## ARTIFICIAL INTELLIGENCE

# Intelligenz zu erzeugen ist harte Arbeit

## Creating intelligence is hard work

Bild/Image: istock.com/monsitj

**Technologievisionäre prognostizieren seit Jahrzehnten eine vollautomatisierte Zukunft. Der Computerwissenschaftler John McCarthy, der wesentlich an der Entwicklung der Disziplin der Artificial Intelligence (AI) beteiligt war, erklärte aber schon 1956: Die Schwierigkeit und Herausforderung liegt darin, „eine Maschine zu erschaffen, die sich so verhält, dass man dies intelligent nennen würde, wenn ein Mensch sich so verhielte“.**

AI ist heute in aller Munde, ein Hype-Begriff. Realistisch betrachtet, ist die Nachbildung der menschlichen Intelligenz aber bis heute nicht einfach. Der Trend steckt doch noch in den Kinderschuhen. In einer aktuellen Befragung von RadarServices sehen das 70% der IT-Sicherheitsspezialisten so. Es wird jedoch viel geforscht und erprobt. Laut einer Analyse von Research and Markets aus dem Jahr 2018 sollen sich die Investitionen bis 2025 auf geschätzte 191 Milliarden US Dollar belaufen. Daher haben auch die befragten Experten in der RadarServices-Studie hohe Erwartungen an die kommenden Jahre: 67% von ihnen sehen bis 2020 gute oder sogar sehr gute Fortschritte beim Einsatz von AI / Machine Learning im Bereich IT-Sicherheit. Für 2025 sind sogar 89% der Experten von einer großen Einsatzfähigkeit überzeugt.

Der dringende Bedarf an intelligenten Maschinen für den Cybersecurity-Einsatz ist nachvollziehbar: Einerseits besteht ein großer Expertenmangel und andererseits explodieren Cyberangriffe aufgrund der steigenden Zahl der mit dem Internet verbundenen Geräte. AI soll helfen, Detection & Response zu automatisieren und effizienter im Vergleich zu anderer softwarebasierter Unterstützung zu machen.

Heute sind wir noch nicht an diesem Ziel angelangt. „Supervised learning / überwachtes Lernen“ nennt sich der aktuelle Status quo der auf dem Cybersecurity-Markt angebotenen AI. Ein Lernalgorithmus versucht also, eine Hypothese zu finden, die möglichst zielsichere Voraussagen trifft. Die Hypothese ist eine Abbildung, die jedem Eingabewert den vermuteten Ausgabewert zuordnet, zum Beispiel ob ein Code Malware enthält oder nicht. Dazu braucht der Algorithmus viele Datensätze, von denen er die gewünschten „Gesetzmäßigkeiten“ lernt und an anderen Daten wiederum anwenden kann. Die zentrale Voraussetzung für diese Art der Intelligenz: Das Set an Beispieldaten ist gut. Einerseits müssen malwarefreie Daten auch tatsächlich „sauber“ sein, ansonsten übersieht AI abnormale Datenpunkte. Andererseits muss sichergestellt sein, dass Cyberangreifer keinen Zugriff auf die „Trainingsdaten“ erhalten können, da sie malware- und malwarefreien Code miteinander vertauschen und so das System überlisten könnten.

In der IT-Entwicklung ist „Machine learning“ der nächste Schritt, um „künstlich“ Wissen aus Erfahrung zu generieren: Ein künstliches System lernt aus Beispielen und kann diese nach Beendigung der Lernphase verallgemeinern. Es werden nicht einfach die Beispiele auswendig gelernt, sondern das System „erkennt“ Muster und Gesetzmäßigkeiten in den Lerndaten. So kann das System durch Lerntransfer auch unbekannte Daten beurteilen oder aber durch Überanpassung am Lernen unbekannter Daten scheitern. Erste Erfolge gibt es, zum Beispiel in einem der größten Kompetenzzentren für Forschung zur automatisierten IT-Risikoerkennung: Das Team im Hause RadarServices bringt sie direkt in die Praxis bei seinen Kunden ein. Allerdings bleiben die Experten auch realistisch: „Wir bleiben lieber auf der sicheren Seite und testen unsere Algorithmen über einen längeren Zeitraum, bevor wir sie als das einzige Analyseinstrument – ohne Experteneinbeziehung – einsetzen“ so Christian Polster, verantwortlich für Research und Technologieentwicklung bei RadarServices.

Der Computerwissenschaftler Donald Knuth fasste den Status quo generell so zusammen: „AI schafft all das, wofür Denkleistung notwendig ist, scheitert aber daran das zu tun, was Menschen und Tiere automatisch ohne Denken schaffen.“

**Technology visionaries have been forecasting a fully automated future for decades. However, computer scientist John McCarthy, who was significantly involved in the development of the discipline of artificial intelligence (AI), explained the following as early as 1956: the difficulty and challenge lies in “creating a machine that behaves in such a way that one would call it intelligent if a human being behaved in such a way”.**

AI is on everyone’s lips today. A real buzzword. Realistically speaking, however, recreating human intelligence remains a difficult undertaking today. The trend is still in its infancy. This is the belief held by 70 percent of IT security specialists, according to a recent survey by RadarServices. However, there is a lot of research and testing going on. According to an analysis by Research and Markets from 2018, the level of investment here is expected to reach an estimated USD 191 billion by 2025. This is why the experts surveyed in the RadarServices study have high expectations for the coming years: 67 percent of them see good or even very good progress in the use of AI/machine learning in the field of IT security by 2020. Indeed, 89 percent of experts believe that it will be possible to use it for a wide range of applications in 2025.

The urgent need for intelligent machines to be used for cybersecurity purposes is understandable: on the one hand, there is a significant lack of experts and, on the other, the number of cyber attacks is rocketing with the increasing number of devices connected to the internet. AI is intended to help automate detection & response and make it more efficient compared to other software-based support.

We have not yet reached this goal. “Supervised learning” is the term currently used for the AI offered on the cybersecurity market. This means that a learning algorithm tries to find a hypothesis that makes predictions that are as accurate as possible. The hypothesis is an image that assigns the assumed output value to each input value, for example whether a code contains malware or not. To do this, the algorithm needs many data sets from which it learns the desired “laws” and can then apply them to other data. The core prerequisite for this type of intelligence: the set of sample data is good. On the one hand, malware-free data must indeed be “clean”, otherwise AI doesn’t see abnormal data points. On the other hand, care must be taken to ensure that cyber attackers cannot gain access to the “training data”, since they could switch malware and malware-free code, thereby outwitting the system.

In IT development, machine learning is the next step in generating “artificial” knowledge from experience: an artificial system learns from examples and can generalise them once it has completed the learning phase. The examples are not simply memorised, but rather the system “recognises” patterns and laws in the learning data. This means that the system can also assess unknown data through the transfer of learning or even fail to learn unknown data due to overadaptation. Initial successes have been achieved, for example in one of the largest competence centres for research into automated IT risk identification: the team at RadarServices puts these directly into practice with its customers. However, the experts also remain realistic: “We prefer to stay on the safe side and test our algorithms over a longer period of time before using them as the only analysis tool – without expert involvement,” says Christian Polster, who is responsible for research and technology development at RadarServices.

The computer scientist Donald Knuth summed up the status quo in this way: “AI does everything that requires thought, but fails to do what humans and animals do automatically without thinking.”

*written by Nicole Jungmann*


Bild/Image: istock.com/monsitj