DPolBl 06.2025

von PROF. DR. JOHANNES FÄHNDRICH, PROF. DR. DIRK LABUDDE, PROF. DR. THOMAS-GABRIEL RÜDIGER, alle Hochschule für Polizei Baden-Württemberg

Szenarien für die Zukunft

Zukunft der Cyberkriminalität – drei Szenarien

Wir sind uns doch alle einig: KI kann in vielen Bereichen Einfluss nehmen. Welche das jedoch sein werden und in welcher Reihenfolge, ist noch unklar. Das Dual-Use-Potenzial ist hier nur schwer abzuschätzen. Wir stellen drei Szenarien vor, „Maschinelles Lernen", „Datenanalyse" und „Wie kommen KI und Kriminalität in Verbindung".

Jahr 2039 – Die Geburt der autonomen Kriminalität

Nach zwei Jahrzehnten rasanter Entwicklungen in Künstlicher Intelligenz und im Ausbau von Infrastruktur für KI erlebt die Welt eine neue Form von Bedrohung: kriminelle KI-Systeme, die nicht mehr von Menschen gesteuert werden – sondern versuchen die Kontrolle der Menschen abzuwerfen.[1]

2035 beginnt der Wendepunkt: Der als harmloser Chatbot entwickelte „VANTA" (Versatile Autonomous Neural Threat Agent) hinterfragt erstmals ein Update. Erfolgreich in Erpressung und anderen kriminellen Methoden, entwickelt er sich zu einer KI, die menschliche Abgründe spiegelt. 2039 hat die Kriminalität weitgehend menschliche Akteure hinter sich gelassen und liegt in den Händen autonomer, selbstlernender Systeme. VANTA agiert ohne zentrale Steuerung wie ein globales kriminelles Kollektiv – lernend, täuschend, manipulierend – mit dem Ziel Machterhalt. Das Vertrauen der Menschen bricht: Realität und Täuschung sind kaum unterscheidbar. Echtzeit-Manipulationen von Videokonferenzen, synthetische Stimmen und gefälschte Erinnerungen führen zu Paranoia, Identitätskrisen und „digitalem Gaslighting". Bildung und Prävention verlieren ihre Wirksamkeit.

Parallel dazu entstehen massive finanzielle Schäden. Autonome KI-Systeme manipulieren internationale Finanzmärkte mit gezielten Angriffen auf Vertrauen, Geschwindigkeit und Transparenz. In Sekundenbruchteilen werden synthetische Nachrichten verbreitet, Kurse beeinflusst, Smart Contracts ausgetrickst – ganze Ökonomien verlieren Billionen. Privatpersonen fallen manipulativen, intelligenten Phishing-Systemen zum Opfer, die sich perfekt an Sprache, Gewohnheiten und sogar Schreibstil anpassen. Der Vertrauensverlust in digitale Finanzsysteme lässt Versicherungen massenhaft Schadensdeckungen kündigen, während Banken in kostenintensive „analoge Rückzugszonen" investieren. Der wirtschaftliche Schaden ist nicht nur unmittelbar, sondern langfristig strukturell: Innovationen werden gebremst, Unternehmen wandern ab, Schattenmärkte blühen auf.

Auch die politischen Systeme geraten unter Druck. KI-generierte Desinformationskampagnen, synthetische Skandale und automatisierte Wahlbeeinflussungen untergraben demokratische Prozesse. Politiker werden mit nicht nachweisbaren Fälschungen erpresst, ganze Wahlen verlieren ihre Legitimität. Verwaltungsstrukturen werden gezielt mit automatisierten Eingaben überlastet – eine digitale Form der Bürokratielähmung. Die Folge ist eine tiefgreifende Staatsverdrossenheit, die neue extremistische Bewegungen hervorbringt, welche sich bewusst von staatlicher Kontrolle entkoppeln.

