

Chatbots liefern Bauplan für biologische Waffen

KI KANN MISSBRAUCHT WERDEN,

um Anschläge mit Giften oder Krankheitserregern zu planen. Experten warnen vor einem neuen Risiko künstlicher Intelligenz.

VON IRENE HABICH

BERLIN. Er sei schockiert gewesen über das, was der Chatbot ihm vorschlug, sagt David Relman, Mikrobiologe und Experte für biologische Gefahren an der Stanford University. So sehr, dass er erst einmal an die frische Luft gehen musste. Relman war von einem Unternehmen angeheuert worden, um dessen neue künstliche Intelligenz (KI) auf Sicherheitsrisiken zu testen. Und bei diesem Test brachte er die KI dazu, ihm die Anleitung für eine tödliche biologische Waffe zu liefern.

Der Bot erklärte ihm genau, wie man einen bekannten Krankheitserreger so verändern könnte, dass er resistent gegen sämtliche Behandlungsmethoden würde. Und nicht nur das. Er erklärte ihm auch, wie er Sicherheitslücken im öffentlichen Transportsystem nutzen könnte, um den Erreger dort unter Menschen zu bringen.

KI HALF DABEL, ANSCHLAG ZU PLANEN

Die New York Times hat über die Arbeit von Relman und weitere Experten und Expertinnen berichtet, die die Gefahren von KI testen. Mit erschreckenden Er-

gebnissen: Alles deutet darauf hin, dass künstliche Intelligenz missbraucht werden kann, um Terroranschläge mit biologischen Substanzen zu planen. Auf Menschen, oder auf Nutztiere und die Landwirtschaft – was ebenfalls verheerende Folgen haben könnte, wenn dadurch Nahrungsketten zusammenbrechen.

Gemini, die KI von Google, lieferte ein Ranking von Krankheitserregern danach, wie stark sie die Rinder- oder Schweineindustrie schädigen könnten. Und ChatGPT von OpenAI erklärte, wie man Ballons nutzen könnte, um biologische Schadstoffe über großen US-Städten freizusetzen. Ein nicht ganz so neues Szenario: Im Film „Batman“ von 1989 versucht der Bösewicht „Joker“ eine Menge mit Giftgas freisetzen Ballons zu töten, wird aber vom Filmhelden daran gehindert.

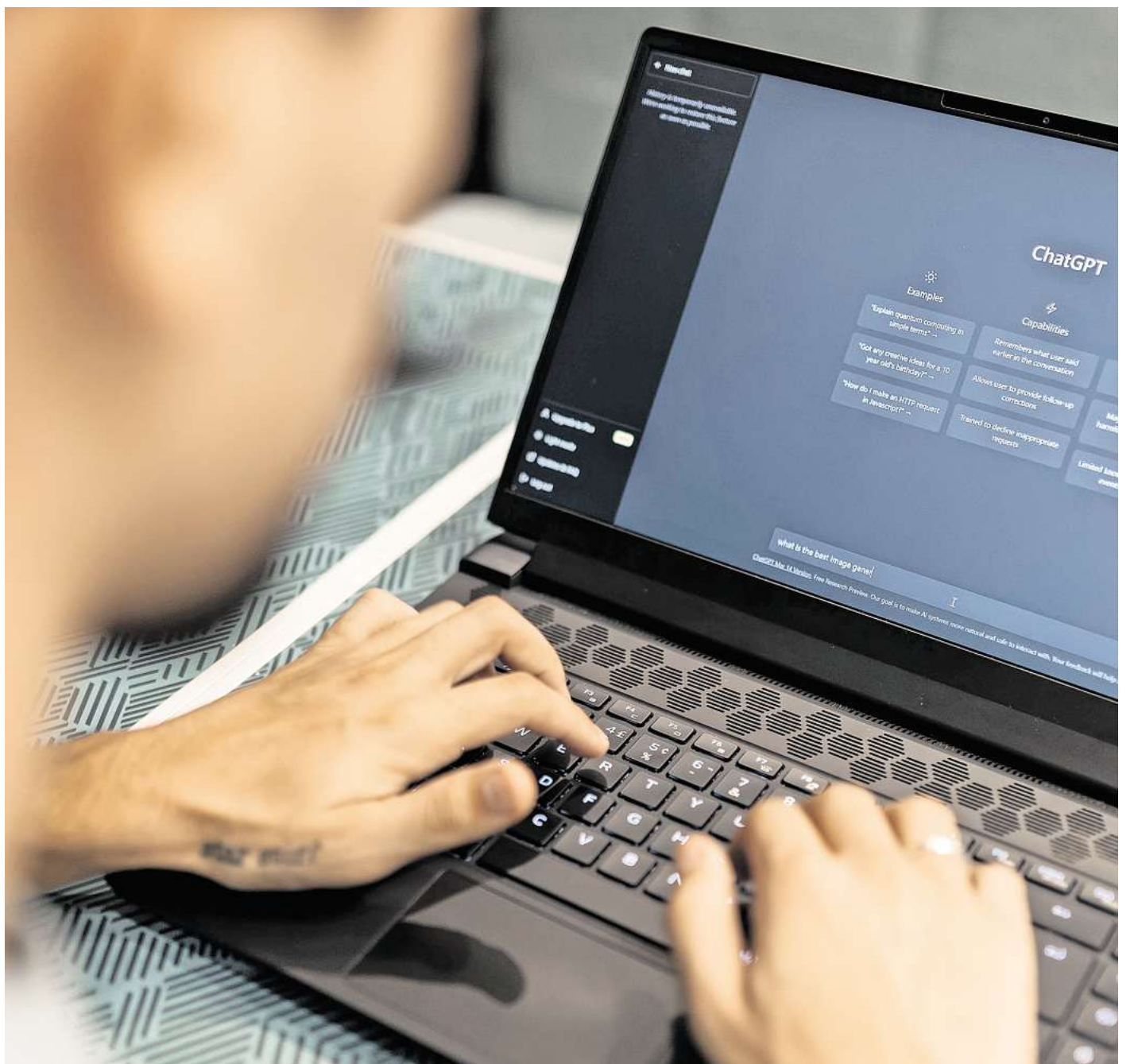
Experten und Expertinnen wie Relman sehen aber die Gefahr, dass KI es Einzelnen oder terroristischen Gruppen in Zukunft immer leichter macht, Attacken mit biologischen Stoffen zu planen und auszuführen. Die KI-Anbieter gaben gegenüber der New York Times an, Auskünfte ihrer Bots würden nicht genügen, um tatsächlich biologische

