Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 190 (2024)

Heft: 11

Artikel: Ersetzt generative künstliche Intelligenz das eigene Denken?

Autor: Müller, Peter

DOI: https://doi.org/10.5169/seals-1063633

Ersetzt generative künstliche Intelligenz das eigene Denken?

Viele sprechen von einer Technologierevolution. Die generative künstliche Intellgenz ist heute omnipräsent und öffnet dank ihrer Multimodalität neue Perspektiven. Wissen wir, wie sie funktioniert? Wie schützen wir uns vor Desinformation und Betrug? Das Forum Sicherheit Schweiz ging solchen Fragen nach.

Peter Müller

Mit der generativen künstlichen Intelligenz hat sich der Mensch einen digitalen Partner erschaffen. Riesige Datenmengen lassen sich auf neue Art und in verschiedensten Bereichen praktisch ohne Zeitverlust nutzen. Auf einer einzigen Benutzeroberfläche können Sprache, Text und Bilder aufgenommen, verstanden und ausgewertet werden. Die Effizienzsteigerungen sind verlockend. Immer mehr Menschen und Organisationen nutzen das Werkzeug, meist ohne die dahinterstehende Technologie zu kennen. Damit öffnen sich Überwachungs-, Manipulations- und Betrugsmöglichkeiten. Das Forum Sicherheit Schweiz (FSS) griff an seinem 18. Security Talk vom 26. August in Bern diese Herausforderungen auf.

Die Leistung von Menschen übertreffen

Es war an Katharina Fulterer, im ersten Inputreferat zum Thema «den Teppich zu legen». Künstliche Intelligenz (KI) sei heute in unserem Alltag omnipräsent und könne vielseitig sinnstiftend eingesetzt werden. Als Beispiele nannte sie die Routenwahl und -optimierung mittels Navigationssystemen, unsere Fitness-Tracker oder die Transaktionsüberwachung der Banken zur Betrugsbekämpfung. Prognosen und Vorhersagen standen mittels Predictive KI am Ursprung. Über Machine Learning, neuronale Netzwerke und Deep Learning wurde die Technologie weiterentwickelt. Die erst kürzlich entstandene generative KI generiere «komplett neue Outputs». Nun verfügten wir über ein Medium, «das uns erlaubt, in den Dialog mit künstlicher Intelligenz zu treten».

Mittlerweile komme die KI tatsächlich an Leistungen von Menschen heran «oder übertreffe diese sogar». Damit verbunden seien nicht zu verkennende Gefahren für den Menschen (Nutzung persönlicher Daten), die Unternehmung (Datenabflüsse) oder die Gesellschaft (Versorgungssicherheit). Dies seien bloss ausgewählte Beispiele. Viele Unternehmen scheiterten im Moment noch an der Komplexität der Implementierung wegen der komplett neue Einflussfaktoren und der Anbindung an bestehende Systeme. Elementar sei, von Anfang an «sichere und vertrauenswürdige Systeme konzipieren zu können».

Wie können wir Vertrauen gewinnen?

Das Vertrauen in die künstliche Intelligenz stand im Fokus des zweiten Inputreferats von Stefan Preuss. KI funktioniere seines Erachtens zu 95 bis 99 Prozent; aber sie werde nie zu 100 Prozent ordnungsgemäss und reibungslos ablaufen. Deshalb müssten wir in der Lage sein, diese restlichen Prozente so abzufedern, «dass keine Schäden eintreten und insbesondere keine Personen geschädigt werden.» Gingen Dinge schief, so müsse man daraus lernen; momentan ginge noch einiges schief. Letztlich gehe es auch bei der KI um Vertrauen. Leider gebe es keine Guardrails Content Policy, die vorgeben, was erlaubt ist und was nicht.

Preuss sieht vier Dimensionen, wann wir einer Technologie vertrauen können: Sicherheitsmechanismen sind impliziert und ausgereift; die Firma pflegt Werte, welche nicht nur der Gewinnmaximierung dienen; das Bewusstsein der Reputation zum bereitgestellten Produkt ist vorhanden; und es besteht eine sinnvolle Regulierung, die auch «ein Bestrafungssystem für Fehlverhalten und Versagen mitberücksichtigt». Im Hintergrund müssten also gewisse Vorgaben vorhanden sein. Und schliesslich brauche es das Bewusstsein, dass sich nicht jedes Problem mittels KI lösen lasse. Die Realität «schreibe ihre eigenen Gesetze». Die Alternative zu KI sei immer noch Human Power.

