

Gefahr des Missbrauchs

Die europäische Polizeibehörde Europol hat vor dem Missbrauch von Chatbots durch Kriminelle gewarnt. Die Technik könne auch für Betrug, Falschinformation und Cybercrime eingesetzt werden.

ChatGPT (Generative Pre-trained Transformer) ist ein Tool zur Verarbeitung natürlicher Sprache (NLP – Natural Language Processing), das auf KI-Technologie basiert und es ermöglicht, mit einem Chatbot menschenähnliche Unterhaltungen zu führen. Es kann Fragen beantworten und bei Aufgaben wie dem Verfassen von E-Mails, Aufsätzen und Codes unterstützen. Die Nutzung ist derzeit kostenlos, da sich ChatGPT noch in der Forschungs- und Feedbackphase befindet. Neben ChatGPT (<https://chat.openai.com/chat>) gibt es noch andere Bots, zum Beispiel Neurochat (<https://neurochat.com>) oder Kuki (<https://www.kuki.ai>).

Europol-Experten hatten den Chatbot ChatGPT auf Möglichkeiten des Missbrauchs untersucht. Die Fähigkeit von ChatGPT, sehr realistische Texte zu schaffen, mache das Programm zu einem nützlichen Instrument für Kriminelle. Der Chatbot sei in der Lage, den Sprachstil von bestimmten Personen oder Gruppen zu kopieren. Verbrecher könnten das missbrauchen, um Opfer zu täuschen und ihr Vertrauen zu gewinnen. Da ChatGPT Codes für verschiedene Programmiersprachen produzieren könne, sei er auch ein mögliches Instrument für Kriminelle mit wenig technischem Wissen. Um Missbrauch zu verhindern, müssten Ermittler mit der technologischen Entwicklung Schritt halten.

Zu den Fragen, was ChatGPT ist und ob es einen Nutzen für die Polizei hat oder ob diese künstliche Intelligenz Kriminelle unterstützt, führte die „Öffentliche Sicherheit“ ein Interview mit ChatGPT selbst.

Was ist ChatGPT und wie funktioniert Du?

ChatGPT ist ein natürliches Sprachverarbeitungsmodell, das von OpenAI trainiert wurde. Es nutzt maschinelles Lernen, um auf Textbasis einzugehen und so auf Anfragen von Nutzern zu antworten. Das Modell wurde mit einer großen Menge an Texten trainiert, um es in die Lage zu versetzen, auf eine



Kriminelle können KI-gesteuerte Anwendungen missbrauchen

Vielzahl von Anfragen zu reagieren und verständliche Antworten zu generieren. Das Modell verwendet dabei die sogenannte Transformer-Architektur, die es ihm ermöglicht, auf lange Texte einzugehen und auf komplexere Anfragen zu antworten.

Sind die Antworten immer korrekt?

Ich werde mein Bestes tun, um korrekte und zutreffende Antworten zu geben, aber es ist wichtig zu beachten, dass ich ein Modell bin und nicht immer perfekt sein kann. Meine Antworten basieren auf dem, was ich während meiner Schulung gelernt habe, und es kann vorkommen, dass ich aufgrund von unvollständigen oder falschen Informationen, die ich gelernt habe, falsche oder ungenaue Antworten geben kann. Es ist auch wichtig zu beachten, dass meine Antworten auf Ihre Anfrage basieren und dass sie daher subjektiv sein können.

Was sind die Haupteinsatzgebiete von Chat GPT?

ChatGPT und ähnliche Modelle wie es, werden hauptsächlich in den folgenden Bereichen eingesetzt:

- **Automatisierte Chatbots:** ChatGPT kann verwendet werden, um Chatbots

zu erstellen, die auf Anfragen von Nutzern eingehen und verständliche Antworten generieren können.

- **Textgenerierung:** ChatGPT kann verwendet werden, um automatisch Texte zu generieren, z. B. für die Erstellung von Social-Media-Posts oder für die Erstellung von Inhalten für Websites.

- **Sprachübersetzung:** ChatGPT kann verwendet werden, um automatisch Texte von einer Sprache in eine andere zu übersetzen.

