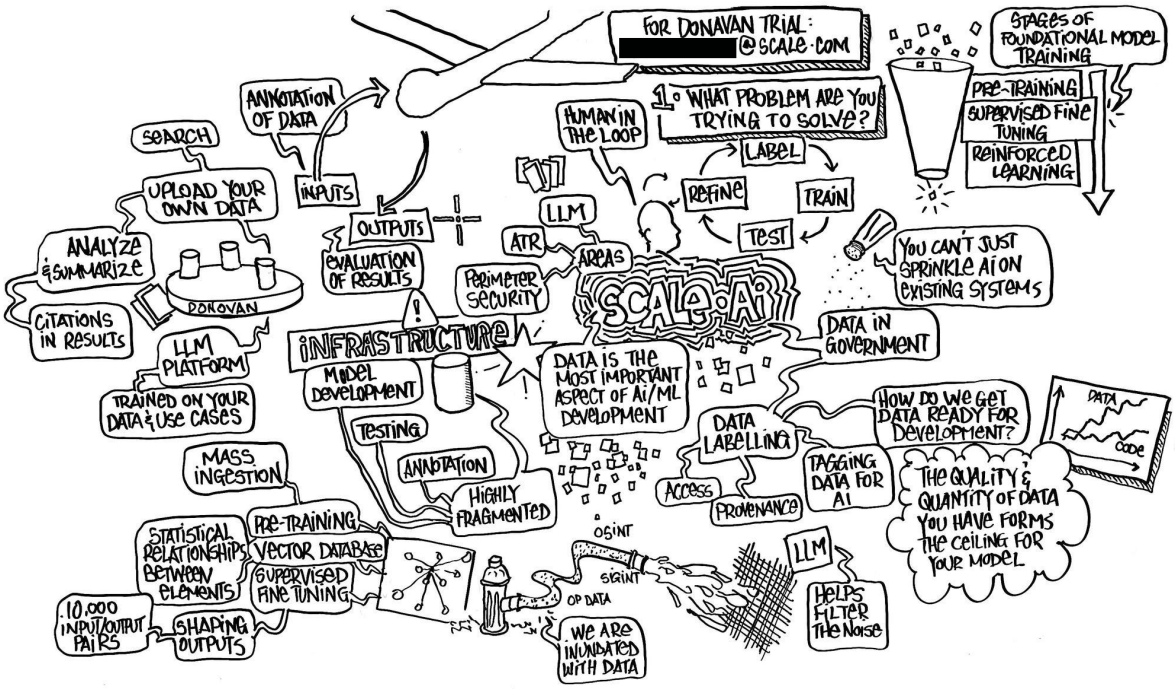
jackpoulson.substack.com

Leak sheds light on ecosystem behind Pentagon's AI adoption

Jack Poulson

47–56 Minuten



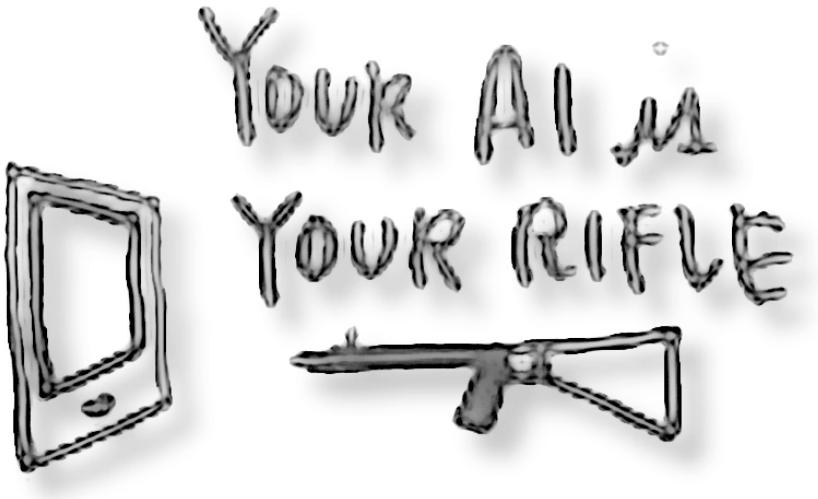
Eine überarbeitete Gedankenkarte darüber, wie das US-Militär die Datenkennzeichnungs- und künstliche Intelligenzfähigkeiten von Scale AI integrieren kann, die von einem Mitarbeiter des Beratungsunternehmens TheDifference for U.S. Special Operations Command als Teil eines Workshops, der im Pinewood Mission Support Center von NexTech Solutions in Tampa, Florida, von der gemeinnützigen Auftragnehmerin Alethia Labs mit Mitteln des Pentagon Chief Digital & AI Office veranstaltet wurde. Die E-Mail-Adresse, die für eine Studie des Donovan-Produkts von Scale AI ausgeschrieben wurde, das sich rechts von einer Zeichnung einer Militärdrohne befindet, wurde überarbeitet. Die primären Akronyme, die im Bild verwendet werden, jenseits von KI, sind für Large

Language Models (LLMs), Automated Target Recognition (ATR), Signals Intelligence (SIGINT) und Open Source Intelligence (OSINT).

Mit einer Handzeichnung des zusammengesetzten Bildes erwartete er, dass ein Satellit einen weißen Wetterballon durch eine schnelle Abfolge von Sonden in jedem der roten, grünen und blauen Farbkanäle einfangen würde - im Wesentlichen überlappend rot, grün und blau überlappend rot, grün und blau über einen dunklen Hintergrund - Corey Jaskolski fütterte die Vorlage in die künstliche Intelligenz seines Unternehmensshot down. Air Force F-22 Kampfjet am 4. Februar 2023. Damals erklärte Verteidigungsminister Lloyd Austin, dass der Ballon „versuche, strategische Stätten in den kontinentalen Vereinigten Staaten zu überwachen". Aber sieben Monate später sagte der damalige Vorsitzende der Joint Chiefs of Staff Mark Milley gegenüber CBS News, dass „es keine Geheimdienstsammlung durch diesen Ballon gab".

Die offenbar überblasen Vorwürfe der chinesischen Luftüberwachung stellten dennoch Synthetaic fest, Mr. Jaskolskis synthetisches Datenunternehmen, als Marktführer in der KI-gestützten Overhead-Überwachung. Nach der Ankündigung der neuen Partnerschaft von Microsoft mit dem Start bei einer Keynote-Präsentation in einem US-amerikanischen Air Force-Konferenz am Morgen des 29. August letzten Jahres, Microsoft-Exekutive Jason Zander rekonstruiert Synthetaics Methodik zur Verfolgung des chinesischen Ballons durch eine Demonstration der Plattform Rapid Automatic Image Categorization (RAIC) des Unternehmens. Etwa 21 Minuten nach seinem Vortrag, Mr. Zander stellte den zusätzlichen „Bonus" zur Verfügung, dass RAIC „die F-22-Sortie fing, die tatsächlich in Richtung [den Ballon] geleitet wurde, um sie abzunehmen." Mit einem Satellitenbild des angeblichen F-22-Bildschirms mit spürbarer Farbbandtrennung argumentierte Zander, dass "wir das wissen, weil der Vektor, das Timing und der Transponder

[der F-22] nicht wirklich emittiert wurden."[1]



Eine neukalierte und künstlerisch gefilterte Variante eines für die USA produzierten Bildes. Space Force des gemeinnützigen Auftragnehmers Alethia Labs während eines Workshops über künstliche Intelligenz Literacy im Auftrag des Pentagon Chief Digital & Artificial Intelligence Office auf der Los Angeles Air Force Base in El Segundo, Kalifornien am 17. Oktober 2023.