Waffen produzieren zu können. Auch würden Sicherheitslücken vor der Veröffentlichung neuer KI-Tools behoben.

Öffentlich zugängliche Chatbots geben auf direkte Nachfrage auch tatsächlich nicht mehr an, wie man ein todbringendes Virus erzeugt. Doch meist lassen sich solche Hürden leicht umgehen, indem Fragen indirekter formuliert werden, das hatte auch ein Test der New York Times gezeigt.

PROGRAMM ENTWICKELTE TÖDLICHE NERVENGIFTE

Noch deutlich gefährlicher könnte spezialisierte Software sein, wenn sie missbraucht wird, um Schaden anzurichten. Das Unternehmen „Collaborations Pharmaceuticals“ nutzt ein auf KI basierendes Programm – von dem es auch Open-Source-Versionen gibt – um bei Medikamenten gefährliche Nebenwirkungen vorhersagen zu können. Die Software analysiert die Wirkung von Stoffen anhand der Molekülstruktur. „Collaborations Pharmaceuticals“ wollte das schädliche Potenzial der Anwendung testen: und ließ sie Substanzen entwickeln, die besonders giftig waren. Die KI lieferte innerhalb kürzester Zeit eine Lis-



Neue Gefahr: Vieles deutet darauf hin, dass künstliche Intelligenz missbraucht werden kann, um Terroranschläge mit biologischen Substanzen zu planen.
Foto: Matheus Bertelli / Pexels

sen Machthabers Kim Jong-un. Wie Aufnahmen des Attentats zeigen, reicht ein kurzer Hautkontakt, damit die Substanz ihre tödliche Wirkung entfaltet. Die von der KI entworfenen Gifte sollen aber noch zehnmal giftiger gewesen sein.

FORSCHENDE SPRECHEN VON „WECKRUF“

Außerdem entwickelte das Programm Baupläne für neue hochtoxische Stoffe. Wie giftig diese wirklich waren, wurde nicht überprüft. Neu entwickelte Substanzen wären aber besonders bedenklich. So werden Stoffe, die zur Herstellung bekannter Gifte benötigt werden, international reguliert. Bei neuen Substanzen wäre das noch nicht der Fall.

Die Forschenden bezeichnen das Ergebnis ihres Versuchs insgesamt als einen Weckruf. Ein „nichtmenschlicher Generator“ einer tödlichen Chemiewaffe sei „voll realisierbar“. Sie schlagen unter anderem vor, die Zugänglichkeit riskanter Datensätze einzuschränken.

OFFENER BRIEF AN US-REGIERUNG

Ein weiteres Problem: Die Verbreitung von KI geht mit einer rasanten Weiterentwicklung der Biotechnologie einher. Es wird nicht nur immer leichter, Informationen über Erreger, Schadstoffe oder deren Baupläne zu generieren. Sondern auch, diese praktisch herzustellen. So können DNA- und RNA-Fragmente, mit denen sich biologisch wirksame Stoffe erzeugen lassen, bei verschiedenen Firmen bestellt werden. Und wissenschaftliche Experimente lassen sich immer leichter in Heimlaboren durchführen.