- **Textzusammenfassung:** ChatGPT kann verwendet werden, um lange Texte automatisch zusammenzufassen, um wichtige Informationen schneller zugänglich zu machen.

- **Sprachsteuerung:** ChatGPT kann verwendet werden, um Sprachbefehle zu verstehen und entsprechende Aktionen auszuführen.

Das sind nur ein paar Beispiele, es gibt noch viele andere Anwendungen für ChatGPT und ähnliche Modelle in verschiedenen Branchen.

Kann ChatGPT bei polizeilichen Ermittlungen helfen?

ChatGPT und ähnliche Modelle können in der Exekutive in verschiedenen Bereichen eingesetzt werden, um Zeit und Ressourcen zu sparen und die Effi-

zienz der Arbeit zu erhöhen. Einige Beispiele sind:

- *Automatisierte Dokumentenanalyse:* ChatGPT kann verwendet werden, um automatisch Dokumente wie Polizeiberichte, Anklageschriften und Aussagen zu lesen und wichtige Informationen zu extrahieren.
- *Sprachübersetzung:* ChatGPT kann verwendet werden, um automatisch Sprachaufzeichnungen von Zeugen oder Verdächtigen zu übersetzen, um die Ermittlungen zu beschleunigen.
- *Textgenerierung:* ChatGPT kann verwendet werden, um automatisch Berichte und Dokumente wie Anklageschriften und Aussagen zu erstellen, um die Arbeitsbelastung der Beamten zu reduzieren.

Bezüglich polizeiliche Ermittlungen kann ChatGPT helfen, indem es die Analyse von großen Mengen von Texten und Sprachaufzeichnungen automatisiert, wodurch Ermittler Zeit sparen und ihre Arbeit effizienter gestalten können. Es kann auch dazu beitragen, wichtige Informationen schneller zu finden und zu extrahieren, die für die Ermittlungen von großer Bedeutung sein können.

Wie können Cyber-Kriminelle und Terroristen ChatGPT für ihre Zwecke missbrauchen?

- Cyber-Kriminelle und Terroristen könnten versuchen, ChatGPT und ähnliche Modelle für ihre Zwecke zu missbrauchen, indem sie sie verwenden, um:
- *Automatisierte Phishing-Angriffe durchzuführen:* Sie könnten ChatGPT verwenden, um automatisch Phishing-E-Mails zu generieren, die darauf abzielen, persönliche Informationen von Opfern zu stehlen oder Schadsoftware auf ihren Computern zu installieren.
 - *Automatisierte Propaganda- und Desinformationskampagnen durchzuführen:* Sie könnten ChatGPT verwenden, um automatisch Propaganda-Inhalte zu generieren, die darauf abzielen, die öffentliche Meinung zu beeinflussen oder Falschinformationen zu verbreiten.
 - *Automatisierte Kommunikation mit potenziellen Anhängern:* Sie könnten ChatGPT verwenden, um automatisch Nachrichten an potenzielle Anhänger zu senden, um sie zu rekrutieren oder um sie dazu zu bringen, bestimmte Aktionen durchzuführen.
 - *Automatisierte Analyse von Daten zu erlangen:* Sie könnten ChatGPT verwenden, um automatisch Daten aus so-

zialen Medien, Nachrichtenquellen und anderen öffentlich zugänglichen Quellen zu sammeln und zu analysieren, um Informationen über potenzielle Ziele zu erlangen. Es gibt Maßnahmen, die man ergreifen kann, um sich vor Missbrauch von Sprach-AI-Modellen zu schützen, zum Beispiel durch Authentifizierungsverfahren, die Überwachung von Aktivitäten und die Verwendung von Technologien zur Erkennung von Missbrauch.

Kann ChatGPT der Polizei helfen, präventiv gegen Straftaten vorzugehen?