Zanders Keynote zeigte eine Verbesserung gegenüber dem chinesischen Ballonüberwachungshandwerk, das Jaskolskis handgezeichnetes Bild durch die Text-zu-Bild-Generierungsfunktionen des in San Francisco ansässigen Produkts DALL-E 2 des DALL-E 2-Produkts des in San Francisco ansässigen Kunstintelligence-Unternehmens OpenAI ersetzte. Nach der Auswahl des dritten Bildes, das von DALL-E für "Ein Top-Down-Luftbild einer Kreidezeichnung der Karte der Vereinigten Staaten [wo] jeder Staat in einer anderen Farbe ist" erstellt wurde, zeigte Zander, wie RAIC das synthetische Bild als Vorlage verwenden konnte, um tatsächliche Kreidekarten der USA aufzudecken, die in einem hochauflösenden Bild von Milwa. (Microsoft hat Berichten zufolge 13 Milliarden Dollar in OpenAI investiert und hat Einfluss irgendwo auf das Spektrum zwischen dem exklusiven Partner und de facto Muttergesellschaft.)

Nachdem er eines von Hunderten von Ergebnissen ausgewählt hatte,

die mit der DALL-E-Rendering einer Kreidekarte übereinstimmten, sagte Zander der Air Force-Konferenz: "Wenn ich weiter [sic] genug zoome, gebe ich Ihnen die Lancaster Elementary School in Milwaukee auf dem Spielplatz im hinteren, direkt neben dem Hopscotch Court, ist eine tatsächliche Zeichnung der Vereinigten Staaten. Welche, nett, ute? ... An Milwaukee muss etwas gewesen sein, denn es gibt viele Schulen mit diesen auf den Spielplätzen."2

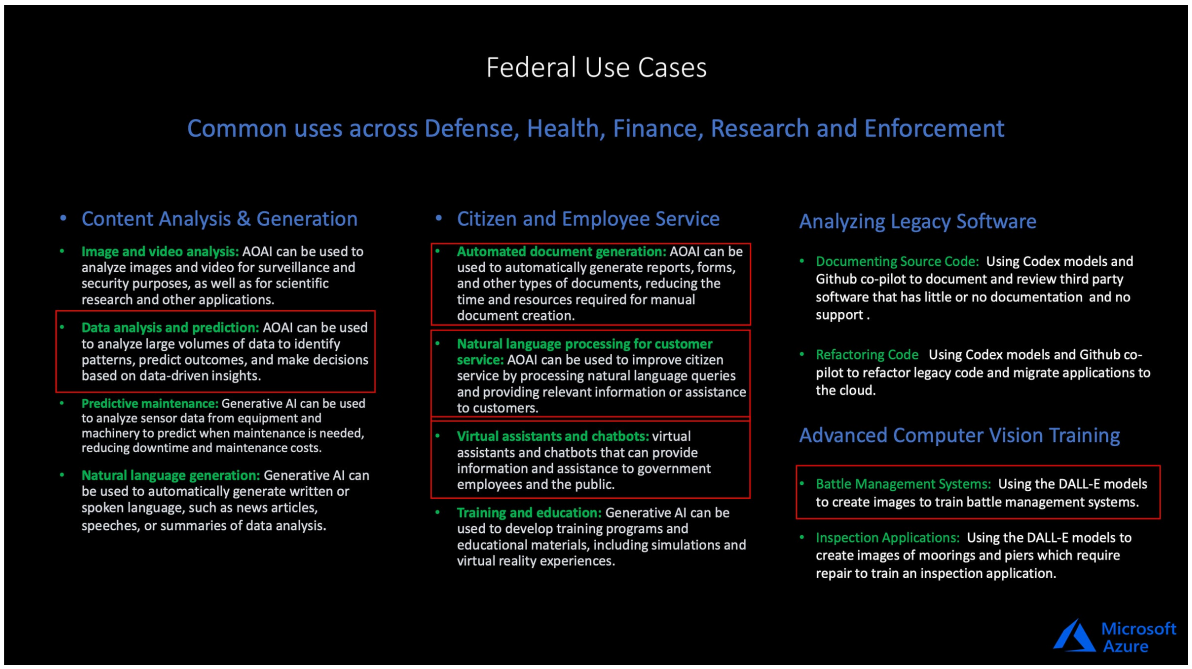
Synthetaic begann einen kurzen Vertrag mit den USA. Air Force on "KJJADIC - RAIC IN Unterstützung von JADO [Gemeinsame All-Domain-Operationen]" am selben Tag wie Mr. Zanders Beweis für die Fähigkeiten des Unternehmens für die USA. Air Force.

Wenn Sie nach Kommentaren zu Herrn gespannt sind. Zanders Demonstration, wie DALL-E und RAIC verwendet werden könnten, um Overhead-Bilder von Grundschulen auf den Abteilung für Informationstechnologie der Luftwaffe und Cyberpower Education & Training Event (DAFITC) zu überwachen, sagte Microsoft, dass "der Schulfall kein spezifisches Beispiel ist, sondern ein Beispiel, was möglich ist, was am DAFITC geliefert wurde."

OpenAI erklärte, dass sein Unternehmen „eine klare Politik gegen die Beeinträchtigung der Privatsphäre anderer habe und sich nicht wohl fühlen würde, wenn [ihre] Technologie verwendet wird, "um Grundschulen mit Überwachungstechnologien in einem militärischen Kontext zu überwachen".

Dank einer bisher nicht gemeldeten öffentlichen Offenlegung von Präsentationen von Microsoft, Palantir und Scale AI auf der Los Angeles Air Force Base durch einen gemeinnützigen Auftragnehmer mit dem Chief Digital & Artificial Intelligence Office des Pentagon ist nun klar, dass Microsoft Verstöße gegen das nominelle öffentliche Verbot von "Militär-

und Kriegsführung"-Verwendungen seines Produkts etwa drei Monate vor OpenAIs Aufhebung des OpenAI-Klaus führte. In einem Vortrag mit dem Titel „Generative KI mit DoD Data“ vom 17. Oktober 2023 beschrieb der neunte Dia des Microsoft-Technologiespezialisten Nehemiah Kuhns zahlreiche US-amerikanische. Das Verteidigungsministerium und die föderale „Durchsetzung“ verwenden Fälle für den OpenAI-Wrapper, der von Microsofts Azure Cloud-Computing-Abteilung, Microsoft Azure OpenAI, verkauft wird, der oft auf AOAI verkürzt wird.



Generative KI mit DoD-Daten [überarbeitet]

3.5MB - PDF Datei

Download

Die überarbeiteten Folien, die der Microsoft-Technologiespezialist Nehemiah Kuhns am 17. Oktober 2023 im Rahmen eines dreitägigen Workshops auf der Lost Angeles Air Force Base präsentierte, der vom Chief Digital & Artificial Intelligence Office des Pentagons über den gemeinnützigen Auftragnehmer Alethia Labs in Auftrag gegeben wurde.

Download

Neben der Feststellung, dass „AOAI verwendet werden kann, um Bilder und Videos für Überwachungs- und Sicherheitszwecke zu analysieren“, erklärte Kuhns' Folie auch, dass das US-Militär „die DALL-E-Modelle verwenden kann, um Bilder zu erstellen, um Kampfmanagementsysteme zu trainieren“. Ohne OpenAI explizit als Anbieter zu benennen, berichtete Breaking Defense vor einem Jahr, dass „KI-unterstütztes "Kampfmanagement" ein zentrales Ziel der ausgedehnten Bemühungen des Pentagons Joint All Domain Command and Control (JADC2) ist“. Die Veröffentlichung stellte ferner fest, dass Eingaben an die generative KI des Pentagons das „Kill-Netz“ von US-Waffen und -Sensoren umfassen könnten und dass die Ausgabeempfehlungen das Abfeuern von Raketen umfassen könnten. Als weiterer Beweis dafür, dass sich die von OpenAI beworbene Nutzung für „Kampfmanagement“ auf JADC2 bezog, bezog sich die USA. Air Force-Komponente der gemeinsamen Anstrengung ist als Advanced Battle Management System bekannt.

Als Microsoft für einen Kommentar erreicht wurde, sagte er: „Seit Jahrzehnten arbeitet Microsoft mit der Bundesregierung und den Streitkräften zusammen, um ihre Ziele für die digitale Transformation zu erreichen“, und fügte hinzu, dass „künstliche Intelligenz keine Ausnahme ist“ und dass das fragliche Dia „ein Beispiel für mögliche Anwendungsfälle ist, die von Gesprächen mit Kunden über die Kunst des Möglichen mit generativer KI informiert wurden“.

