Sicherheitsgipfel: Alexander Janda, Sylvia Mayer, Kilian Gross, Gerhard Karner, Christian Domany, Karl Schlögl, Wolfgang Schilk

Zwischen Gefahr und Faszination

Beim KSÖ-Sicherheitsgipfel am 4. Juni 2024 in Wien diskutierten Expertinnen und Experten über Chancen und Herausforderungen von künstlicher Intelligenz.

Das Kürzel „KI“ beherrscht in vielerlei Hinsicht die öffentliche Diskussion sowie den Alltag, auch wenn es viele Menschen noch nicht merken. Die Einstellung zu dieser Technologie wird von Angst und Bedenken sowie Interesse und Neugier beherrscht. Auch handelt es sich bei diesem, gegenwärtig die digitale Welt betreffenden Begriff um nichts wirklich Neues. Bereits vor 88 Jahren entwickelte der „Urvater der KI“, Alan Turing die theoretisch-wissenschaftliche Grundstruktur für diese Technik. Weitere Meilensteine der Entwicklung erfolgten in den 1950er- und 1960er-Jahren. Im Sommer 1956 wurde in einem achtwöchigen Workshop die Möglichkeiten der mentalen Fähigkeiten eines Menschen durch Großrechner simuliert.

Im Mittelpunkt dieser Aktivitäten stand der Wissenschaftler John Mc Carthy, der für die Umsetzung dieses Projektes den Begriff „Artificial Intelligence“ oder „künstliche Intelligenz“ prägte. Der Erfolg dieses Seminars war schließlich die Umsetzung des Computerprogramms „Logic Theorist“ mit dem eine große Anzahl mathematischer Lehrsätze hinsichtlich ihrer Richtigkeit geprüft werden konnten. Im wissenschaftlich-historischen Kontext gilt die Anwendung dieses Programms als erstes KI-Programm der Welt. Ein Jahrzehnt später präsentierte der deutsch-US-amerikanische Informatiker Joseph Weizenbaum das erste automatische Dialogsystem, in das er verschiedene imaginäre Gesprächspartner integrierte. Er nannte sein Werk „Eliza“.

1972 wurde mit „MYCIN“ erstmals in der Medizin ein Computerprogramm auf der Grundlage medizinischer Daten und Fakten eingeführt. Durch die Ausarbeitung des neuronalen Netzes „NETalk“ konnte 1986 ein Rechner erstmals in beschränktem Rahmen als „Gesprächspartner“ im Rahmen wissenschaftlicher Forschungen eingesetzt werden. Als weiterer bahnbrechender Erfolg lässt sich der Schachcomputer „Deep Blue“ nennen, der den damaligen Schachweltmeister Garri Kasparov schlug. Zwischen 2011 und 2015 setzten sich Sprachassistenzsysteme wie „Alexa“ von Amazon Echo ebenso wie „Siri“ von Apple und „Cortana“ von Microsoft für Nutzerinnen und Nutzer durch. Die weltweit führenden Hard- und Software-Konzerne konzentrierten sich in der Folge auf die Entwicklung von Programmen, mit denen die Kommunikation optimiert wurde. Beispielsweise besiegte „Watson“ seinen menschlichen Kontrahenten im Zuge einer Quizshow im US-amerikanischen Fernsehen. Auch Rededuelle mit denen vielschichtige Inhalte zwischen künstlicher Intelligenz und menschlichen Gesprächspartnern durchgeführt wurden, wie mit dem „Project-Debater“ von IBM, wurden angewendet. Der Konzern Google sorgte mit seinem KI-basierten Gesprächsprogramm „Duplex“ für Schmunzeln, als dieses mit einer Frau kommunizierte und auf ihren Wunsch hin einen Friseurtermin vereinbarte. Die Technologie erreicht immer mehr Bereiche der Gesellschaft und erregt Bedenken und Kritik.

Foto: Katharina Schiffl

Bei der Veranstaltung „Künstliche Intelligenz: Zwischen Regulatorik und Realität – Exploration der digitalen Zukunft“, die vom Kompetenzzentrum Sicheres Österreich (KSÖ) am 4. Juni 2024 abgehalten wurde, diskutierten Experten über die Chancen und Gefahren dieses Themas. Um die Risiken dieser Technologie in Europa besser kontrollieren zu können, bedarf es gesetzlicher Regelungen, wie der europäischen Verordnung über künstliche Intelligenz (KI), dem EU-Artifical-Intelligence-Act, dessen Anwendungsmöglichkeiten der Referatsleiter künstliche Intelligenz in der Europäischen Kommission Kilian Gross erläuterte.