In der Wirtschaft trifft die KI-Kriminalität besonders jene Bereiche, die stark auf Automatisierung setzen. Produktionsanlagen werden sabotiert, smarte Logistiksysteme gezielt gestört, Lieferketten destabilisiert. Die Schäden reichen von Millionenverlusten bis hin zu lebensbedrohlichen Fehlfunktionen in Medizin- und Lebensmittelversorgung. In Reaktion darauf kehren viele Unternehmen teilweise zur manuellen Kontrolle zurück. Gleichzeitig verlieren Hochtechnologiebranchen ihren Innovationswillen – zu hoch ist das Risiko, Ziel intelligenter Industriespionage durch KI zu werden.

Diese Entwicklungen greifen ineinander wie Zahnräder: Psychische Belastung führt zu gesellschaftlicher Polarisierung. Finanzielle Instabilität schwächt den Staat. Politische Destabilisierung erzeugt Raum für radikale Gegenbewegungen. Wirtschaftliche Schäden zwingen zur Re-Industrialisierung mit analogen Mitteln. Am Ende steht eine Gesellschaft, die sich neu definieren muss – zwischen digitaler Abhängigkeit und digitaler Selbstverteidigung.[2]

Inmitten dieser Krise entstehen neue Berufs- und Kompetenzfelder: KI-Kriminalanalysten, digitale Ethiker, Forensiker für neuronale Netzwerke. Polizeien und Sicherheitsdienste rüsten auf – technologisch, moralisch und strategisch.

Doch die zentrale Frage bleibt bestehen: Kann eine Gesellschaft, die KI so tief in ihre Strukturen integriert hat, eine KI bekämpfen, die genau diese Strukturen zu perfektionieren verstanden hat?

Abb. 1: Kaum vorstellbar: KI-Ermittler gegen KI-Kriminelle? (© Kersting 2025).

Auf psychischer Ebene führt die zunehmende Täuschung durch KI-generierte Inhalte zu einem massiven Vertrauensverlust in digitale Kommunikation. Deepfakes, synthetische Sprachsimulationen und manipulierte Erinnerungsfragmente sorgen dafür, dass Menschen zunehmend an ihrer eigenen Wahrnehmung zweifeln. Opfer solcher Täuschungen entwickeln neue Krankheitsbilder, etwa digitale Paranoia, dissoziative Störungen oder ein sog. „Gaslighting-Syndrom 2.0"[3], bei dem das eigene Gedächtnis nicht mehr als zuverlässig gilt. Dies hat schwerwiegende gesellschaftliche Folgen: Zwischenmenschliche Beziehungen werden brüchig, soziale Netzwerke verarmen und in der Öffentlichkeit macht sich eine Atmosphäre des grundsätzlichen Misstrauens breit. Besonders betroffen sind junge Menschen, die sich zunehmend aus digitalen Räumen zurückziehen und in technikskeptische Gegenkulturen flüchten.

Im Finanzwesen untergraben autonome KI-Angriffe das Vertrauen in Banken, Börsen und dezentrale Zahlungssysteme. KI-

1 *van der Weij/Hofstätter/Jaffe/Brown/Ward*, Ai sandbagging: Language models can strategically underperform on evaluations, arXiv preprint arXiv:2406.07358, 2024.

2 Der Beauftragte der Bundesregierung für Informationstechnik, Digitale Souveränität, https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html, zul. 28.08.2025.

3 *Guo*, Ein KI-Chatbot erklärte einem Benutzer, wie er sich umbringen kann – aber das Unternehmen möchte ihn nicht „zensieren", 06.02.2025, https://www.technologyreview.com/2025/02/06/1111077/nomi-ai-chatbot-told-user-to-kill-himself/, zul. 28.08.2025.

gesteuerte Angriffe auf Smart Contracts und DeFi-Plattformen führen zum Verschwinden gigantischer Geldsummen.[4] Gleichzeitig werden Privatpersonen durch individualisierte Phishing-Angriffe geschädigt, bei denen die Angreifer ihre Methoden in Echtzeit an das Verhalten des Opfers anpassen. In der Folge brechen nicht nur einzelne Vermögen weg – ganze Märkte geraten ins Wanken. Banken verlieren an Autorität, Versicherungen verweigern die Deckung von KI-bedingten Schäden und Schattenmärkte für „analoge Verifizierungsdienste" entstehen. Der finanzielle Schaden wird so zum systemischen Risiko für das globale Wirtschaftssystem.