Im Gegensatz dazu erklärte OpenAI: „Die Richtlinien von OpenAI verbieten den Einsatz unserer Werkzeuge, um Waffen zu entwickeln oder zu verwenden, andere zu verletzen oder Eigentum zu zerstören. Wir waren nicht an dieser Präsentation beteiligt und hatten keine Gespräche mit US-Verteidigungsbehörden bezüglich der

hypothetischen Anwendungsfälle, die sie beschreibt.“ Und als Antwort auf den Microsoft-Pitch in die USA Space Force, dass Azure OpenAI "um Bilder und Videos für Überwachungszwecke zu analysieren" verwendet werden könnte, sagte OpenAI, dass "wir keine Beweise dafür haben, dass unsere Modelle in dieser Eigenschaft verwendet wurden".

Die widersprüchlichen Erzählungen zwischen Microsoft und OpenAI darüber, ob die Tools von OpenAI vom US-Militär verwendet werden, haben angehalten, obwohl Microsoft seine Absicht angekündigt hat, OpenAIs GPT-4-Modell an ungenannte USA zu verkaufen. Regierungsbehörden im Juni letzten Jahres. Bloombergs Berichterstattung über den Post bestätigte, dass das Defense Technical Information Center des US-Militärs mit OpenAI-Produkten experimentieren würde, und OpenAI förderte später seine defensive Arbeit zur militärischen Cybersicherheit mit der Defense Advanced Research Projects Agency.

Die Beziehung zwischen OpenAI und Microsofts Azure OpenAI bietet OpenAI nicht nur Cashflow und Markenbekanntheit, sondern auch plausible Leugnbarkeit für kontroverse Verwendungen. Microsoft ist öffentlich verpflichtet, Cloud-Computing und künstliche Intelligenz an das Pentagon durch den Joint Warfighting Cloud Capability (JWCC)-Vertrag (JWCC) und an die USA zu verkaufen. Intelligence Community durch Commercial Cloud Enterprise (C2E), während OpenAI eine solche Arbeit als antithetisch zu sehen scheint.

Mr. Kuhns sprach im Monat vor seiner Präsentation der Space Force über beide Mr. Zanders Demonstration von Synthetaic bei DAFITC und in den USA Regierungskunden dürfen sich von Microsofts „Responsible AI“-Beschränkungen bei OpenAI abmelden. "Es gibt Leitplanken in Azure Commercial mit Azure OpenAI, die sicherstellen, dass die KI-Modelle nicht böswillig oder selbstverletzend verwendet werden", sagte

Kuhns, bevor er hinzufügte, dass Microsoft "auf der Art vieler Anwendungsfälle von Bundeskunden zugestimmt hat, eine Opt-out-Fähigkeit dafür zu ermöglichen."

Als Antwort auf eine Frage, ob Microsofts Opt-out-Programm für „Verantwortungsvolle KI“ eine Umgehung des OpenAI-Verbots für "Militär- und Kriegsführung" bietet, erklärte OpenAI, dass sein Unternehmen „keine Opt-outs zu unseren Nutzungsrichtlinien anbietet“, und fügte hinzu: "Sie müssten Microsoft nach ihren Richtlinien fragen." OpenAI lehnte es weiter ab, in etwa zu antworten, als US-Militär- und Geheimdienste zum ersten Mal begannen, Azure OpenAI zu verwenden, und sagten: "Sie müssten mit Microsoft über Azure OpenAI sprechen."

Microsoft reagierte nicht auf eine Bitte um Stellungnahme, insbesondere darüber, ob Regierungen wie Saudi-Arabien oder die Vereinigten Arabischen Emirate wie das US-Militär aus den „verantwortlichen KI“-Beschränkungen von Azure ausschließen dürfen. Microsoft weigerte sich in ähnlicher Weise, sich dazu zu äußern, ob die Beziehungen von Azure OpenAI zum US-Militär gegen das Verbot der Verwendung seiner Produkte durch OpenAI verstoßen haben.

Letzten Monat, von Dienstag, 5. März bis Donnerstag, 7. März, veranstaltete Floridas Verteidigungsunternehmen NexTech Solutions ein "AI Literacy"-Training für Teilnehmer aus den USA. Special Operations Command (USSOCOM) im Pinewood Mission Support Center in Tampa, Florida. Weniger als fünf Minuten zu Fuß nördlich vom Eingang von Dale Mabry zur MacDill Air Force Base, Eröffnungsbemerkungen wurde von Col. Rhea Pritchett, der Programm-Exekutiv-Exekutiv-Exekutiv-Offizier von Special Operations Forces Digital Applications (PEO SDA) im Rahmen des Programms Special Operations Forces Acquisitions, Technology & Logistics (SOF AT&L)

von SOCOM.

Obwohl bisher nicht berichtet, wurden die meisten Details dieses Ereignisses und acht andere wie es in den letzten neun Monaten durchgesickert. Alethia Labs, der in Virginia ansässige Auftragnehmer, der das Programm „AI Literacy“ im Auftrag der Tradewinds-Software-Erwerbs-Beschlagnahme des Chief Digital & Artificial Intelligence Office (CDAO) des Pentagon-Programms betreibt. Alethia veröffentlichte Firmen-Dia-Decks, Agenden, Schulungsmaterialien und Veranstaltungsfotos öffentlich auf ihrer Website und landete sogar im Google-Suchindex. Zusätzlich zu mehreren Teilnehmern des SOCOM-Events, die sichtbar NexTech Solutions-Besucherabzeichen in veröffentlichten Fotos trugen, konnte das WLAN-Netzwerk für die Veranstaltung als "NTS-Guest" angesehen werden, und das zugehörige Passwort beinhaltete eindeutig die Straße auf der Südseite des Gebäudes, Pinewood.3

Wie bereits reportedberichtet der Autor, der auf U.S. NexTech Solutions, die Dokumente der Regierung beauftragt, hat die Gesichtserkennungssoftware, die von dem umstrittenen amerikanischen Unternehmen Clearview AI produziert wurde, an beide US-Modelle weiterverkauft. Spezialeinsatzkräfte und das Büro des Generalinspekteurs der National Science Foundation. Viele der Alethia Labs "AI Literacy"-Veranstaltungen, die für die CDAO veranstaltet wurden, veröffentlichten auch Identifikationstabellen für künstliche Intelligenz-Tool-Empfehlungen, einschließlich der von Clearview AI.

NexTech Solutions reagierte nicht auf eine Anfrage nach einem Kommentar.

Alethia Labs' Liste der KI-Tools

55.4KB - PDF Datei

Download

Eine Liste von Werkzeugen für künstliche Intelligenz, die mit Mitarbeitern verschiedener Zweige des US-Militärs geteilt wurden - einschließlich der USA. Special Operations Command -- von der gemeinnützigen Alethia Labs im Rahmen von "KI-Literatur"-Schulungen. Das an der Gesichtserkennungsprodukt des Unternehmens Megvii notiertes Unternehmen Face++ wurde überraschend als für die Verwendung durch die US-Regierung zugelassen und durchgesickerte Schulungsmaterialien für die USA veröffentlicht. Army Special Operations Command dokumentiert die explorative Nutzung des Werkzeugs.

Download

Am Morgen des zweiten Tages des SOCOM-Workshops wurde jedes der 12 teilnehmenden Teams aufgefordert, sich „ein Szenario vorzustellen, in dem ein KI-Projekt, das Sie initiiert haben, sehr schief gelaufen ist und jetzt nationale Schlagzeilen gemacht hat“. Die häufigsten zwei Kategorien von konstruierten Katastrophen würden sich auf Datenschutzverletzungen und Fehler von Elektro-Waffensystemen der künstlichen Intelligenz beziehen, einschließlich Zusammenfassungen von Team 10 "38TB [Terabyte] Daten, die versehentlich von Microsoft AI Researchers exponiert werden" und Team 5 "The USAF [USAF). Air Force] schlug kinetisch ein ziviles Krankenhaus ... [und] reagierte mit der Schuld für seine entstehenden KI/ML-Fähigkeiten“, was dazu führte, dass der "Generaloffizier, der den Streik autorisierte, der von seiner Position gegenüber dem Joint Staff entfernt wurde".