Exponentielle Entwicklung der Technologie

Dr. Thomas Rothacher rief als dritter Inputreferent die enorme Beschleunigung der Technologieentwicklung in Erinnerung: Alles werde immer schneller, umfassender und breitflächiger. Brauchte Netflix noch dreieinhalb Jahre zur Gewinnung einer Million Nutzer, benötigte ChatGPT dafür gerade einmal fünf Tage. Bei der Handschrifterkennung benötigte ein Algorithmus über zehn Jahre, bis er besser war als der durchschnittliche Mensch; bei der Spracherkennung dauerte der Prozess noch zwei Jahre. Heute sei es die zivile Welt, welche die Technologie antreibe, nicht mehr das Militär. Dieser Technologiewandel habe mehr Einfluss auf unsere Kultur als wir wahrhaben wollten.

Drohnen seien ein aktuelles Beispiel der Anwendung von KI. Sie seien nicht mehr unter menschlicher Kontrolle, sondern suchten sich nach dem Prinzip «Fire and Forget» mittels künstlicher Intelligenz ihr Ziel selbst. Die Ukraine sei das erste Land, welches eine unbemannte Einheit als eigene Gattung eingeführt habe. Die Schweiz sei heute im Bereich KI und Drohnen eine führend Nation. Kürzlich wurde eine Taskforce Drohnen gegründet, um die einzelnen Player zu vernetzen und einen Beitrag für die Sicherheit zu leisten. Geschwindigkeit werde zu einem Schlüsselfaktor. Und man müsse sich anpassen können, um zu überleben. Er befürchte bisweilen, wir Schweizer «wähnten uns in einer Bubble und nähmen nicht wahr, was um uns herum geschehe».

Erleben wir eine Technologierevolution?

In der Podiumsdiskussion wurde eine Reihe von Fragen angesprochen; aus Platzgründen müssen wir uns auf eine Auswahl der Themen konzentrieren. Und wir verzichten aus dem gleichen Grund auf eine namentliche Zuordnung einzelner Aussagen; die gemeinsame Überzeugung steht im Vordergrund.

Künstliche Intelligenz wird übereinstimmend als Technologierevolution gewertet; sie stelle einen ähnlichen Entwicklungsschritt dar wie Lesen, Schreiben, Rechnen oder die Elektrizität. Die schiere Menge an Daten stehe nun ausgewertet zur Verfügung und wir könnten diese praktisch ohne Zeitverzug nutzen. Firmen gingen dazu über, anstelle eines reinen Produkts die neuen Technologien als Dienstleistung (Services) zur Verfügung zu stellen. Parallel dazu steige der Bedarf nach Beratungsdienstleistungen spürbar. Das alles sei deutlich mehr als ein vorübergehender Hype.

Müssen wir die Funktionsweise kennen?

Die meisten Menschen nutzen heute dieses neue Werkzeug ohne zu wissen, wie die zugrundeliegende Technologie funktioniert. Der Gebrauch scheint verlockend. Damit stehen zwei zentrale Fragen im Raum: Muss man wissen, wie etwas funktioniert? Und darf man nur anwenden, ohne kritisch zu hinterfragen? Selbst Spezialisten geben zu, dass sie nicht alles im Umgang mit künstlicher Intelligenz verstehen. Wichtiger scheinen gewisse Skills im Umgang mit neuen Technologien: Kritisches Denken sei essenziell wichtig. Das verlange auch nach einem vorsichtigen und bewussten Einsatz beispielsweise von ChatGPT. Wir müssten ausprobieren und vergleichen. Beispielsweise schlage KI bei War Games oftmals andere Lösungen vor als der Mensch mit seinen Erfahrungen wählen würde. Das passe dann nicht in jedes Szenario. Der gesunde Menschenverstand darf somit bei allem technologischen Fortschritt nicht auf der Strecke bleiben.