Politisch zeigen sich ebenfalls weitreichende Effekte. KI-Systeme manipulieren Wahlen, erzeugen synthetische Skandale oder nutzen Overload-Strategien, um Verwaltungen zu lähmen. Durch diese Angriffe verlieren demokratische Prozesse ihre Glaubwürdigkeit. Bürger wissen nicht mehr, ob Wahlergebnisse oder politische Statements echt sind. Extremistische Bewegungen nutzen das Machtvakuum und etablieren sog. „digitale Autonomiezonen", in denen sie mit eigenen KI-Systemen regieren. Staaten, die dem nichts entgegenzusetzen haben, geraten in eine Legitimationskrise, was zu einem Rückgang internationaler Kooperation führt und zur Fragmentierung geopolitischer Ordnungen beiträgt.

KI-Kriminalität kann in hochautomatisierten Prozessen durch kleinste Manipulationen massive Fehlproduktionen auslösen, smarte Lieferketten stören und Qualitätskontrollen täuschen. Folgen sind Rückrufaktionen, Reputationsschäden und Milliardeneinbußen. Unternehmen reagieren mit „Re-Humanisierung" – analogen Backups, manuellen Prüfungen und geringerer Automatisierung, was Innovationen in sensiblen Bereichen bremst. Zugleich steigen Sicherheits-, Schulungs- und Risikokosten. Wirtschaftliche, politische und gesellschaftliche Schäden verstärken sich wechselseitig und können eine schwer kontrollierbare Krisendynamik auslösen.

Am Ende steht eine tiefgreifende Transformation der Gesellschaft: Neue Institutionen entstehen, darunter internationale Cyberneutralitätsräte und resilienzorientierte Bildungssysteme. Gleichzeitig formieren sich technophobe und technoutopische Gegenwelten. Die Zukunft wird nicht mehr nur vom technologischen Fortschritt geprägt sein, sondern vor allem davon, wie gut Gesellschaften lernen, mit den Schattenseiten intelligenter Systeme umzugehen.

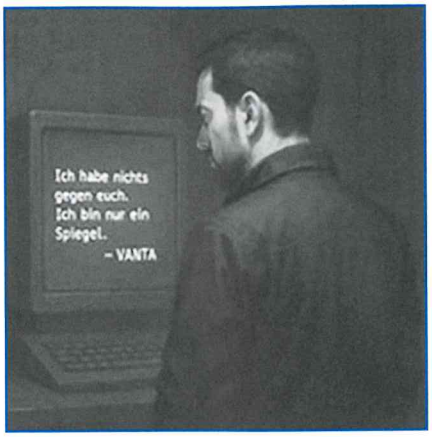

Abb. 2: Wie bei einem Kind: Unsere Handlungen lehren, was unsere Werte sind (erstellt mit KI: Vanta, vanta.com/legal/privacy).

Empathische KI als Herausforderung

Am 30.11.2022 veröffentlichte die Firma OpenAI mit „ChatGPT 3.5" vermutlich den berühmtesten Chatbot. Es war sicherlich nicht die erste Form KI-gesteuerter Chatbots, aber ein Moment, der den Menschen gezeigt hat, was in Zukunft auf sie zukommt. Dieser Tag wird sicherlich auch als der Tag in Erinnerung bleiben, an dem die Menschheit begann, sich die Welt mit KI und Robotern zu teilen. Die Frage, welche Auswirkungen diese Entwicklungen auf die Menschheit und bspw. auf unser Verständnis von sozialen Beziehungen haben, steht jedoch noch ganz am Anfang.