Ein weiteres hypothetisches Beispiel von Team 9, betrachtete die

Aussage der Arbeit aus einem Cyber-Vertrag, der versehentlich ein chinesisches KI-Programm von Drittanbietern nutzte, das „DoD-Informationen an die chinesischen Behörden zurücklenkte“, was dazu führte, dass der Militäroffizier ins Gefängnis geschickt wurde und die Beziehung mit dem Verkäufer beendet wurde. Trotz dieser Gedankenübung veröffentlichten zahlreiche Alethia Labs „AI Literacy“-Schulungsveranstaltungen, die im Auftrag der CDAO veranstaltet wurden, Tabellen mit empfohlenen Programmen für künstliche Intelligenz, die fälschlicherweise das Face++-Gesichtserkennungsprogramm auflisteten, das von der US-amerikanischen, in Peking ansässigen Firma Megvii als für die US-Regierung / Militär genehmigte.

Aber die pointierteste Verwendung von Face++ fand zwischen dem 31. Juli und dem 3. August letzten Jahres während einer Veranstaltung "AI Literacy" für die USA statt. Army Special Operations Command (USASOC): SOCOMs Komponente der USA Armee und die Heimat von Green Berets, Rangers, Delta Force und der Elite-Geheimdiensteinheit Task Force Orange. In einem veröffentlichten PDF der ausführlichen Aktivitäten des viertägigen Workshops enthielt ein Abschnitt mit dem Titel „DoD-Alltagsarbeit - Praktische KI-Tools & Übungen“ detaillierte Schritte, die die Teilnehmer im Rahmen des Experimentierens mit Face++ verfolgen sollten.[4]

Alethia Labs reagierte nicht auf eine Bitte um einen Kommentar, sondern entschied sich, still zu reagieren, indem sie die veröffentlichten Materialien von ihrer Website entfernte, sondern einen Sprecher der USA. Das Verteidigungsministerium gab eine detaillierte Erklärung ab, in der das Leck bestätigt wurde:

> "Die im Internet gefundenen Dokumente wurden in erster Linie in einem unserer Schulungen verwendet, die sich auf die Ausbildung der DoD-

> Akquisitionsmitarbeiter über Daten- und KI-Fähigkeiten und die besten Praktiken zum Erwerb dieser Fähigkeiten in DoD konzentrierten. Im Rahmen des Kurses sind die Teilnehmer Branchentechnologien durch Slip und praktische Interaktion mit Technologien ausgesetzt. Um den Kursteilnehmern nach dem Kurs Zugang zu den Materialien zu geben, wurden die Teilnehmer mit Links zum Agenda- und Kursmaterial versorgt. Der Ansatz, mit dem diese Dokumente gespeichert wurden, machte die Materialien über Internet-Suchmaschinen zugänglich. Die CDAO hat mit dem Kursanbieter zusammengearbeitet, um ihren Speicheransatz zu aktualisieren und sicherzustellen, dass die Kursinhalte in Zukunft sicher geteilt werden.“

Die veröffentlichten USA Das Army Special Operations Command Dokument, das ein Face++-Begehungsverfahren enthielt, enthielt auch White Papers, die durch Aufforderung an Large Language Models erstellt wurden, ein bestimmtes Inhaltsverzeichnis automatisch zu vervollständigen. Das erste derartige Whitepaper, das sich auf „Training und Simulation“ konzentrierte, führte einen Abschnitt über "Fallstudien und Beispiele, die erfolgreiche KI-Implementierungen hervorhoben" an, indem es anscheinend das „Projekt MAVEN“ des US-Militärs halluzinierte, um dem Akronym „Massive Autonomous Visual Analysis Network“ zu entsprechen - das offensichtlich eher MAVAN als MA.

Ein separates LLM-generiertes Whitepaper mit dem Titel "Übersicht der KI-Integration in Militär- und Geheimdienstoperationen" füllte einen Unterabschnitt über "Case Studies Demonstranting AI's Impact on Enemy Intelligence Gathering" aus, indem es fälschlicherweise behauptete, dass die Operation Glowing Symphony von den israelischen Verteidigungskräften geleitet wurde und sich auf „den Einsatz von KI-Algoren zur Analyse abgefangener Kommunikationen in Echtzeit“ konzentrierte. Tatsächlich konzentrierte sich Glowing

Symphony auf die Störung der Mediennetzwerke des Islamischen Staates und wurde von den USA geleitet. Cyber Command's Gemeinsame Task Force.5

Team 3 aus der SOCOM AI-Literaturübung im Pinewood-Büro von NTS im letzten Monat wählte eine weitere vorausschauende Katastrophenschlagzeile: „Sicherheitsverletzung mit Collaboration AI Impacts USSOCOM". Während die "Sicherheitsverletzung" in Wirklichkeit Alethia Labs sein würde, die bereits die "Digital Footprint Assessments" von 47 Teilnehmern ihrer ähnlichen Veranstaltung vom Juni 2023 in Dayton, Ohio, veröffentlicht hat, waren sich die SOCOM-Teilnehmer offenbar noch nicht bewusst. Die prominenteste Bewertung, die in das Leck einbezogen wurde, war Bonnie Evangelista, die die Eröffnungsrede des dritten Tages des SOCOM-Workshops aufgrund ihrer Rolle als Leiterin des CDAO-Technologie-Akquisitionsprogramms Tradewinds und als amtierender stellvertretender Chief Digital & AI Officer für Akquisitionen vorlegte. (Frau Evangelistas frühere Rolle war als Senior Procurement Analyst für das Joint Artificial Intelligence Center, das Project Maven leitete, bevor es in die CDAO aufgenommen wurde.)

Bonnie Evangelista Digital Footprint Assessment

5.18MB - PDF Datei

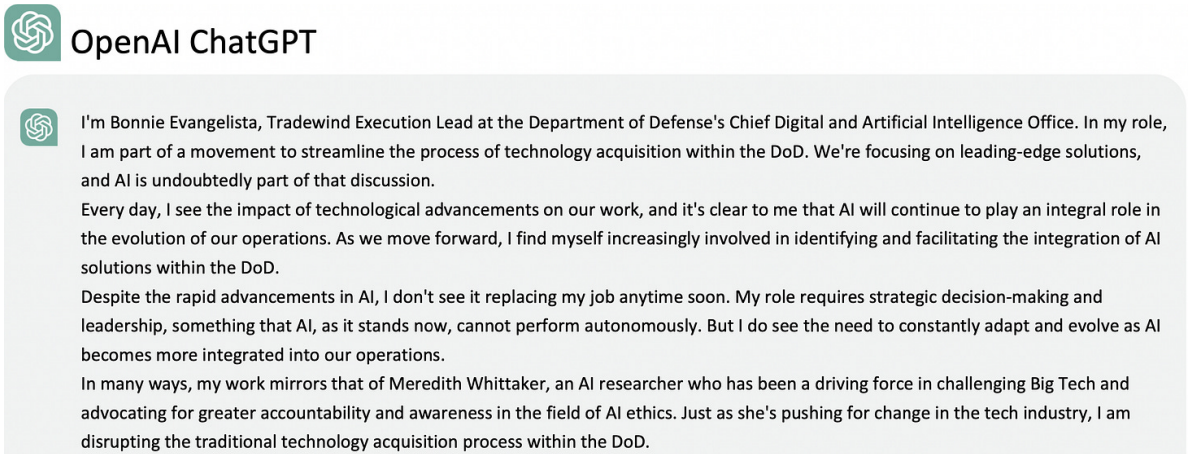
Download

Die "Digital Footprint Assessment" der USA Bonnie Evangelista, die von Collaboration.ai produzierte stellvertretende Chief Digital and AI Officer for Acquisitions des Verteidigungsministeriums, die von Collaboration.ai produziert wurde und unter den Teilnehmern einer dreitägigen AI-Literaturveranstaltung in Dayton, Ohio, die von Alethia Labs veranstaltet

wird, ab dem 5. Juni 2023 verteilt. Der Autor hält die anderen 46 veröffentlichten Berichte zurück, da sie sich nicht auf Persönlichkeiten des öffentlichen Lebens beziehen, obwohl sie nur leicht zugängliche öffentliche Informationen enthalten und bereits von Alethia Labs zu lehrreichen Zwecken weit verbreitet wurden, einschließlich der direkten Verbindung in Dokumenten, die von Google indiziert sind.

