„Deep Learning“

Wie maschinelles Lernen die Welt verändert

CHRISTOPH MEINEL
Geboren 1954 in Meißen, Institutsdirektor und Geschäftsführer des Hasso-Plattner-Instituts, Potsdam, Dekan der Digital Engineering-Fakultät der Universität Potsdam.

Seit einigen Jahren erlebt das Thema Künstliche Intelligenz (KI) eine Renaissance. Neue Big Data-Technologien, leistungsfähige Verfahren maschinellen Lernens und Hardware einer Leistungsklasse, auf der diese Technologien und Verfahren in Sekundenschnelle ausgeführt werden können, haben der menschlichen Sehnsucht nach künstlicher Nachbildung menschlicher Intelligenz neue Nahrung gegeben. Sie versprechen ein großes Innovationspotenzial für neue Dienstleistungen und Produkte in allen gesellschaftlichen Bereichen.

Mit der Entwicklung der ersten Computer Mitte des letzten Jahrhunderts erhielt das Nachdenken über Künstliche Intelligenz eine erste breite gesellschaftliche Relevanz, beflügelt durch die Phantasie von Science-Fiction-Autoren. In den 1960er- bis 1980er-Jahren kam es zu einem zweiten KI-Hype.

Die Computer wurden leistungsfähiger, und so nahm der Gedanke Gestalt an, Maschinen mit den Fähigkeiten Künstlicher Intelligenz auszustatten: Da das menschliche Handeln regelbasiert sei, glaubte man, bei entsprechender Programmierung seien Computer in der Lage, so wie wir zu „denken" und zu „handeln".

Einem anderen Ansatz folgend, entwickelte sich seit Mitte der 2010er-Jahre der dritte weltweite KI-Hype. Mithilfe neuer Rechner mit ungekannter Rechenleistung und auf Basis von inzwischen massenhaft verfügbaren elektronischen Daten aus allen Bereichen unseres Lebens konnten musterbasierte Lernverfahren *(Deep Learning)* entwickelt werden, die Computer befähigen, selbst zu lernen und so entscheidende Fortschritte in der Bereitstellung von Künstlicher Intelligenz erzielen.

Was genau hat sich damit verändert im Vergleich zur regelbasierten KI, und warum haben diese Veränderungen das Potenzial, unsere Zivilisation global in einem Maße zu verändern, wie es bisher nicht und auch heute nur in vagen Umrissen vorstellbar ist? Die wichtigste Neuerung in der KI-Forschung war die Abkehr vom gängigen KI-Paradigma, dass intelligente Maschinen deshalb über menschenähnliche Intelligenz verfügen, weil menschliche Denkmuster einprogrammiert werden, also sämtliche „Denkschritte" in mühsamer Programmierarbeit im Detail vorbestimmt werden. Neue Ansätze, mit denen Maschinen in die Lage versetzt werden, basierend auf statistischen Verfahren zu lernen, haben sich als erfolgreicher erwiesen. Die neuen Verfahren, die allgemein als *Machine Learning,* genauer als *Deep Learning* bezeichnet werden, durchdringen eigenständig die ihnen gestellte Aufgabe mittels einiger weniger Lernregeln und sind fähig, semantische Muster in den verschiedensten Szenarien zu erkennen.

TRAINING FÜR NEURONALE NETZE

Zwar wurden die technischen Grundlagen für das *Deep Learning,* sogenannte neuronale Netze, bereits in den 1950er-Jahren gelegt; es fehlten jedoch bis vor wenigen Jahren wichtige technische Voraussetzungen, um dem Konzept zum Durchbruch zu verhelfen. Zum einen wurden erst leistungsfähige Grafikprozessoren (*Graphic Processing Units,* GPUs) entwickelt, die in der Lage sind, neuronale Netze in der gebotenen Geschwindigkeit so zu trainieren, dass sie ähnlich der Arbeitsweise des Gehirns aus einzelnen Signalen, zum Beispiel aus den Pixeln eines Bildes, immer umfassendere semantische Strukturen „erkennen" können, im Falles des Bildes einzelne Kanten, dann geometrische Gebilde bis hin zu Gesichtern bestimmter Personen.

