrüchen in Gegenden, die eine höhere gewerbliche Nutzung hatten. Einbrüche verlagerten sich von Wohngegenden in Viertel mit weniger Einwohnern. Hierbei liegt die Annahme nahe, dass sich die Täter bewusst Gegenden aussuchen, in denen sie am wenigsten wahrscheinlich ertappt werden und wo die leichteren und weniger beaufsichtigten Einbruchsorte verfügbar sind. Da der untersuchte Zeitraum von einem Monat eher kurz war, fordern die Studienverfasser eingehendere Analysen mit mehr Datenmaterial. Ähnlich wie bei anderen amerikanischen Städten wie Austin, Los Angeles, Memphis und San Francisco wird in Detroit in Summe ein Rückgang der Einbruchskriminalität aufgrund der Covid-19-Maßnahmen beobachtet.

Studie: Felson et al.: Routine activity effects of the Covid-19 pandemic on burglary in Detroit, March, 2020. Crime Science (2020) 9:10.



Künstliche Intelligenz wird viele Vorteile in der Cyber-Sicherheit bringen, etwa um Schwachstellen schneller zu finden.

Kryptografie und Cyber-Sicherheit. Die US-amerikanischen Tech-Riesen arbeiten an der Entwicklung von Quantencomputern. In Österreich ist das *Austrian Institute of Technology (AIT)* führend in diesem Bereich. Auch viele Staaten interessieren sich für Quantentechnologie. Dabei geht es den Staaten vor allem darum, als Erster ein Verfahren zu entwickeln, das vor Attacken mittels Quantencomputer sicher ist. Die Europäische Kommission wendet eine Milliarde Euro an Fördermitteln dafür auf, dass aus der Quantentechnologie nicht nur Quantencomputer, sondern auch andere konkrete Produkte und Anwendungen entstehen. Das *KFV* empfiehlt in seiner Studie, dass Staaten und Konzerne in Zukunft in diesem Bereich mehr zusammenarbeiten sollen, um umfassende Konzepte zu entwickeln, damit das Potenzial und die Gefahr von Quantencomputern analysiert und Maßnahmen gesetzt werden können.

Künstliche Intelligenz. Zuletzt müssen die Entwicklungen im Bereich der künstlichen Intelligenz (KI) beobachtet werden. Das so genannte „Deep Learning“ (eine besonders potente Form maschinellen Lernens) brachte in letzter Zeit nicht nur alltagstaugliche Technologie hervor, es wird auch in der Kriminalitätsbekämpfung eingesetzt. Technologie-Unternehmen setzen Experten und leistungsstarke Computer ein, um an der Entwicklung von KI zu arbeiten. Das *KFV* meint, dass Cyber-Kriminelle vor allem aktiv sein werden beim Hacking, Kodieren, bei Deepfakes sowie der Automatisierung von Angriffen. KI wird hier viele Vorteile in der Cyber-Sicherheit bringen, etwa um Schwachstellen schneller zu finden. Quantencomputer und KI werden laut *KFV* die Cyber-Sicherheitslandschaft revolutionieren.

Senioren. Das *KFV* hebt in seiner Studie besonders die Bedeutung der Digitalisierung für die Gesellschaft hervor. Es geht insbesondere auf Seniorinnen und Senioren, als Risikogruppe im Bereich Kriminalität durch neue Technologien, ein. Aufgrund der voranschreitenden Digitalisierung bewegt sich diese Gruppe vermehrt im digitalen Raum und ist dadurch den hier typischen Kriminalitätsformen ausgesetzt. Das *KFV* geht davon aus, dass der Neffen- oder Enkeltrick oder das Love-Scamming in digitaler Form insbesondere als Deepfake eingesetzt werden wird. Immer mehr Haushaltsgeräte werden bald nur noch hochtechnologisiert zu kaufen sein, was vermehrt Schutzmaßnahmen erfordern wird, mit denen diese Gruppe nicht vertraut sein könnte. Zum Schutz dieser Gruppe fordert das *KFV* ein hohes Engagement der Zivilgesellschaft und der Strafverfolgungsbehörden in der Präventionsarbeit.

Die rasanten technologischen Entwicklungen bestimmen das staatliche, wirtschaftliche und gesellschaftliche Handeln. Zum einen bringt uns dieser Fortschritt Verbesserungen, wie den Einsatz von Quantencomputern in der Cyber-Sicherheit oder die 5G-Technologie für Unternehmen, zum anderen birgt er aber auch beträchtliche Risiken. *Caroline Schmidt*

FOTO: CHARFSINN86/STOCK.ADOBE.COM