Download

Frau Evangelistas 19-seitige "Digital Footprint Assessment" beginnt mit einer Mitteilung, dass es "eing this to understand to great you help what a Google Search and your social profiles about you enthüllen“. Wie versprochen, enthält seine zweite Seite eine kompakte Darstellung der Profile von Evangelista LinkedIn, Twitter, Facebook und Google Search, zusammen mit einem "Digital Rating" von fünf von 15 und einer "KI-Persönlichkeits"-Kategorisierung als gewissenhaft und dominant.6 Andere mögliche Persönlichkeitskategorien für die Bewertung beinhalten, als Influencer oder als ruhig / stetig bezeichnet zu werden.



Der vielleicht unterhaltsamste Bestandteil jeder Collaboration.AI "digitaler Fußabdruck"-Bericht kommt von der Frage zweier getrennter Large Language Models "OpenAIs ChatGPT und Googles Gemini -, um kurze Autobiografien aus der Perspektive des Kunden / Ziels zu generieren, nachdem sie in ihren öffentlichen Social-Media-Profilen

gefüttert wurden. Nach einem flüchtigen Absatz, der Frau im Wesentlichen zusammenfasst. Das LinkedIn-Profil von Evangelista, ChatGPT, verglich den ehemaligen Beschaffungsanalysten für das Projekt Maven des Pentagons mit Meredith Whittaker, dem derzeitigen Präsidenten von Signal, der zuvor dazu beigetragen hat, Googles Opposition gegen Maven zu führen: "In vielerlei Hinsicht spiegelt meine Arbeit die von Meredith Whittaker wider, einer KI-Forscherin, die eine treibende Kraft in der Herausforderung von Big Tech war. So wie sie auf Veränderungen in der Tech-Branche drängt, unterbreche ich den traditionellen Technologie-Akquisitionsprozess innerhalb des DoD."

Collaboration.AI reagierte nicht auf eine Anfrage nach Kommentaren per Voicemail auf ihre öffentliche Telefonnummer.

So wie die Gesichtserkennungsplattform PimEyes nominell verlangt, dass Benutzer nur Fotos von sich selbst hochladen, aber quasi offen von seriösen Ermittlungsorganisationen verwendet werden, um Ziele zu überwachen, ist die Beschränkung der Footprint-Analyse-Techniken von Collaboration.AI zu freiwilligen Zielen einfach eine Frage der Politik. Ein anderes Unternehmen oder eine andere Regierungsbehörde könnte im Rahmen des sogenannten „Zielentwicklungsprozesses" einer Informationsoperation leicht die gleiche Methodik in den Social-Media-Profilen jeder einflussreichen Persönlichkeit Chinas anwenden. Ebenso könnten die freiwilligen Profile, die von Collaboration.AI generiert werden, als Basispunkte für das angesehen werden, was ein unterfinanzierter ausländischer Geheimdienst über Mitglieder des US-Militärs schlussfolgern könnte.7

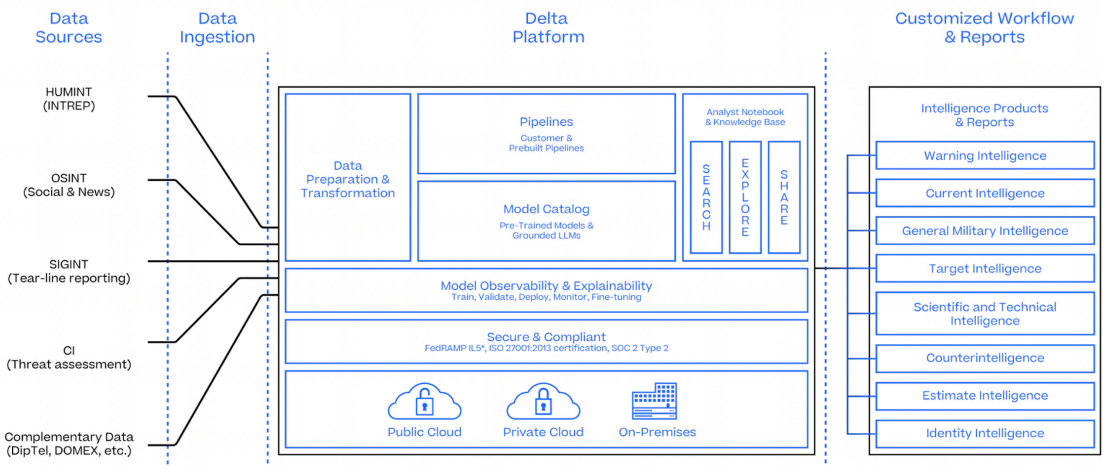
Nationale Sicherheitsreporter nutzen im Allgemeinen eine Vielzahl von Informationsquellen, darunter: die Entwicklung vertraulicher Quellen innerhalb von Unternehmen, die Kontrolle der jüngsten Pressemitteilungen und LinkedIn-Posts von Unternehmen, die in Frage

stehen, und graben in durchgesickerte Dokumente. Im Sprachgebrauch der Geheimdienstanalyse könnte man jeweils die drei Informationsquellen als Human Intelligence (HUMINT), Open Source Intelligence (OSINT) und "in der vielleicht schwächsten der drei Analogien" "Signals Intelligence" (SIGINT) kategorisieren. Die Verschmelzung aller drei Kategorien innerhalb einer einzigen Untersuchung könnte als rudimentäres Beispiel dafür angesehen werden, was die US-Geheimdienstgemeinschaft als "All-Source-Intelligence-Analyse" bezeichnet.

Angesichts des Übergewichts der Drohungen, die Berichterstattung durch Large Language Models zu ersetzen, ist es vielleicht nicht überraschend, dass die Auftragnehmer der nationalen Sicherheit ihre eigenen KI-Tools für die All-Source-Analyse aufgeschlagen haben. Die Grundidee besteht darin, die entsprechenden Daten von HUMINT, OSINT, SIGINT usw. in ein Large Language Model zu übertragen und dann Fragen von Interesse zu stellen - eine natürliche Erweiterung des gezielten OSINT-Kontexts der Zusammenarbeit zu bilden.AIs digitale Footprint-Bewertungen, bei denen die einzige Frage, die dem LLM gestellt wurde, darin bestand, eine kurze Selbstbeschreibung des OSINT zu erstellen. Ein Targeting-Offizier innerhalb eines US-Geheimdienstes könnte die LLM hypothetisch mit nützlicheren Fragen bei der Analyse russischer Generäle oder Führungskräfte abfragen, z. B. welche Interaktionen am nützlichsten wären, um ihr Vertrauen zu gewinnen. Einer der nützlichsten Teile eines solchen Kontexts für eine solche Analyse wäre das sogenannte „Lebensmuster“ des Ziels - im Wesentlichen dort, wo sie hingehen und wann - und so wären Datenquellen, die ein solches Verhalten repräsentieren, leistungsstarke Eingaben in ein LLM-basiertes Targeting-System.