Zum anderen stehen uns erst mit dem Aufkommen von Big Data die notwendigen Ressourcen zum Training der maschinellen Lernverfahren zur Verfügung. Spätestens, seitdem Smartphones zum Massenphänomen wurden

und praktisch jeder über diverse Applikationen zum Massendatenlieferant auf einschlägigen digitalen Plattformen wurde, steht die Ressource „Daten“ in ausreichender Menge zur Verfügung, neuronale Netze zu trainieren. Dabei werden Hunderttausende einfache Berechnungselemente zu Berechnungsarchitekturen zusammengeschaltet. Die anfangs aufgenommenen Eingabewerte, etwa die Pixelwerte eines Bildes, werden an die benachbarten Berechnungselemente weitergeleitet und dort mit den Daten der anderen Nachbarn und den eigenen verrechnet. Bei der Weiterleitung können die berechneten Werte verstärkt oder abgeschwächt werden. Das Netzwerk wird dann mit immer neuen Eingaben mit dem Ziel trainiert, dass sich an jeder der Hunderttausenden Verbindungsleitungen zwischen zwei Berechnungselementen der jeweils „richtige“ Verstärkungs- beziehungsweise Abschwächungswert einstellt.

Besonders interessant und in einem gewissen Maße auch beunruhigend ist dabei die Tatsache, dass *Machine Learning*-Verfahren zunächst keine Rückschlüsse darauf zulassen, wie die Maschine zu ihrem Ergebnis kommt, und dass sie, wie in statistischen Verfahren üblich, nicht mehr absolut wahre Ergebnisse ausgibt, sondern eben nur wahrscheinliche. Das bedeutet, dass es bei jedem *Machine Learning*-Verfahren zu einer gewissen Fehlermenge kommt.

DATENGETRIEBENE GESELLSCHAFT

Mit der weltweiten Vernetzung von Menschen und Maschinen ist eine neue Dimension der Globalisierung erreicht. Damit gehen neue Herausforderungen für die Menschheit als Ganzes einher. Diese reichen von der Klimadebatte über die Koordinierung globaler Migrationsströme bis hin zur Versorgung einer weiterwachsenden Weltbevölkerung. Ohne die Nutzung der Digitaltechnologie und intelligenter KI-Verfahren wird sich die rasant steigende Komplexität unserer Welt nicht beherrschen lassen.

Unmittelbarer Ausdruck dieser steigenden Komplexität ist die explodierende Menge elektronischer Daten, die die verschiedenen Phänomene unserer Welt beschreiben. Wir bekommen von immer mehr Details Kenntnis, die unser Denken, Handeln und Entscheiden beeinflussen. Schon heute sind alle Bereiche unserer Gesellschaft datengetrieben, und das wird sich verstärken. Allein auf YouTube werden pro Minute 400 Stunden an Videomaterial hochgeladen. Über 35 Milliarden IoT-Geräte, also Technologien zum Betrieb und zur Nutzung des Internets der Dinge (*Internet of Things,* IoT), produzieren jede Sekunde Massen an Produktions-, Bewegungs- und Zustandsdaten. Das Gleiche gilt für die weltweit zweieinhalb Milliarden Smartphone-Nutzer. Der medizinische Scan eines einzigen menschlichen Organs liefert jede Sekunde zehn Gigabyte an Daten. Es werden jedoch auch jeden Tag fast 400.000 neue Schadprogramme in die Welt gesetzt. Um aus dieser Datenmenge überhaupt

sinnvolle Informationen gewinnen zu können, sind maschinelle Unterstützung und automatisierte Verfahren notwendig: je intelligenter, umso besser.

Bis heute sind die Grenzen der neuen Technologie kaum zu ermessen und bieten Anlass zu gesellschaftlichen Debatten. Dabei sollten wir mit größerer Neugier und kritischer Distanz sowohl Potenziale und Leistungskraft als auch die Risiken der neuen KI-Werkzeuge erkunden. Sicher werden sie, ob in der industriellen Produktion, bei digitalen Dienstleistungen oder in den Bereichen der Kommunikation und *Governance,* weitreichende Vorteile und ein Feuerwerk an Innovationen bieten und helfen, in vielen Bereichen gesellschaftliche Probleme zu lösen.