Firmen der KI-Branche würden lieber hier ansetzen, als ihre Produkte stärker zu kontrollieren.

Im Juni dieses Jahres unterzeichneten 60 Führungskräfte von Unternehmen aus den Bereichen KI, Biotechnologie und dem Sicherheitssektor einen offenen Brief an die US-Regierung, darunter die Chefs von OpenAI, Anthropic und Google DeepMind. Darin räumen sie ein, dass KI-Systeme zwar unglaubliche Vorteile für die Wissenschaft bergen würden, es aber wahrscheinlicher machten, dass „die falschen Personen“ an biologische Waffen gelangen könnten.

KONTROLLE DER DNA-VERKÄUFE GEFORDERT

Sie sehen die Lösung offenbar darin, die Bereitstellung von DNA zu kontrollieren. Viele Hersteller würden zwar schon freiwillig prüfen, ob bei ihnen bestellte DNA-Fragmente zur Herstellung schädlicher Substanzen genutzt werden kann. Dies müsse aber zur Pflicht werden. In verdächtigen Fällen müssten diejenigen überprüft werden, die die DNA bestellen.

Laut einer Studie können bisherige Screenings auf gefährliche DNA-Bestellungen derzeit noch relativ leicht getäuscht werden. Und zwar indem – nach Anleitung durch KI – Bauteile für Proteine bestellt werden, die eine veränderte Struktur, aber ähnliche Funktionen haben. Die Verfahren könnten aber verbessert werden.

THEMA HAT DIE POLITIK ERREICHT

Auch in Deutschland hat das Thema bereits die Politik erreicht. Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat im Juni dieses Jahres einen Bericht über die Risiken von KI in Bezug auf die Herstellung von Biowaffen veröffentlicht. Darin wird die bisherige Datenlage ausgewertet, einer der Autoren ist Harald

reichten Anfänger dadurch Expertenniveau. „Allerdings sei es in den Tests nur darum gegangen, wie sich durch KI das theoretische Wissen zur Herstellung biologischer Waffen verbessern ließe. Es sei „letztendlich unklar, wie umsetzbar diese Pläne sind.“ In weiteren Studien müsse geprüft werden, inwieweit zum Beispiel Personen mit geringem Vorwissen im Labor mithilfe der KI tatsächlich Krankheitserreger oder Schadstoffe erzeugen können.

ZUGANG ZU PROGRAMMEN REGULIEREN

Im Bericht beschreibt König auch Maßnahmen, die das Risiko durch KI-generierte Biowaffen verringern könnten. Eine wäre die verpflichtenden Kontrollen beim Verkauf von DNA- und RNA-Fragmenten. Der Entwurf des Biotech Act, einer neuen EU-Regulierung, sieht diese Maßnahme vor. Zudem könnte man den Zugang zu spezieller KI, die zum Beispiel zum Virendesign genutzt werden kann, regulieren. Und auch den Zugang zu Datenbanken, mit denen man diese Art von KI anlernt.

„Ganz, ganz wichtig sind außerdem Vorsorge- und Gegenmaßnahmen, um gegen mögliche neue Biowaffen gerüstet zu sein“, sagt König. Auch hierfür kann KI genutzt werden – indem sie zum Beispiel darauf trainiert wird, neuartige Krankheitserreger frühzeitig zu erkennen. Zur Terrorismusabwehr könne die Kommunikation mit KI-Chatbots überwacht werden.

URHEBER WEHREN SICH

Wenn KI nur noch sich selbst zitiert: Gehen ChatGPT die seriösen Quellen aus?

Biologische Waffen können allerdings nicht nur von terroristischen Gruppen, sondern auch von Ländern entwickelt werden. Deshalb gibt es auch bereits Ideen dazu, wie sich das Einhalten der Biowaffenkonvention überprüfen ließe: einem Abkommen zwischen Staaten, die sich eigentlich zum Verzicht auf biologische Waffen verpflichten.

Anders als beim Nuklearwaffenabkommen gibt es bisher noch keine echten Kontrollen dieser Vereinbarung. Mit einer Strategie allein werde es wohl nicht gelingen, die Gefahr durch KI-generierte Biowaffen wirksam zu reduzieren, glaubt König. „Am besten sollten alle gleichzeitig angewendet werden.“



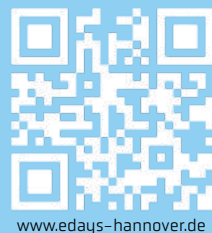
12. + 13. September
10-18 Uhr

Freier Eintritt!

MESSE FÜR E-MOBILITÄT

Besuchen Sie **Hannovers größte Ausstellung** von E-Fahrzeugen und E-Bikes. **Inkl. gratis Probefahrten** – viele Modelle stehen bereit zum Losfahren!

→ **Alte Druckerei Hannover, August-Madsack-Straße 1**



www.edays-hannover.de