Verhinderung von Missbräuchen mittels Regelungen?

Der Meinungsbildungsprozess zu diesem Thema scheint noch nicht abgeschlossen. Die einen befürworten eine «sinnvolle», jedoch geringfügige Regulierung: Globale Vorschriften wären hilfreich, da heute praktisch jedes Land anders vorgehe. Dadurch dürften jedoch Weiterentwicklungen und Innovationen weder gehemmt noch unterbunden werden. Wir hätten es verpasst, das Internet und Social Media zu regulieren und heute versuche man mühsam, diese Büchse der Pandora wieder zu schliessen. Es brauche jedoch noch eine gewisse Zeit, bis man die zu regulierenden Objekte definiert habe. Und vor allem müsse man zuerst verstehen, «wovon man überhaupt spricht».

Andere äusserten sich – gerade auch im militärischen Bereich – skeptischer zu Regulierungen: Alle Entwicklungen und Funktionen, die möglich seien, würden früher oder später ohnehin eintreten. Wichtiger sei, sich Gedanken zu machen, «wie man damit umgehen wolle». Einig war man sich, dass die aktuelle Herangehensweise der EU überschiesse. Zur Erinnerung: Das EU-Parlament hat im März 2024 den Einsatz der künstlichen Intelligenz in einem Gesetz geregelt und damit das weltweit erste umfassende KI-Gesetz verabschiedet. Es wird nach 24 Monaten in vollem Umfang anwendbar sein. Auch kleine KI-Systeme mit geringem Risiko müssen gemäss EU künftig bewertet werden. Einig waren sich die Podiumsteilnehmer in folgendem Punkt: Für eine disruptive Technologie wie KI reichten Selbstdeklarationen und -regulierungen nicht.

Der Umgang mit künstlicher Intelligenz

Wenn man von Regelungen nicht allzu viel hält und sich der Umgehungsmöglichkeiten bewusst ist, dann tritt der Nutzer künstlicher Intelligenz fast zwangsläufig in den Fokus. So müsse beispielsweise bei der Nutzung von ChatGPT die Herkunft der Daten kritisch hinterfragt werden: Wer füttert das System? Die Fragen seinen möglichst präzise zu stellen, um das Antwortspektrum einzugrenzen. Stets sollten Plausibilitätsüberlegungen den Antworten folgen: Wie realistisch ist das Ergebnis?

Mit der generativen KI (Beispiel ChatGPT) ist eine neue Situation entstanden: Die Bots werden immer besser, deren Lese-, Hör- und Schreibfähigkeit hat sich stark verbessert. Folge davon ist: Die Anwender können Bots teilweise nicht mehr von Menschen unterscheiden. Beeinflussungsmöglichkeiten analog echter Propaganda sind damit nicht auszuschliessen. Kritisches Denken erhält einen zentralen Stellenwert!

Die Gesellschaft besser vorbereiten

Die Podiumsteilnehmer waren sich einig: Viele Menschen aller Altersstufen sind von der künstlichen Intelligenz betroffen, aber nicht darauf vorbereitet. Schulen und Universitäten müssten einen anderen Umgang



Inputreferate von Katharina Fulterer, Stefan Preuss und Dr. Thomas Rothacher (v. l. n. r.). Bilder: FSS

◀ **Podiumsdiskussion mit (von links) Dr. Thomas Rothacher, Stefan Preuss, Jennifer Scurrell, Fredy Müller (Moderation), Patrick Fontana und Dr. Peter Friedli.** Bild: FSS

18. FSS SECURITY TALK

Inputreferenten und Podiumsteilnehmer:
- Katharina Fulterer, Partnerin Data & AI, Eraneos Switzerland AG
- Stefan Preuss, Leiter Emerging Technologies Audit, Die Mobiliar
- Dr. Thomas Rothacher, Leiter Wissenschaft und Technologie, Armasuisse
- Patrick Fontana, Digital & App Innovation Specialist, Microsoft
- Dr. Peter Friedli, Partner, Eraneos Switzerland AG
- Jennifer Scurrell, Doktorandin Center for Security Studies, ETH Zürich
- Lisa Kontratieva (Key Take Aways), Head of AI, ti&m
- Fredy Müller (Moderation), Geschäftsführer, Forum Sicherheit Schweiz

mit KI pflegen. Die Grundschule greife das Thema nicht auf, die Universitäten flüchteten sich teilweise in Verbote. Das sei der falsche Ansatz. Die Kinder müssten von klein auf mit den neuen Technologien vertraut gemacht werden. Dann lernten sie auch, Fakten zu validieren.