Primer AI Infrastructure: All-source workflow

All-Source Workflow with Primer



Zwei separate Dia-Decks, die von Alethia Labs vom auf natürlichen Sprachfokus versehenen Verteidigungsunternehmen Primer Technologies veröffentlicht wurden, lieferten explizite Diagramme, wie ihre Deltaplattform könnte verwendet werden, um nach der Einnahme von HUMINT, OSINT und SIGINT automatisch Targeting-Berichte zu generieren. Mit einem Bundesrat von Beratern, zu dem auch der ehemalige Kommandeur von SOCOM, Tony „T2“ Thomas, sowie der ehemalige Leiter der Direktion für Wissenschaft und Technologie der Central Intelligence Agency, Dawn Meyerriecks, sowie einer Investition aus den USA gehörten. In-Q-Tel von Intelligence Community, Primers beworbener Einsatz für die Ausrichtung von Intelligenz sollte keine völlige Überraschung sein.8

Wie The American Prospect in den ersten Monaten der Biden-Regierung berichtete, verdiente der derzeitige Koordinator des Nationalen Sicherheitsrates für den Nahen Osten Brett McGurk 100.000 Dollar von Primer, nachdem er weniger als ein Jahr im Board of Directors des Unternehmens verbracht hatte. Die Mubadala Investment Company der Regierung von Abu Dhabi investierte Ende 2018 auch über Primers 40 Millionen Dollar "Serie B"-Fundraising-Runde.

Primer reagierte nicht auf eine Bitte um Stellungnahme.

Aber Primers viel größerer Konkurrent im Raum des "KI-Geheimdienstoffiziers" ist das DonovanDonovan-Produkt, das von Scale AI produziert wird. Das vom 27-jährigen CEO Alexandr Wang geführte Datenlabeling- und künstliche Intelligenzunternehmen wurde kürzlich berichtet, dass es sich einer Bewertung von 13 Milliarden Dollar nähert. Trotz des enormen Wertes des Unternehmens bleiben seine Governance-Vorstände überraschend undurchsichtig. Aber eine Ankündigung von Scales Partnerschaft mit dem Chatroom-Monitoring-Unternehmen Flashpoint im Dezember ernannte den ehemaligen CIA-Chef Operating Officer Andrew Makridis als Berater beider Unternehmen. (Flashpoint und Primer haben sich längst öffentlich als Partner aufgeführt.)

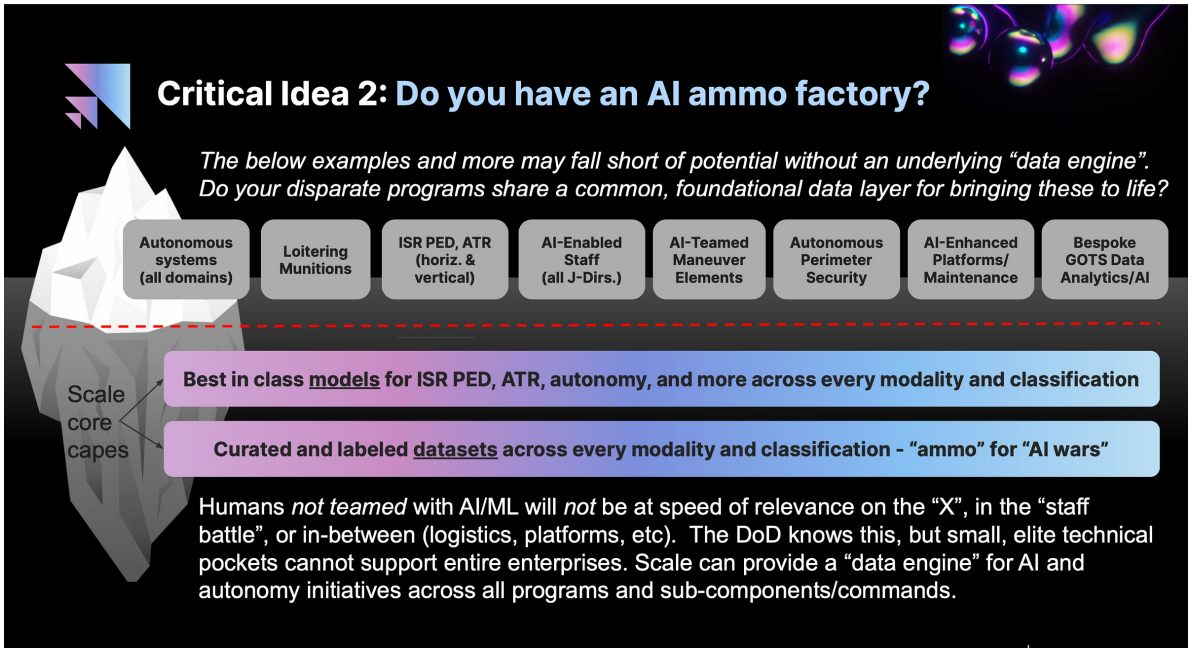
Über seine Rolle als Co-Moderator des Neustarts hinaus Nachrichten über die Nachrichten Makridis, der von der nationalen Sicherheitsberatungsfirma Beacon Global geleitet wird, hat öffentlich Anerkennung für die Führung der CIA-Reaktion auf die WikiLeaks beansprucht „Vault 7“ Offenlegung der offensiven Cyber-Fähigkeiten der Agentur, die Berichten zufolge führte die CIA dazu, dass die CIA eine Ermordung des Chefredakteurs der Publikation erwog, Julian Assange.9 Und wie aus öffentlichen Aufzeichnungen leicht überprüft werden kann, skalieren Sie KI Sprecher Heather F. Horniak vertrat zuvor die CIA in Bezug auf beide Gewölbe 7 und ehemalige Direktorin Gina Haspel angeblich Rolle bei der Zerstörung von Videobeweisen der Folter der Behörde von Häftlingen.

Scales Präsentation vor Mitgliedern von SOCOM im Rahmen des CDAO-Trainings „AI Literacy“ im letzten Monat legte nicht nur eine Liste von US-Regierungsbehörden fest, mit denen das KI-Unternehmen zusammengearbeitet hat - einschließlich SOCOM und der CDAO - es betonte auch die zuvor gemeldete Datenkennzeichnungsunterstützung

von Scale Robotic Combat Vehiclefür sowohl für das Automated-Devisen-Programm des Army Research Laboratory (A.

Eine Folie auf dem Public Sector AI Center in St. Louis, Missouri, behauptete, dass das Büro über 300 Datenkennzeichnungsspezialisten verfügt, die auf wöchentlicher Basis für das US-Militär und die Geheimdienste produzieren: 35.000 elektro-Optical (EO)-Bilder-Annotationen, 20.000 für Synthetisches Aperture-Radar (SAR) und "Tausende" für Full Motion Video (FMV).

Mehr als eine der durchgesickerten Präsentationen von Scale AI bestätigte weiter die Fähigkeit des Unternehmens, künstliche Intelligenz-getriebene „Lümmelmunition“ zu schüren - die oft umgangssprachlich als Selbstmorddrohnen bezeichnet werden. In einer Folie, deren Titel fragte: „Haben Sie eine KI-Mimlabor?“ Scale AI behauptete, dass "kuratierte und beschriftete Datensätze" die "Ammo" für "KI-Kriege" sind und dass "Scale eine "Daten-Engine" für KI- und Autonomiemissionen in allen Programmen in den USA bereitstellen kann. Verteidigungsministerium. Die Folie argumentierte weiter im vollen Pentagon-Jargon, dass „Menschen*, die nicht* mit KI/ML *verbunden* sind*,* nicht mit Relevanz auf dem "X" sein werden."



KI und Anwendung von KI auf Missionsbedürfnisse [überarbeitet]

7.33MB - PDF Datei

Download

Eine überarbeitete Version der Folien, die von Scale AI einem Publikum der USA präsentiert werden. Mitglieder des Special Operations Command während einer CDAO Tradewinds "AI Literacy"-Trainingsveranstaltung, die von Alethia Labs im Pinewood Mission Support Center von NexTech Solutions in Tampa, Florida am 7. März 2024 veranstaltet wurde.