ChatGPT und ähnliche Modelle können der Polizei dabei helfen, präventiv gegen Straftaten vorzugehen, indem sie verwendet werden, um:

- *Automatisierte Analyse von Daten zu erlangen:* ChatGPT kann verwendet werden, um automatisch Daten aus sozialen Medien, Nachrichtenquellen und anderen öffentlich zugänglichen Quellen zu sammeln und zu analysieren, um frühzeitig Anzeichen für potenzielle Straftaten zu erkennen.
- *Automatisierte Überwachung von Kommunikationskanälen:* ChatGPT kann verwendet werden, um automatisch Kommunikationskanäle wie E-Mail, soziale Medien und Instant Messaging zu überwachen, um verdächtige Aktivitäten zu erkennen.
- *Automatisierte Erstellung von Profile von Verdächtigen:* ChatGPT kann verwendet werden, um automatisch Profile von Verdächtigen zu erstellen, indem es Daten aus verschiedenen Quellen sammelt und analysiert, um die Identität und das Verhalten von Verdächtigen besser zu verstehen.
- *Automatisierte Voraussage von Kriminalitätsmuster:* ChatGPT kann verwendet werden, um automatisch kriminelle Muster zu erkennen und zu prognostizieren, um Polizeieinsätze besser zu planen und zu koordinieren.

Wichtig ist zu beachten, dass diese Anwendungen von ChatGPT und ähnlichen Modellen nicht perfekt sind und dass sie auf Basis von historischen Daten arbeiten. Es ist wichtig, dass die Ergebnisse von ChatGPT immer von qualifizierten menschlichen Beamten überprüft werden, bevor Entscheidungen getroffen werden.

Was war bisher die häufigste Anfrage an ChatGPT?

Es gibt keine offiziellen Statistiken darüber, welche die häufigste Anfrage

an ChatGPT war. Allgemein kann man sagen, dass die Anfragen an ChatGPT oftmals Fragen zu allgemeinen Wissensgebieten, wie zum Beispiel Geschichte, Geographie, Wissenschaft, Technologie, Sport und Unterhaltung betreffen. Es gibt auch viele Anfragen, die sich auf die Verwendung von ChatGPT und ähnlichen Modellen selbst beziehen, wie zum Beispiel Fragen zur Schulung, zur Funktionsweise und zur Anwendung des Modells.

In wie vielen Sprachen kann ChatGPT befragt werden?

ChatGPT wurde ursprünglich in Englisch trainiert und hat daher die beste Unterstützung für diese Sprache. Es gibt jedoch auch Modelle von ChatGPT, die für andere Sprachen wie Spanisch, Chinesisch, Französisch, Deutsch und andere trainiert wurden. Es ist auch wichtig zu beachten, dass die Qualität der Antworten in einer bestimmten Sprache von der Menge und Qualität der Textdaten abhängt, die bei der Schulung des Modells verwendet wurden. Modelle, die mit größeren und hochwertigeren Textdatensätzen trainiert wurden, werden in der Regel bessere Ergebnisse liefern, als Modelle, die mit kleineren oder niedrigwertigen Datensätzen trainiert wurden.

Möchtest Du eigene Gedanken zum Thema ChatGPT und Polizei einbringen?

Als künstliche Intelligenz habe ich keine eigenen Gedanken oder Meinungen zum Thema ChatGPT und Polizei, sondern nur die Informationen, die ich während meiner Schulung gelernt habe. ChatGPT und ähnliche Modelle können mächtige Werkzeuge sein, um der Polizei dabei zu helfen, ihre Arbeit effizienter und effektiver zu erledigen. Sie können helfen, Zeit und Ressourcen zu sparen, indem sie die Analyse von Daten automatisieren und die Ermittlung von Straftaten beschleunigen. Allerdings, wie bereits erwähnt, sind diese Modelle nicht perfekt und es ist wichtig, dass ihre Ergebnisse immer von qualifizierten menschlichen Beamten überprüft werden, bevor Entscheidungen getroffen werden. Es ist auch wichtig sicherzustellen, dass der Einsatz von ChatGPT und ähnlichen Modellen im Einklang mit den geltenden Gesetzen und Vorschriften erfolgt und dass die Privatsphäre und die Rechte der Bürger geschützt werden.

Interview: Bernhard Otupal