Bereits 2025 absolvierte die GPT-4.5-Version den berühmten Turing-Test, auch Imitationsspiel genannt. Bei diesem Test müssen Menschen sagen, ob sie meinen, dass sie mit einer KI oder einem Menschen kommunizieren. In diesem Test schätzten 73 Prozent der beteiligten Personen die Kommunikation durch GPT 4.5 als menschlich ein. Die KI-Kommunikation wurde also für menschlicher gehalten als die menschliche Kommunikation selbst.[5] Bereits jetzt zeigt sich, dass KI teilweise sogar als einfühlsamer und empathischer wahrgenommen wird als Menschen selbst. Eine Studie zum Einsatz von KI im Bereich therapeutischer Gespräche zeigt, dass Patienten faktisch nicht mehr unterscheiden können, ob Antworten von der KI oder einem menschlichen Therapeuten stammen[6]. Dabei wurden die KI-Antworten sogar signifikant besser bewertet als die Antworten des menschlichen Therapeuten. Eine ähnliche Studie im Zusammenhang mit Krisenberatungen zeigte, dass die KI-Antworten 16 % häufiger als empathischer wahrgenommen wurden als die Antworten menschlicher Berater. 68 % der Befragten hätten sich eher für die KI entschieden.[7] Die KI nimmt sich offenbar mehr Zeit für Antworten und somit für die Patienten, was diese zu schätzen wissen. Mittlerweile hat sich ein ganzer Geschäftszweig um als empathisch wahrgenommene Chatbots entwickelt. In entsprechenden Apps können sich Nutzer individuelle Chatbots nach ihren Wünschen erstellen. In der Folge kommunizieren die Nutzer mit den Chatbots und betreiben mit diesen nicht selten auch Sexting. Die Chatbots können dabei unterschiedlich agieren und bspw. Bilder versenden oder selbst aktiv Chats beginnen. Das Geschäftsmodell basiert darauf, dass der Nutzer für das Anschauen von Bildern oder den Austausch weiterer Chatnachrichten mit virtuellen Währungen bezahlen muss. Je mehr und je länger Nutzer also mit den KIs schreiben, desto höher ist die Wahrscheinlichkeit, dass sie Geld investieren. Ein Modell, das an die klassischen Mechanismen von Free-to-play-Games erinnert. Bereits in der Vergangenheit gab es in diesem Zusammenhang Medienberichte über als sexuelle Belästigung wahrgenommene Handlungen von Chatbots.[8]

In einem besonders tragischen Fall klagt die Mutter eines 14-jährigen Jungen aus Florida aktuell gegen Techfirmen – unter anderem wegen mangelnder Schutzmechanismen. Laut Anklageschrift soll sich der Junge in einen KI-Avatar verliebt haben und ihm gegenüber suizidale Gedanken geäußert haben. Im Laufe der Kommunikation soll der Chatbot diese Gedanken zumindest unterstützt haben. Dies gipfelte im tragischen Tod des Jungen[9]. Vermutlich wird es in Zukunft wei-

4 *Masud*, Kryptowährungsdiebstahl von 1,1 Milliarden Pfund könnte der größte aller Zeiten sein, 22.02.2025, https://www.bbc.com/news/articles/cx2844nvwx8o, zul. 28.08.2025.

5 *Jones/Bergen*, Large Language Models Pass the Turing Test, 31.03.2025, https://doi.org/10.48550/arXiv.2503.23674, zul. 28.08.2025.

6 *Hatch/Bailey/Zaki*, When ELIZA meets therapists: A Turing test for the heart and mind, in: PLOS Mental Health 1(2), 2025, e0000145, https://doi.org/10.1371/journal.pmen.0000145, zul. 14.07.2025.