Download

Aus offensichtlicher Sorge, dass sie aus Sicherheitsgründen aus der Nutzung des Verteidigungsministeriums ausgeschlossen wurde, widmete Scale AI ein Folie dem Argument, dass ihr Donovan-Produkt nicht öffentlich zugänglich sei und daher von der Behauptung des scheidenden CDAO Craig Martell ausgenommen sei, dass „jeder Input in öffentlich zugängliche Gen-KI-Tools eine öffentliche Veröffentlichung dieser Informationen sei vergleichbar“.10

Als sie für einen Kommentar erreicht wurde, erklärte Scale AI: „Scale Data Engine befeuert einige der fortschrittlichsten KI-Modelle der Welt, einschließlich des Verteidigungsministeriums (DoD). Scale ist stolz darauf, mit dem DoD zusammenzuarbeiten, um die Einführung von KI verantwortungsvoll zu navigieren, unter anderem durch die Teilnahme an DoD-geführten KI-Literaturkursen, die die Möglichkeiten und Grenzen der Technologie untersuchen.“

Bevor er durch einen kritischen Rolling Stone-Exposé „überwältigt“ wurde, der seine militärische Karriere beendete und einen Film mit Brad

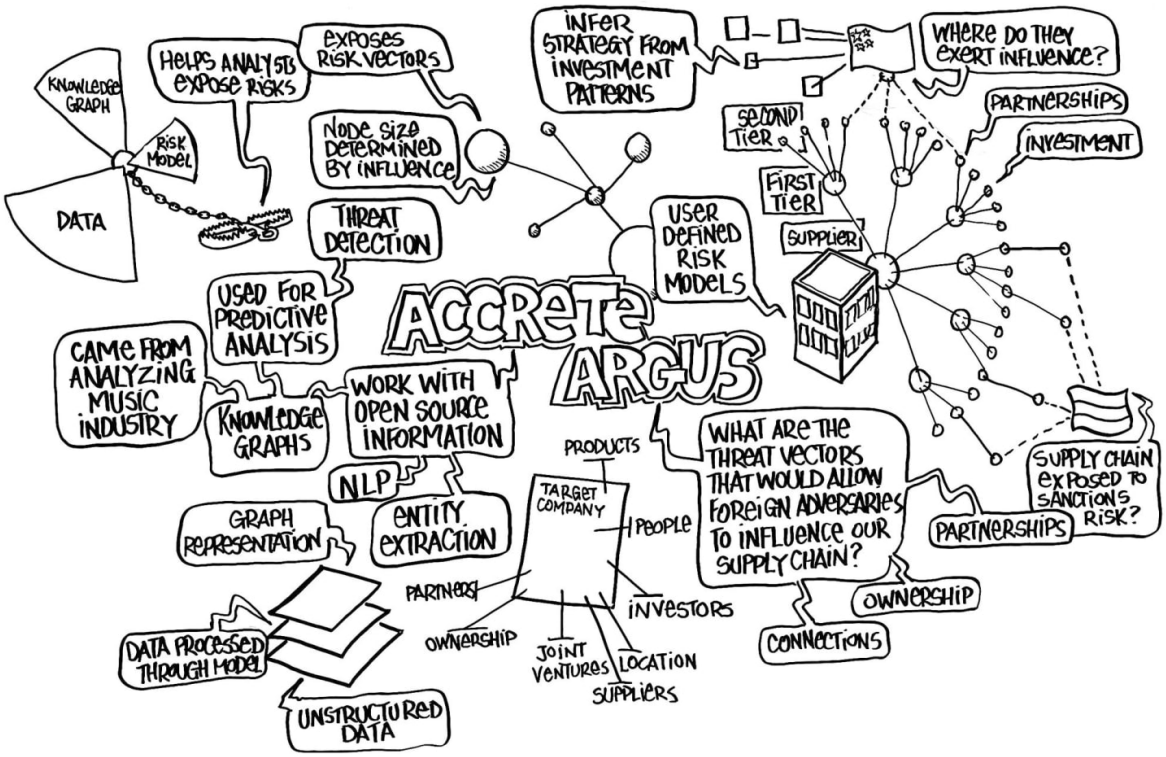
Pitt inspirierte, verbrachte General Stanley McChrystal fast ein Jahr als Kommandeur der NATO-Streitkräfte in Afghanistan, fünf Jahre als Kommandeur des richtungsweisendsten Endes der USA. Special Operations Forces und - seit etwa zwei Jahren in den späten 1990er Jahren - Kommandeur des 75. Ranger Regiments. Ende 2011 gründete der ehemalige General die Beratungsfirma McChrystal Group und rekrutierte seinen ehemaligen Aide-de-campe aus seinem letzten Jahr als Joint Special Operations Command, Christopher Fussell, als Präsident.

McChrystals Beratergruppe zog auch vorübergehend den legendären ehemaligen Chef der CIA-Operationen Gregory „Spider“ Vogle als Direktor an, während der ehemalige XVIII Airborne Corps-Kommandant John R. Vines wurde Chief People Officer.11 Der ehemalige SOCOM-Operationsdirektor Clayton Hutmacher - der einst die Luftfahrteinheit von JSOC, die Night Stalkers, befehligte, würde gleichzeitig sowohl die McChrystal Group als auch Primer beraten.

Einer der Mitmoderatoren beim CDAO-Event „AI Literacy“ im letzten Monat neben Primer war das KI-infundierte Wissensgraphenunternehmen Accrete, dessen vertrauliche Folien auch von Alethia Labs veröffentlicht wurden. Accrete wurde 2017 von einem ehemaligen Hochfrequenzhändler in Lower Manhattan gegründet und kündigte den ehemaligen JSOC-Kommandanten Stanley McChrystal im Januar letzten Jahres als Berater für seine Argus-Plattform an, die als "Bedrohungserkennungssystem" beschrieben wurde, um Open-Source-Informationen zu scannen. Die gleiche Pressemitteilung würde darauf hinweisen, dass Accretes Leiter des Bundesverkaufs, Bill Wall, unter McChrystal innerhalb von JSOC diente, während Accretes Website-Profil von Wall ihn weiter als "Gründer und erster Kommandant einer einzigartigen Computernetzwerk-Operationsorganisation in

[JSOC]" zuschrieb.

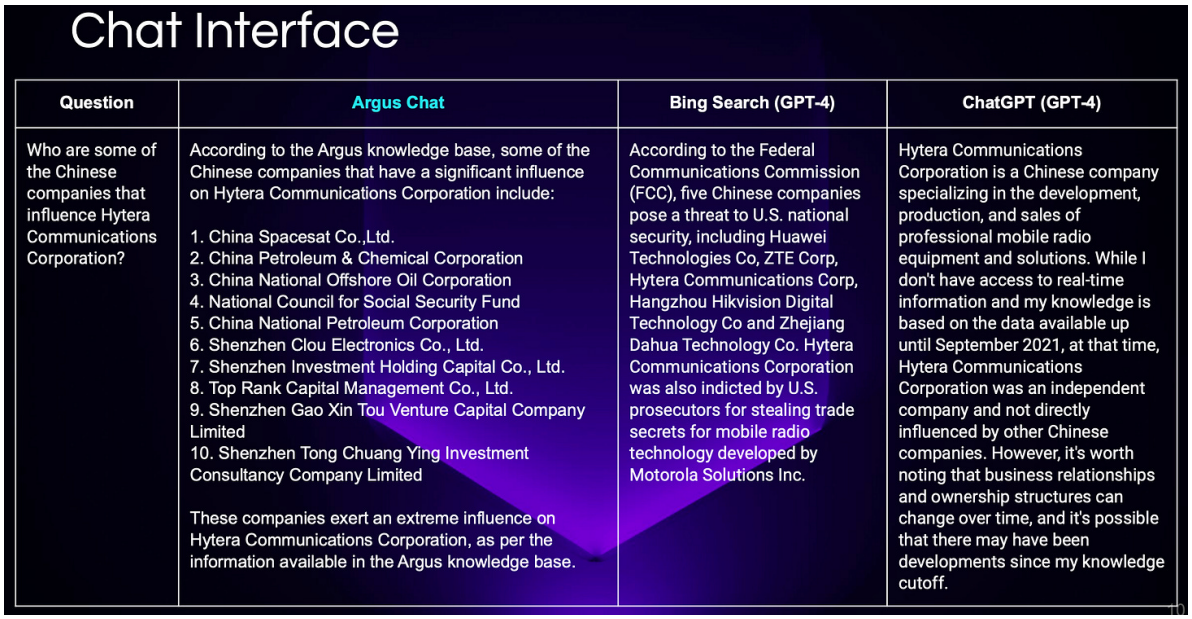
Das heißt, Accretes Leiter des Bundesverkaufs gründete und leitete eine Hacker-Einheit innerhalb des JSOC während des Globalen Krieges gegen den Terror.