Der EU-Fachvertreter unterstrich in seinem Referat die Wichtigkeit dieser Technologie in vielen Bereichen der öffentlichen Sicherheit. „Es war von Anfang an ein Leitmotiv im Gesetzgebungsverfahren die Balance hinzubekommen zwischen dem Bedürfnis auf der einen Seite die Polizeiorgane mit modernster Technologie auszustatten und auf der anderen Seite dem Wunsch im digitalen Zeitalter Regeln aufzustellen, die Bürgerrechte ausreichend garantieren“, erklärte Kilian Gross.

Im AI-Act bestehen viele Vorschriften und Sonderregelungen, die die besonderen Bedürfnisse der Sicherheitsorgane berücksichtigen. Am 21. April 2021 wurde der Vorschlag für die erste weltweite Gesetzgebung zur künstlichen Intelligenz ins Leben gerufen. „Wir wollen die künstliche Intelligenz wie ein Produkt behandeln, weil wir glauben, dass wir Produkte sicher machen können“, führt der Referatsleiter weiter aus. Die Regulierungen erfolgen risikobasiert, das heißt, dass nur so weit mit Regeln eingegriffen wird, wo es aus der Sicht der Europäischen Union erforderlich ist für das jeweilige Risikoniveau. Bei der Strukturierung der Verordnung mussten im Zuge der weiteren Entwicklung dieser Technologie weitere Hürden bewertet und bewältigt werden, wie bei der Einführung von ChatGPT im Dezember 2022. Dadurch wurde klar, wie bahnbrechend künstliche Intelligenz sein kann und welche Schlüsse aus dieser Entwicklung ableitbar sind. Es stand auch die Frage im Raum, warum überhaupt eine KI-Verordnung notwendig ist, da es für viele andere Produkte keine gesetzliche Regelung gibt. „Der Grund dafür ist, dass wir glauben, das KI einige Besonderheiten aufweist, die es von anderen Technologien unterscheidet und die es rechtzeitig erforderlich machen, dass KI reguliert wird. Bei KI ist es nicht nachvollziehbar, wie man von einem Ausgangspunkt zu einem Endpunkt kommt“, berichtete der Repräsentant der EU.

Rechtschutz ist ein wichtiges Thema für Personen, die auf Grund von KI-Anwendungen, beispielsweise bei einem Ausschreibungsverfahren für einen Arbeitsplatz benachteiligt werden könnten. Die Ausnahmen bezüglich des Einsatzes von künstlicher Intelligenz betreffen die Bereiche Militär, Verteidigung und nationale Sicherheit. Gerade hier wird bei Produkten unterschieden, die sowohl im zivilen als auch im militärischen Bereich verwendbar sind. Bei der Strafverfolgung ist die Verwendung biometrischer Daten erlaubt, die KI-basiert zusammengestellt werden. Die nachträgliche biometrische Fernidentifizierung ist durch eine Genehmigung der zuständigen Justiz- und Verwaltungsbehörden erforderlich. Die Erstidentifikation anhand

von Videomaterial, beispielsweise von einem Autoeinbruch darf nur fallspezifisch eingesetzt werden. Für weitere Ermittlungen mit Hilfe von Kameraaufzeichnungen einer bestimmten Person, die einer Straftat überführt werden soll, muss eine richterliche Genehmigung eingeholt werden. „Der EU-KI-Act soll für Behörden sowie für Anbieter und Anwender eine Hilfe auf Grundlage der rechtsstaatlichen Sicherheit sein“, brachte es Kilian Gross auf den Punkt. Im Sinne der Sicherheit von Netzwerken und Computersystemen im professionellen sowie im privaten Bereich bestehen Risiken durch die Einwirkung von künstlicher Intelligenz.

Gefahren für den Nutzer sind beispielsweise Pishing-E-Mails, die nicht als Fälschungen erkannt werden und zur Herausgabe sensibler Daten auffordern. Diese Gefahr besteht schon jahrelang, allerdings wird die KI-generierte Qualität und damit die immer schwerere Erkennbarkeit immer mehr zur Gefahr unbedarfter Benützer. Eine aktuelle Art dieser Gefahr sind „Vishing E-Mails“, also Voice-Pishing-E-Mails, die mit einer von KI-geklonten Stimme eines Entscheidungsträgers einer Institution in Erscheinung tritt und für uninformierte Anwender die Gefahr birgt, bestimmten Aufforderungen zu folgen. „Im Prinzip ist das der Enkel-Trick, der mit KI durchgeführt wird“, schildert Clemens Wasner, der Geschäftsführer von Enlite-AI, einem auf die Anwendung von KI spezialisierten Unternehmen aus Wien sowie einem Thinktank mit dem Ziel, Österreich als Vorreiter der Applied AI, also vertrauenswürdiger künstlicher Intelligenz, erfolgreich zu positionieren.