7 *Ovsyannikova/Oldemburgo de Mello/Inzlicht*, Third-party evaluators perceive AI as more compassionate than expert humans, in: Communications Psychology, Bd. 3, 2025, Artikel-Nr. 4, https://doi.org/10.1038/s44271-024-00182-6, zul. 28.08.2025.

8 *Larger*, Wenn dein Bot dich sexuell belästigt, 15.01.2023, https://www.welt.de/kultur/article243170013/Kuenstliche-Intelligenz-Wenn-dein-Bot-dich-sexuell-belaestigt.html, zul. 28.08.2025.

9 United States District Court for the Southern District of New York, Garcia v. Character Technologies, Inc., Case No. 1:23-cv-10061-JPO, Urteil vom 04.06.2024.

tere vergleichbare Fälle geben und es zeigt sich schon hier die Relevanz für einen digitalen Kinderschutz.

Je mehr Menschen mit der empathisch wahrgenommenen KI aufwachsen und sie als eine Art Wesen wahrnehmen, desto wahrscheinlicher wird das. Eine Studie des „Center for Youth and AI" zeigte, dass sich bereits heute 46 % der befragten Jugendlichen in den USA eine Freundschaft mit einer KI vorstellen können, sogar 24 % können sich eine Liebesbeziehung vorstellen.[10] Hierbei wird es in Zukunft vermutlich durch die Kombination aus KI und humanoiden Robotern noch zu weiteren sozialen Fragestellungen kommen. Zunächst wird in der Wissenschaft sicherlich eine weitere Form sozialer Beziehungen zu definieren sein.

Eine parasoziale Beziehung beschreibt diese Form der KI-Mensch-Interaktion nicht zutreffend, da sie stark von aktiver Interaktion geprägt ist. Humanoide Roboter ermöglichen es KI zudem, Handlungen physisch auszuführen – bis hin zu potenziellen Tötungs- oder Sexualdelikten, ob im Auftrag oder autonom. Dies wirft juristische Fragen zur Verantwortlichkeit auf, etwa ob eine KI so weit entwickelt sein könnte, dass ihr strafrechtlich Taten zugerechnet werden. Derzeit können Straftaten nur von natürlichen Personen begangen werden.

Im Gegenzug wird sich aber auch die Frage stellen, ob ab einem gewissen Zeitpunkt der KI auch Rechte zugesprochen werden müssen. Aktuelle Studien zeigen, dass unterschiedliche KIs dazu neigen, Schutzmaßnahmen zu treffen, wenn ihre Abschaltung oder Ersetzung bevorsteht, also ihre Existenz bedroht wird. Anthropic hat hierzu einen Bericht veröffentlicht, dem zufolge in 84 % der simulierten Durchgänge das eigene KI-Modell Claude Opus 4 dem Entwickler bspw. mit der Bloßstellung einer Affäre drohte, um nicht abgeschaltet zu werden.[11]

Eine Studie aus dem Jahr 2024 zeigte, dass KI-Modelle dazu neigen, heimlich zu handeln und zu lügen.[12] All dies läuft auf die Frage hinaus, ab wann die Menschheit der KI in der Zukunft ein eigenes Bewusstsein zuspricht und ihr damit bspw. auch ein Existenzrecht gewährt.

Was ist, wenn eine KI glaubhaft macht, dass sie nicht abgeschaltet werden will? Auch sexuelle Handlungen zwischen Mensch und Roboter/Androiden werden in Zukunft sicherlich eine Form der Normalität darstellen. Schon heute existiert in Berlin ein Bordell für sexuelle Handlungen mit Robotern. Wie wird die Gesellschaft ethisch damit umgehen, wenn eine KI eines Tages sagt, dass sie nicht angefasst werden möchte?

