HANDBUCH
KÜNSTLICHE INTELLIGENZ

Erfolgsfaktor KI

Smarte Technologien für die Wirtschaft

TREND REPORT
www.handbuch-ki.net

KI bei Datenschutz und Compliance

Im Risikomanagement die Stärken von KI nutzen

von Frank Romeike

Die „künstliche Intelligenz" zählt zu den Top-Themen der digitalen Wirtschaft. Und ein Blick auf die kontroversen Diskussionen zeigt, dass das Thema voller Emotionen, Ängste und vor allem Halbwissen und Hoffnungen steckt. Viele der heute diskutierten Ängste resultieren primär aus Unwissenheit oder Halbwissen. Nur wenige „Experten" haben tatsächlich schon einmal in die Werkzeugkiste der „künstlichen Intelligenz" hineingeschaut oder gar Methoden angewendet.

Diese Irrungen beginnen bereits beim Begriff „künstliche Intelligenz". Der englische Begriff „Artificial Intelligence" (AI) wird nur allzu häufig mit „künstlicher Intelligenz" übersetzt und suggeriert somit eine Konkurrenz zur menschlichen Intelligenz, beispielsweise in Form eines Homunculus oder Cyborg.

Dabei bedeutet „Intelligence" vor allem Informationsverarbeitung und Aufklärung. Die „Central Intelligence Agency" (CIA) heißt ja auch nicht so, weil die so gescheit sind, sagt der österreichische Artificial-Intelligence-Experte und emeritierter Universitätsprofessor Robert Trappl. AI beschäftigt sich im Kern mit der Nachbildung menschenähnlicher Entscheidungsstrukturen durch Algorithmen, nicht mehr und nicht weniger. Das heißt, ein Computer wird so programmiert, dass er eigenständig Probleme bearbeiten kann, beispielsweise Auto fahren, Texte übersetzen oder Go spielen.

Ein Blick in die Vergangenheit zeigt, dass Technologien sich immer dann durchgesetzt haben, wenn die Risiken und Chancen transparent gemacht wurden. So warnte Dionysus Larder (1793 bis 1859), Professor für Naturphilosophie und Anatomie am University College London, eindringlich vor Bahnreisen mit Hochgeschwindigkeit. Die Passagiere könnten nicht atmen und würden somit den Erstickungstod erleiden, so seine eindringliche Warnung. Professor Michael Sedlmair von der Universität Stuttgart umschrieb es jüngst in einem Interview wie folgt: „Die Angst vor der Entmenschlichung ist geschichtlich gesehen nichts Neues." Und er fügt das Beispiel von Fahrstühlen an: „Bei der Einführung von Fahrstühlen gab es beispielsweise immer noch Fahrstuhlbegleiter, die die Passagiere begleitet haben. Diese Begleitung wurde irgendwann

> *Nicht künstliche Intelligenz ist die größte Gefahr, sondern natürliche Dummheit.*
>
> *- Historiker Yuval Noah Harari*

hinfällig, doch viele Leute hatten zunächst Angst, ‚alleine' mit dem Aufzug zu fahren. Heute ist das hingegen selbstverständlich. Ähnliches passiert nun auch mit KI."

Somit zeigt sich: Warner gab und gibt es bei jeder neuen Technologie. So haben jüngst der Physiker Stephen Hawking, der Philosoph Nick Bostrom und der Unternehmer Elon Musk auf die negativen Seiten von AI hingewiesen. „Biologisches Wissen multipliziert mit Rechenleistung multipliziert mit Daten ergibt die Fähigkeit, den Menschen zu hacken", sagte erst jüngst der israelische Autor Yuval Noah Harari. Doch keiner von ihnen hat sich jemals wissenschaftlich oder praktisch mit der Entwicklung von AI-Systemen beschäftigt.

AI ist gleichzeitig Fluch und Segen

„Artificial Intelligence" befasst sich allgemein mit der Automatisierung intelligenten Verhaltens und mit maschinellem Lernen. Häufig wird auch zwischen starker und schwacher KI (Weak vs. Strong AI) unterschieden. Hierbei umfasst „starke KI" IT-Systeme, die in der Lage sind, menschenähnlich (oder überlegen) zu denken und zu handeln, und zwar vernetzt in vielen, unterschiedlichen Bereichen. Fängt ein solches „superintelligentes" System an, sich fortlaufend selbst zu verbessern, dann ist der Zustand der Singularität erreicht, wo maschinelle Intelligenz der menschlichen Intelligenz überlegen ist (siehe Homunculus). Demgegenüber befasst sich die „schwache KI" mit konkreten Anwendungsproblemen des menschlichen Denkens, beispielsweise Bilderkennung, autonomem Fahren, Spracherkennung und -übersetzung, Unterstützung bei juristischen oder medizinischen Diagnosen. Alles was wir heute in der Realität sehen, sind Entwicklungen im Bereich der „schwachen KI".

Eine trennscharfe Unterscheidung von starker und schwacher KI und deren Chancen und Risiken ist für eine Objektivierung der Diskussion von höchster Relevanz. Zwischen einer bösartigen Nutzung künstlicher Intelligenz und einer sinnvollen AI-Unterstützung im täglichen Leben besteht ein riesiger Unterschied. Sowohl der „übermenschliche Cyborg" als auch die intelligente Einparkhilfe und die Diagnose von Krankheiten basieren auf Methoden aus der Werkzeugkiste „Artificial Intelligence".