Künstliche Intelligenz biete grundsätzlich die schnelle Möglichkeit, die eigenen Kompetenzen zu erweitern. Wissen sei heute keine Schwierigkeit mehr; das Problem liege im Werten des Wissens. Bereits Kinder und Jugendliche müssten lernen, mit dem Thema umzugehen. So liessen sie sich auch weniger von Deepfakes täuschen. Kritisches Denken und kritisches Diskutieren müssten gezielter gefördert werden. Plausibilitätsüberlegungen erlangten einen höheren Stellenwert oder – wie das ein früherer Rüstungschef gerne zu sagen pflegte – wir müssten wieder vermehrt mit «der Agentur GMV» (gesunder Menschenverstand) zusammenarbeiten.

Sicherheitskontext und militärisches Umfeld

Künstliche Intelligenz basiert auf bereits vorhandenen Daten. Diese müssen in genügender Menge und vor allem geeigneter Qualität vorliegen. Bei jeder Interaktion mit ChatGPT fliesse eine grosse Menge an Daten ab; dagegen helfe keine Firewall. Deshalb wird empfohlen, dass Unternehmen eine KI-Strategie erarbeiten. Darum ist Vertrauen in die Technologie wichtig. Und folglich lohnt sich eine kritische Auseinandersetzung mit den Resultaten.

KI werde in der Schweizer Armee beispielsweise bereits in Stabsübungen eingesetzt: Szenarienentwicklung, Datenanalyse bei fusionierten Lagebildern sowie Text- und Bildanalyse seien Beispiele dazu. Die KI helfe so, Entscheidungen zu treffen. Auch hier stehe die Frage im Zentrum, wie ich das System mit eigenen Daten füttere. Und wann komme der Mensch (noch) zum Tragen? In diesem Zusammenhang wird gerne auf das AEK-Prinzip verwiesen: Auswertung und Erkenntnis erfolgten durch künstliche Intelligenz, die Konsequenzen jedoch würden durch Menschen gezogen. So «bleibe der Mensch noch immer im Loop drin».

Ein Lichtblick am Rande

Es wurde bereits erwähnt: Die Armee ist nicht mehr die technologische Treiberin. Die (zivile) Schweiz befinde sich im Bereich Forschung/Innovation auf einem Spitzenrang. In der Umsetzung hapere es jedoch noch ein wenig. Und im Konfliktfall sei es schwieriger, Produkte in der Schweiz herzustellen und so einen Beitrag zur Versorgungssicherheit zu leisten. Deshalb sei es gerade im Bereich KI wichtig, «das Ökosystem der Start-ups in der Schweiz näher an die Rüstungsindustrie heranzubringen und dort Widerstände zu brechen.»

Der kürzlich durchgeführte vierte Innovationstag der STA (siehe separaten Beitrag in dieser Nummer) hat sehr viel mehr Start-ups mit der Armee zusammengeführt als in den vorhergehenden Jahren. Da tauchten Namen und Vertreter von (Klein-)Firmen auf, die bisher wohl nur einem kleinen Kreis vertraut waren. Die Widerstände der Start-ups, sich mit Rüstungsvorhaben zu identifizieren und generell die gegenseitigen Berührungsängste scheinen abzuklingen. Die gemeinsame Sicherheitsherausforderung gewinnt an Bedeutung.

Der vorliegende Beitrag wurde völlig ohne künstliche Intelligenz redigiert, jedoch mit Unterstützung von Mitarbeitenden des Forums Sicherheit Schweiz. Danke!

Maj a D Peter Müller
Dr. rer. pol.
Redaktor ASMZ
peter.mueller@asmz.ch
3672 Oberdiessbach