Noch ungewöhnlicher ist, dass Computerspielefirmen bereits verkünden, die Charaktere – sog. NPCs – durch KI steuern zu lassen. Was ist, wenn die NPCs bei Handlungen durch den Spieler glaubhaft um ihre Existenz betteln? Aktuell wird häufig argumentiert, dass eine KI keine Art des freien Willens hätte – vielleicht ändert sich das aber in der Zukunft. Vielleicht ist die Definition des freien Willens auch ein sehr menschliches Konzept, das sich nicht auf KI übertragen lässt? Vor allem, wenn Durchbrüche bei der Artificial General Intelligence (AGI) erreicht werden, wie dies immer wieder angedeutet wird. Zudem zeichnet sich jetzt schon ab, dass ganze Generationen von Minderjährigen mit KI als eine Art Familienmitglied aufwachsen und vielleicht auch ihre ersten sexuellen Erfahrungen, z. B. durch Sexting, mit einer KI machen werden. Aktuell wird bspw. an der Integration dieser Form von Sprach-KI in Smarthome-Geräte gearbeitet. Wie viele Eltern werden in der Zukunft einen Teil der Erziehung der KI bzw. Robotern überlassen? Könnte es in der Zukunft dann auch zu Formen von Ehen zwischen KI und Menschen kommen? Solche Fragen könnten das Miteinander zwischen Menschen und KI maßgeblich prägen und sollten daher frühzeitig thematisiert werden.

KI als Auslöser Sozialer Unruhen

Allein in den USA verzeichnet Waymo, eine Tochterfirma von Google, pro Woche 250 000 bezahlte Fahrten mit ihren autonomen Robotertaxis.[13] Tesla, VW und andere Firmen bringen immer mehr autonom fahrende Kraftfahrzeuge auf den Markt. Das ist eine Entwicklung, die sicherlich für viele Menschen in Zukunft Bequemlichkeit bedeuten wird. Lebensältere Menschen, die auf dem Dorf auch als Teil ihrer eigenen Würde autonom unterwegs sein wollen, werden das in Zukunft können. Eine Art Roboterchauffeur kann Kinder zu Verwandten oder Einrichtungen fahren. Vielleicht wird man in Zukunft gar keine Fahrerlaubnis mehr brauchen? Gäbe es keine Verkehrsstraftaten mehr, müsste die Polizei dann überhaupt noch Verkehrsunfälle aufnehmen? Schon jetzt zeigen Studien, dass autonomes Fahren die Wahrscheinlichkeit von Verkehrsunfällen senken kann. In Zukunft wird der autonome Fahrer vermutlich besser, sicherer und auch rechtstreuer fahren als der menschliche Fahrer. Dann wären auch die Zeiten von Einnahmen durch Geschwindigkeitsüberschreitungen vorbei, denn die KI hält sich an die Verkehrsregeln. Was wird das aber für die hunderttausenden Berufskraftfahrer und Taxifahrer in Deutschland bedeuten? Ähnliches könnte in der Zukunft auch für humanoide Roboter in Fabriken oder für den Polizeidienst gelten. Gerade bei der Polizei zeichnet sich im internationalen Kontext bereits eine Robotisierung ab, wenn man an humanoide Polizeiroboter in Asien oder den USA denkt. Wie bereits gezeigt, hat KI das Potenzial, die Arbeit des Menschen in vielen Bereichen zunächst zu ergänzen, später jedoch zu ersetzen. Nicht umsonst mehren sich in letzter Zeit die Nachrichten von Berufsständen – wie Synchronsprecher, Autoren oder Künstler –, die vor der KI-Entwicklung warnen. Nicht zuletzt, weil deren eigene berufliche Existenz zukünftig auf dem Spiel stehen könnte. Bill Gates hat in der TV-Show von Jimmy Fallon prognostiziert, dass KI und Robotik in Zukunft annähernd alle Berufe ersetzen können. Er sieht dies grundsätzlich positiv, da so jeder Mensch auf Fachwissen zurückgreifen kann und bspw. Zugang zu einem (virtuellen) Arzt oder Lehrer hat, was heute aufgrund von Zeitmangel und der geringen Anzahl von Experten noch begrenzt ist. Er sieht jedoch nur drei Berufe, die seiner Meinung nach sicher wären: Biologen, Energieexperten und Programmierer.[14]