„HATE SPEECH“ IN SOCIAL MEDIA

Zwei Milliarden Menschen nutzen Social Media-Plattformen, um sich über Geschehnisse in der Welt zu informieren, sich mit ihren Freunden und Geschäftspartnern auszutauschen, Werbung zu schalten und für politische Positionen zu streiten. Diese Plattformen im Cyberraum schaffen eine weltumspannende Öffentlichkeit und entwickeln eine bisher unvorstellbare Dynamik. Die Auswirkungen auf Gesellschaft und Individuum sind nicht hinreichend erforscht, geben aber Anlass zu Besorgnis. Phänomene der Online-Kommunikation in Sozialen Medien wie Fake News, Filterblasen und Hassreden verändern den politischen Diskurs.

Eine Ursache liegt in der hergebrachten Kultur der politischen Diskussion, bei der Informationen zunächst gründlich geprüft und abgestimmt werden. Neue politische Akteure scheren sich nicht um solche Prozesse und haben dadurch einen strukturellen Vorteil. Auch Anonymität führt zum Verlust des Anstands und lässt das bisher geübte Niveau des gesellschaftlichen Diskurses erodieren. Beleidigungen und *Hate Speech* bis hin zu Morddrohungen sind an der Tagesordnung. Man kann natürlich appellieren, dass sich jeder an die tradierten Anstandsregeln halten möge. Vor dem Hintergrund der niedrigschwelligen Möglichkeiten, im Netz und in den sozialen Medien spontan und ungefiltert Informationen zu verbreiten, scheint das jedoch naiv und aussichtslos. Weltweit existieren über 1,3 Milliarden Webseiten, täglich kommen etwa 150.000 neue dazu. Auf Twitter werden jeden Tag 700 Millionen Nachrichten versendet, 1,3 Milliarden Facebook-Nutzer teilen stündlich 180 Millionen Inhalte.

Der Schlüssel zur Lösung dieses Problem liegt einerseits in verstärkter digitaler Bildung, andererseits in der beherzten Nutzung von KI-Technologien, um die Massen an täglich produzierten Daten automatisiert zu durchforsten und die gröbsten Verstöße gegen persönliche Rechte aufzuspüren. Die Zukunft digitaler partizipatorischer Prozesse wird sich daran entscheiden, ob es den digitalen Plattformen und sozialen Medien gelingt, in enger Zusammenarbeit

mit den Stakeholdern in Politik und Gesellschaft diese Auswüchse mit geeigneten Mitteln und Regularien zu verhindern und geeignete Kontrollinstanzen zu installieren. Ohne den Einsatz von KI-Techniken wird es nicht möglich sein, von den neuen, innovativen Kommunikationskanälen wirklich zu profitieren. Gewiss sind bisherige Filtertechniken nicht perfekt, aber ein wichtiger Baustein, um den globalen politischen Diskurs zu zivilisieren und die mit dem Internet entstandene Vision einer produktiven demokratischen globalen Öffentlichkeit Wirklichkeit werden zu lassen.

„DIGITAL HEALTH“ UND INDUSTRIE 4.0

Eine weitere Herausforderung besteht darin, der wachsenden und älter werdenden Weltbevölkerung die bestmögliche Gesundheitsversorgung zu bieten. Derzeit ist unser Gesundheitssystem unangemessen teuer. Im Mittelpunkt steht die Behandlung von Krankheiten, anstatt den Schwerpunkt auf die Vorsorge und Vermeidung von Krankheiten zu legen. Auch sind Verfahren und Diagnosen im Gesundheitssystem viel zu wenig personalisiert. Der Einsatz intelligenter Systeme wird individualisierte und dadurch viel wirkungsvollere Therapien ermöglichen und helfen, Medikamente zielgenauer und ohne Nebenwirkungen einzusetzen. Die exzessive und gefährliche Nutzung von Antibiotika kann eingeschränkt, die Medikamentendosis dem individuellen Stoffwechsel angepasst und vorausschauend diagnostiziert werden.

Mit neuronalen Netzwerken ist es bereits heute möglich, Krebserkrankungen frühzeitig zu erkennen und die Hautkrebsvorsorge zu verbessern. Anhand von Hautpigmentaufnahmen können intelligente Bildanalyseverfahren für den Arzt unsichtbare Indikatoren für bösartige Tumore erkennen. Ausreichend trainierte Systeme erlauben, die Belastung bildgebender Diagnoseverfahren (Bestrahlung) zu reduzieren, indem aus Magnetresonanztomographie-(MRT)-Aufnahmen automatisch präzise Röntgenaufnahmen generiert werden. Auch Herz-Kreislauf-Krankheiten werden mithilfe von *Smartwatches* oder *Wearables,* die beständig die Herzfrequenz messen, zuverlässiger behandelt werden können.