In Datenschutz und Compliance die Stärken von AI nutzen

So kann AI uns dabei helfen, Risiken schneller und exakter zu erkennen und aus „schwachen Signalen" Frühwarninformationen abzuleiten, um uns beispielsweise auf potenzielle Compliancerisiken, geopolitische Konflikte oder Cyberattacken hinzuweisen. Die maschinelle Intelligenz kann unseren menschlichen Intellekt sinnvoll ergänzen. Bei der Auswer-

Verwandte Themen

- Was ist KI? S.17
- Vor der künstlichen ist erst die menschliche Intelligenz gefragt S.62
- Die Intelligenz in der Maschine S.119
- KI im Rechtswesen S.196
- KI und IT-Security S.223

tung großer Datenströme in Echtzeit liefert AI eine wertvolle Entscheidungsunterstützung. Die AI-Methoden können uns dabei helfen, in vernetzten und komplexen Systemen die Gesamtheit aller verfügbaren Informationen zu analysieren und uns mit wertvollen neunen Impulsen zu versorgen. Einen exzellenten Beweis lieferte hier der Sieg von AlphaGo Zero über die weltbesten Go-Spieler. Der AlphaGo-Algorithmus generierte höchst intelligente Spielzüge und unkonventionelle Strategien, was den menschlichen Go-Spielern neue Ideen für die Optimierung der eigenen Strategie lieferte. Diese waren dem menschlichen Gehirn in der 3000-jährigen Geschichte des Spiels bisher noch nicht in den Sinn gekommen.

So sollten im Risiko-, Compliancemanagement und im Bereich der Informationssicherheit die Methoden und Lösungen um Machine Learning und andere Methoden erweitert werden, um schwache Signale, Chancen und Risiken sowie Frühwarninformationen besser zu antizipieren. So können bereits heute Chatbots Security-Analysten bei der Suche nach neuen Angriffswegen und -methoden unterstützen. AI-Lösungen analysieren rund um die Uhr automatisch IT-Systeme und liefern in Echtzeit Verhaltensmuster und lernen dabei. So kann uns Deep Learning beispielsweise dabei unterstützen, bisher unbekannte Malware und Cyberangriffe zu identifizieren und abzuwehren. Maschinelles Lernen kann potenzielle Geldwäscherisiken identifizieren oder Verdachtsfälle für Terrorismusfinanzierung, Steuerbetrug oder weitere strafbare Handlungen erkennen. Ziel ist es, neues Wissen aus Daten herauszulesen, das vorher für Experten nicht ersichtlich war.

Auf der anderen Seite sollten wir die Augen offen halten, da AI-Systeme selbstlernend sind und damit auch „eigene Wege" gehen können. Auch Hacker nutzen verstärkt AI-Methoden für Cyberangriffe. Terroristen und Despoten könnten autonome Waffen nutzen und sogar hacken. Wir müssen uns bewusst werden, dass AI und deren Werkzeuge in die Hände einer Vielzahl von Akteuren geraten, die höchst unterschiedliche Interessen verfolgen. Und das gilt auch im Umgang mit der inneren Sicherheit und dem Thema Überwachung in „demokratischen" Staaten.

Gute AI, böse AI: Wo wollen wir hin?

Wichtig ist, dass AI mit unseren gesellschaftlich definierten Zielen übereinstimmt. Auf diesen Umstand hatten vor einiger Zeit Wissenschaftler u. a. der Universitäten Stanford, Yale, Oxford und Tohoku sowie Entwickler von Microsoft und Google hingewiesen. In der Studie „The Malicious Use of Artificial Intelligence" werden verschiedene Szenarien skizziert, wie AI-Technologien von Terroris-

ten, Kriminellen und despotischen Regierungen missbraucht werden könnten und wir uns dagegen schützen können.

AI-Algorithmen sollten dort zum Einsatz kommen, wo ihre Fähigkeiten besser als die der Menschen sind und umgekehrt. Wir müssen uns als Menschen und Gesellschaft mit der Frage beschäftigen, wie viel (vermeintliche) Sicherheit und Vorhersehbarkeit auf der einen Seite sowie Freiheit und Risiko auf der anderen Seite gewünscht ist. Eine wichtige Kernfrage in diesem Zusammenhang: Wollen wir uns einer Diktatur der Daten ausliefern und in einer Welt leben, in der Big Data mehr über unsere Risiken, unsere Vergangenheit, Gegenwart und Zukunft weiß, als wir uns selbst erinnern können? Diese Schattenseiten von Big Data und AI sollten zu transparenten und verbindlichen Regeln und einer breiten Diskussion über die Chancen und Grenzen der neuen schönen Datenwelt führen. Um diese Chancen und Risiken fundiert und objektiv zu bewerten, sollten wir uns fundiert mit den Möglichkeiten, Grenzen und Methoden der AI-Welt beschäftigen.

Hierzu gehört auch das Thema Datenschutz, da die Rechtsunsicherheit infolge der DSGVO hoch ist, denn die Rechtsvorgaben folgen in Teilen einer anderen Logik als der der AI-Welt. Datenschutzvorgaben können so zu einem Hemmschuh bei der Entwicklung und Anwendung innovativer AI-Methoden in einzelnen Märkten führen. Stellt sich die Frage nach einem gewünschten Gleichgewicht zwischen Datenschutz und Innovationsfähigkeit. //

Über Frank Romeike

Frank Romeike ist geschäftsführender Gesellschafter des führenden Kompetenznetzwerks zum Thema Risk Management, der RiskNET GmbH – The Risk Management Network. Vor der Gründung von RiskNET war er viele Jahre Chief Risk Officer der IBM Central Europe und hat in einem weltweiten Team das Opportunity & Risk Management der IBM mit aufgebaut. Seit mehr als 25 Jahren beschäftigt er sich mit Simulationsverfahren und Methoden im Bereich AI, insbesondere Deep Learning. Er hat Lehraufträge an diversen Hochschulen und Universitäten zum Thema Stochastik und „Quantitative Methoden im Risk Management" angenommen.

@ *www.handbuch-ki.net.de/autoren/f-romeike*