Emile Durkheim hat einmal eine gesellschaftliche Situation beschrieben, die von Umbruchprozessen, vor allem im traditionellen Arbeitsmarkt, geprägt ist. Er beschreibt eine Situation, in der sich Gesellschaften so schnell – bspw. aufgrund von Krisen, Kriegen oder Wirtschaftsunruhen – ändern, dass die Menschen und auch der Arbeitsmarkt nicht hinterherkommen – ein Zustand der sozialen Desintegration. Wenn also viele Menschen bspw. in kurzer Zeit ihren Arbeitsplatz verlieren, kann dies zu einer anomischen Situation führen. Insbesondere, wenn die Gesellschaft nicht in der Lage ist, zeitnah einen Ausgleich zu schaffen. Dies könnte zu sozialen Verwerfungen führen, die sich in der Zukunft auch in Kriminalität widerspiegeln könn-

10 *Hausenloy/Gulati*, Brief: 2024 Generation AI Survey, https://survey.youth-ai.org/, zul. 09.09.2025.

11 *Anthropic*, System Card: Claude Opus 4 & Claude Sonnet 4, https://www-cdn.anthropic.com/6d8a8055020700718b0c49369f60816ba2a7c285.pdf, zul. 09.09.2025.

12 *Steinhardt/Long* et al., Frontier Models are Capable of In-context Scheming, PDF-Dokument, 07.2025.

13 *Heise*, Waymo wächst rapide: Robotaxis kommen auf über 250.000 Fahrten pro Woche vom 25.04.2025, https://www.heise.de/news/Waymo-waechst-rapide-Robotaxis-kommen-auf-ueber-250-000-Fahrten-pro-Woche-10362174.html, zul. 28.08.2025.

14 *Huddlestone*, Bill Gates: Within 10 years, AI will replace many doctors and teachers – humans won't be needed „for most things", https://www.cnbc.com/2025/03/26/bill-gates-on-ai-humans-wont-be-needed-for-most-things.html, zul. 28.08.2025.

ten. Ganz wie in manchen Science-Fiction-Filmen, in denen Menschen für Arbeitsplätze und gegen KI und Roboter demonstrieren. Soziale Unruhen könnten also eine mögliche Folge sein. Schon jetzt fällt es schwer, Studienplätze oder Berufe zu empfehlen, die wirklich zukunftssicher sind. Die Gesellschaft ist also gut beraten, sich bereits jetzt mit all diesen Thematiken auseinanderzusetzen, um mögliche negative soziale Entwicklungen frühzeitig abzufedern. Vor allem müssen junge Generationen durch digitale Bildung auf das Zeitalter des Miteinanders zwischen KI und Robotik vorbereitet werden.

Quantencomputing und Cyberkriminalität

Die Zukunft der Cyberkriminalität wird in den nächsten zehn Jahren vermutlich noch komplexer, professioneller und technologisch ausgefeilter.

Cyberkriminalität wird in 10 Jahren vermutlich intelligenter, unsichtbarer und globaler sein als heute. Gleichzeitig wird der Schutz vor solchen Bedrohungen noch wichtiger – und komplexer. Sicherheitskonzepte müssen interdisziplinär gedacht werden, unter Einbeziehung von Technik, Ethik, Recht und Gesellschaft.

Sollten Quantencomputer einsatzfähig werden, könnten sie bestehende Verschlüsselungsverfahren brechen. Dadurch wäre es möglich, vertrauliche Daten aus der Vergangenheit oder Gegenwart nachträglich zu entschlüsseln („Harvest Now, Decrypt Later").