Die deutsche Industrie kann von KI-basierten Entwicklungen in der Automatisierungstechnik profitieren. Das Internet der Dinge, also die Vernetzung der Maschinen, verspricht neue Produktionsweisen, die nicht nur effizienter und preiswerter ablaufen, weil Prozesse haargenau ineinandergreifen können, sondern auch personalisierte Produkte in direkter Interaktion mit ihren Kunden „on demand“ anbieten können. Der Einsatz menschlicher Arbeit kann anhand von Kompetenzprofilen besser geplant werden und zu Produktionssteigerung und höherer Jobzufriedenheit führen. Wer die digitalen Plattformen für die IoT-Welt entwickelt, die global zum Standard werden, wird in der Industrieproduktion der Zukunft den Ton angeben.

Alle diese Innovationen sind nichts ohne Sicherheit. Der Erfolg digitaler Dienste und Produkte wird wesentlich davon abhängen, ob sie vertrauenswürdig mit persönlichen Daten umgehen und sicher und verlässlich funktionieren. Daher ist die Entwicklung von immer leistungsfähigeren Verfahren zur Garantie von Cybersicherheit die Grundlage für nachhaltigen wirtschaftlichen Erfolg. Mit zunehmender Vernetzung von Menschen und Maschinen über das Internet wird es schwieriger, den Überblick über Schwachstellen und Schadsoftware zu behalten. Nicht nur, dass Cyberkriminalität immer lukrativer wird, weil digitale Systeme bei der Wertschöpfung eine immer größere Rolle spielen: Auch kommt es mit jedem weiteren Nutzer und zusätzlich angeschlossenen Gerät mit seinen Schwachstellen zu neuen Möglichkeiten des Angriffs auf das Gesamtsystem. Die Cybersicherheit eines Systems entscheidet sich am schwächsten Glied. Es ist daher von grundlegender Bedeutung, einen hohen Cybersicherheitsstandard zu erreichen.

NEUARTIGE ANGRIFFSMUSTER

Auch hier, bei der Analyse von Netzwerken und der Bewertung von Cybersicherheitsarchitekturen, werden intelligente KI-Verfahren eine große Rolle spielen. Ohne diese wird es zum Beispiel nicht möglich sein, unbekannte Angriffsvektoren zu identifizieren. Gängige Antivirensoftware kann hier nicht weiterhelfen; sie basiert auf hergebrachten regelbasierten Verfahren und kann nur bereits bekannte Schadsoftware herausfiltern. Notwendig sind selbstlernende KI-Systeme, die anhand ständiger Musterbeobachtung Anomalien erkennen können, die von potenziell schädlichen Programmen herrühren. Das Gleiche gilt im Bereich des Cloud-Computings. Immer mehr Unternehmen speichern ihre Daten in der Cloud und verfügen über hochkomplexe Firmennetzwerke, die täglich über zwei Milliarden Events mit einem Datenfluss von über vier Terabyte verwalten. Ausschließlich mit Techniken des maschinellen Lernens können neuartige Angriffsmuster erkannt und unschädlich gemacht werden. Techniken des intelligenten maschinellen Lernens werden in allen gesellschaftlichen und ökonomischen Bereichen immer wichtiger und haben ein sehr großes Innovationspotenzial. Wer diese Techniken vor anderen beherrscht, verfügt über einen Vorsprung, der sich direkt in Wertschöpfung und Wohlstand ummünzen lässt. Daher ist es so wichtig, dass sich Deutschland und Europa im globalen Wettbewerb nicht durch theoretische Diskussionen abhängen lassen, sondern beherzt ihre Forschungsstärke ausspielen und in neue Produkte wandeln.

Wir brauchen einen evidenzbasierten und pragmatischen Umgang mit den neuen Techniken des maschinellen Lernens. Es wird nichts helfen, sich in theoretischen Diskursen über das Für und Wider der Anwendung von Künstlicher Intelligenz zu verlieren – stattdessen muss rigoros empirisch geprüft werden, inwiefern sie in der Lage sind, gesellschaftliche Probleme zu lösen.