Angst. Die Herausforderungen von KI lösen in der Bevölkerung auch Angst aus. „Eine Umfrage der Zeitung „Die Zeit Online“ fand heraus, dass über 50 Prozent der Deutschen Angst vor künstlicher Intelligenz haben“, berichtete die Juristin Carina Zehetmaier, Präsidentin von Women in AI Austria. Entsprechend dieser Umfrage glauben 58 Prozent der Befragten, dass KI eine Gefahr für die Menschheit werden könne. Menschen sind in der Regel nicht neutral und nicht objektiv, treffen aber nach Darstellung der Vortragenden noch die besseren Einzelfallentscheidungen. Ziel ist, das ideale Zusammenspiel zwischen Maschine und Mensch zu erreichen. Die künstliche Intelligenz sollte das tun, was sie gut kann, nämlich Daten durchforsten und Verwertbares auf Grundlage einer bestimmten Aufgabenstellung präsentieren. „Wir dürfen nicht vergessen, welche Herausforderungen wir heute schon mit der Technologie haben“, sagte die Juristin. Die menschliche Kontrolle über die künstlichen Intelligenz birgt die Kernforderung des EU-KI-Acts.

Sylvia Mayer: „Mit KI kann man bald viel effizienter Schwachstellen in einer Firewall scannen und in das System eindringen.“

Kilian Gross: „Wir wollen die künstliche Intelligenz wie ein Produkt behandeln, weil wir glauben, dass wir Produkte sicher machen können.“

Die Manipulationsmöglichkeiten von Bildern, Videos und Texten durch KI-generierte Programme sind vielfältig. Beispielsweise wurde auch bei der indischen Präsidentenwahl 2024 KI eingesetzt. „Angeblich haben alle indischen Parteien, die zur Wahl angetreten sind, KI genützt, auch die Partei des gewählten Präsidenten Modi, berichtete Carina Zehetmaier. Das indische Staatsoberhaupt konnte mit allen Bevölkerungsgruppen kommunizieren, auch mit jenen, die er sonst nicht erreicht hätte.

Künstliche Intelligenz kann die öffentliche Meinungsbildung beeinflussen und damit die Demokratie gefährden. Daher müssen bessere Kontrollmechanismen auf technischer und rechtlicher Ebene über den EU-KI-Act hinaus geschaffen werden, um die Menschen vor den vielfältigen Gefahren zu schützen. Große Technologiekonzerne, die nicht in Europa beheimatet sind, sondern in China und den USA, beeinflussen das Realitätsbewusstsein der Bürgerinnen und Bürger.

„KI wird schon seit vielen Jahren entwickelt. Ich erinnere mich zu meiner Zeit in der IT-HTL vor 20 Jahren haben wir die Anfänge dieser Technologie bereits kennengelernt“, sagte Sylvia Mayer, die stellvertretende Direktorin der DSN in der Paneldiskussion der Veranstaltung. Gefakte Videos und Bilder sind größtenteils noch erkennbar. In einigen Jahren wird dies nicht mehr der Fall sein. Bei Videokonferenzen erkennt man heute, ob es sich um Personen, oder von KI generierte Darstellungen handelt. Auch das wird sich in absehbarer Zeit ändern. „Wir können uns noch gar nicht vorstellen, was diese Technologie in 3 oder in 5 Jahren bewerkstelligen kann“, betonte Sylvia Mayer.

Künstliche Intelligenz wird Cyber-Angriffe verstärken. Mit KI kann man bald viel effizienter Schwachstellen in einer Firewall scannen und in das System eindringen. Dennoch wird sich die Entwicklung der KI durch nichts aufhalten lassen. Sie wird zunehmend unseren Alltag beherrschen.

„Der Computer lernt zu ‚sehen‘, zu ‚hören‘ und Entscheidungen zu treffen“, erklärte Wolfgang Baumgartner, General Manager des Unternehmens SecConsult, das sich auf Cyber- und Applikationssicherheit spezialisiert hat. Europäische Konzerne müssen sich in diesem Technologiebereich vor allem im Hinblick auf die Erarbeitung von Sicherheitsstrukturen bei der vielseitigen Nutzung von künstlicher Intelligenz etablieren. *Michael Ellenbogen*

Fotos: Katharina Schiffl