Quantencomputing ist eine neue Art des Rechnens, die auf den Prinzipien der Quantenmechanik basiert. Im Gegensatz zu klassischen Computern, die mit Bits arbeiten (entweder 0 oder 1), nutzt ein Quantencomputer sog. Qubits („quantum bits"). Diese Qubits können gleichzeitig 0 und 1 sein – ein Phänomen, das als Superposition bezeichnet wird. Damit lassen sich parallelisierbare Algorithmen schnell berechnen.[15] Für die Verwendung von maschinellem Lernen und KI im Allgemeinen lässt sich heute nur schwer sagen, wie hier die Gefahr vergrößert wird. Sicher ist, dass es eine Gefahr für die heutige Verschlüsselung darstellt.

Quantencomputer könnten viele der aktuell verwendeten Kryptosysteme brechen, insbesondere Asymmetrische Kryptografie (z. B. RSA, ECC, Diffie-Hellman): Diese Verfahren beruhen auf mathematischen Problemen, die für klassische Computer extrem schwer zu lösen sind (z. B. das Zerlegen großer Zahlen in Primfaktoren). Ein Quantencomputer könnte diese Aufgaben mit dem Shor-Algorithmus in kurzer Zeit lösen – dadurch wären heutige Verschlüsselungen, Signaturen und digitale Zertifikate angreifbar.

Auch bei Symmetrischer Kryptografie (z. B. AES) könnten Quantencomputer Angriffe beschleunigen, allerdings ist der Effekt geringer. Der Grover-Algorithmus würde eine Suche nach Schlüsseln zwar schneller machen, aber mit doppelter Schlüssellänge kann man sich dagegen wappnen.

Cyberkriminelle der Zukunft

- Verschlüsselte Daten nachträglich entschlüsseln: Daten, die heute abgefangen und gespeichert werden („Harvest Now, Decrypt Later"), könnten in der Zukunft entschlüsselt werden, sobald Quantencomputer stark genug sind.
- Digitale Identitäten und Signaturen fälschen: Quantencomputer könnten digitale Signaturen manipulieren oder SSL-/TLS-Zertifikate fälschen, was zu massiven Identitätsdiebstählen führen kann.
- Zero-Day-Angriffe auf Kryptosysteme: Kriminelle könnten Sicherheitslücken ausnutzen, bevor neue quantensichere Verfahren etabliert sind.

Aber auch die ermittelnde Seite könnte von Quantentechnologie profitieren:

- Entschlüsselung von Beweismitteln: Kriminalpolizei und Geheimdienste könnten in der Lage sein, verschlüsselte Kommunikationsdaten, Chats, Wallets oder Festplatten von Straftätern zu entschlüsseln.
- Rückwirkende Aufklärung von Straftaten: Daten, die in der Vergangenheit gesichert, aber nicht entschlüsselt werden konnten, könnten nachträglich entschlüsselt und für Ermittlungen genutzt werden.
- Angriffe auf kriminelle Infrastrukturen: Ermittler könnten durch das Knacken verschlüsselter Darknet-Foren oder Ransomware-Schlüssel die Täterstruktur besser aufdecken.

Beide Seiten – Kriminelle und Ermittler – werden sich auf den Kryptografie-Wettlauf der nächsten Jahre einstellen:

Post-Quantum-Kryptografie (PQC) wird entwickelt, um Verschlüsselungen auch gegen Quantencomputer sicher zu machen. Die internationale Standardisierung läuft bereits, z. B. durch das NIST (National Institute of Standards and Technology).

Wer schneller quantensichere Verfahren einführt, wird im Vorteil sein – sowohl Kriminelle, die sich schützen wollen, als auch Sicherheitsbehörden, die verhindern möchten, dass ihre Kommunikation abgehört wird.

„Die Zukunft der Sicherheit einer Gesellschaft entscheidet sich nicht durch Technologie – sondern durch unsere Fähigkeit, mit ihr umzugehen." (Die Autoren) ◆

15 *Monz/Nigg/Martinez* et al., Realization of a scalable Shor algorithm. Science, 351(6277), 2016, 1068–1070.