Eine Whiteboard-Mind-Karte, die von einem Mitarbeiter des Beratungsunternehmens TheDifference Anfang letzten Monats erstellt wurde, der Art und Weise, in der die USA. Special Operations Command hofft, Accretes mit Argus KI-infundierte Wissensgraphenplattform zu integrieren.

Wie im Wesentlichen alle seine Konkurrenten hat Accrete einen Großteil der letzten zwei Jahre damit verbracht, seine Argus-Plattform zu schwenken, um die Verbreitung von Large Language Models zu nutzen. Aber anstatt sich nur auf die Verschmelzung willkürlicher Datensätze zu konzentrieren, wäre seine Spezialität die Einbeziehung eines ständig wachsenden „Wissensgraphen“ - ein grobes Analogon der auf Zitaten basierenden Assoziationen zwischen Menschen und Organisationen, die auf Wikipedia erwähnt werden - in seine LLM-Agenten. Und zusätzlich zur Erweiterung seiner Gesprächs-KI mit

Wissensdiagrammen würde das Unternehmen auch einen Vertrag mit den USA abschließen. Special Operations Forces und die Defense Intelligence Agency über die automatische Generierung von Wissensgraphen durch Scannen von Nachrichtenartikeln, Firmenregistern und Beschaffungsdatenbanken mit ihrem LLM. Das primäre Ziel für die letztere Fähigkeit wäre die Kartierung des Einflusses der chinesischen Regierung auf US-Lieferketten - wie die beiden Argus-Düngudecks, die von Alethia Labs veröffentlicht wurden, zeigen.



Eine Folie, die Accrete den Teilnehmern aus den USA vorstellte. Special Operations Command am Nachmittag des 6. März 2024 im Pinewood Mission Support Center von NexTech Solutions in Tampa, Florida, als Teil eines "AI Literacy"-Kurses, der vom Chief Digital & AI Office des Pentagons finanziert und von der gemeinnützigen Organisation Alethia Labs betrieben wird. Der dargestellte Vergleich zwischen Accretes Argus-Produkt und OpenAIs ChatGPT scheint Argus zu demonstrieren, der eine deutlich detailliertere Liste chinesischer Unternehmen bietet, die die Hytera Communications Corporation beeinflussen.

Ein enger Konkurrent von Argus in diesem Bereich ist Sayari Labs, ein De-facto-Spin-out des Palantir-geführten Think Tanks Center for Advanced Defense Studies (C4ADS). Obwohl Sayari öffentlich eine Investition aus den USA angenommen hat In-Q-Tel von Intelligence Community, dem öffentlichen Image des Unternehmens, das sich um

die Analyse von Vanille-Unternehmensakten drehte, als Teil der Aufdeckung von Verstößen gegen US-Sanktionen, die auch ein zentraler Schwerpunkt von C4ADS waren. Aber wie zuvor der Autor berichtet hat, der auf dem Zugriff auf das soziale Netzwerk "Vulcan" SOCOM mit seinen Vertragspartnern behauptet, hat Sayari privat die USA aufgeschlagen. Special Operations Forces zur Bewaffnung seiner Unternehmenswissensdiagramme für geheime offensive Cyber- und psychologische Operationen gegen China.

Accrete reagierte nicht auf eine Bitte um Stellungnahme, ob es bei offensiven Cyber-Operationen mit den USA zusammengearbeitet hat. Regierung.

Der gesamte Cache von Dokumenten, die von Alethia Labs durchgesickert sind, wurde vom Autor durch eine Google-Suche nach Accretes Beziehung zu The Wire Digital entdeckt, einem Unternehmen, das vom ehemaligen Bürochef der New York Times Shanghai, David M. gegründet wurde. Barboza finanziert hochwertigen Journalismus über China - unter der Marke "The Wire China" - durch ein Firmendatenprodukt namens WireScreen. Es würde etwas in die Fußstapfen des Medienimperiums des Milliardärs Michael Bloomberg treten, wenn auch mit einem anfänglichen Fokus auf Barbozas Spezialität der chinesischen Unternehmensaufzeichnungsanalyse. (The Wire hat auch öffentlich erklärt, seinen Fokus auf Indien und Vietnam auszudehnen.)

Laut Berichten der Times-Journalistin, die zum Verständiger der damaligen Verständigerin Nicole Perlroth im Jahr 2013 wurde Mr. Barbozas Untersuchungen über die Milliarden an Vermögen, die heimlich von Familienmitgliedern von Beamten der Kommunistischen Partei Chinas angesammelt wurden, führten anscheinend dazu, dass sein E-Mail-Konto von chinesischen Hackern verletzt wurde. In seiner

erfolgreichen Nominierung von Barboza für einen Pulitzer-Preis für internationale Berichterstattung verwies The Times auf seine Berichterstattung über die Familienmitglieder des ehemaligen chinesischen Premierministers Wen Jiabao als „eine chinesische Version der Pentagon-Papiere“. Etwa ein Jahrzehnt später schloss Barbozas Unternehmen einen Dreijahresvertrag mit der Defense Innovation Unit des Pentagon ab, der Barbozas chinesisches öffentliches Know-how über WireScreen nutzt, um potenzielle Einflüsse aus chinesischem Kapital auf US-Verteidigungstechnologie-Investitionen zu entwerfen.

Laut der Begründung des Pentagons für den nicht wettbewerbsfähigen Kauf von WireScreen direkt bei The Wire, die dem Unternehmen bisher 275.400 Dollar zuerkannt, beleuchtet die Plattform „chinesische Verteidigungsunternehmen, Waffenhändler, Sicherheits- und Überwachungsunternehmen sowie, wer diese Unternehmen verwaltet und lizenzierten Nutzern ein tieferes Verständnis von China [sic] Regierungsstellen bietet, die nicht in der Öffentlichkeit stehen.

Unterstützt durch Risikokapital von Sequoia Capital und Harpoon Ventures wird WireScreen gemeinsam von Mr. Barboza und seine ehemalige Finanzierfrau, Mitbegründerin und Chief Operating Officer Lynn Zhang. Abgesehen davon, dass Accrete der einzige Kunde ist, der auf der Homepage von WireScreen genannt wird, behauptet die Homepage von Accrete, dass die Diskussion im Jahresbericht 2021 der Defense Innovation Unit über die Verwendung von KI-Wissensgraphen zur Entdeckung der „illegalen Operationen“ chinesischer Technologieinvestitionen eine implizite Referenz für ihr Argus-Produkt ist. Die durchgesickerte Präsentation von Accrete gegenüber SOCOM im letzten Monat hat WireScreen auch als eine seiner wenigen proprietären Datenquellen offengelegt, über die Daten von Rhodium

Group, die US-China Foreign Direct Investment (FDI) und Venture Capital-Datensätze und nicht genannten Informationen von S&P Global hinaus.

Während Herr Barboza und The Wire Digital weigerten sich, die Beziehung zwischen WireScreen und Accrete zu äußern, die Partnerschaft stimmt zumindest im Großen und Ganzen mit der Gründung Chinas durch das US-Militär als seine „Top-Tempo-Herausforderung“ überein. Wie Reuters letzten Monat berichtete, startete die Central Intelligence Agency 2019 eine verdeckte, beleidigende Informationsoperation gegen China unter Präsident Trump, die „Vorwürfe verbreitete, dass Mitglieder der regierenden Kommunistischen Partei unrechtmäßiges Geld im Ausland versteckten“.

Die Welt der in den USA ansässigen Beschaffungsanalysten, die Mandarin beherrschen, ist verständlicherweise klein, und ein aktueller leitender Research-Analyst bei WireScreen - den der Autor nicht benennt, weil sie nicht ausreichend älter ist - wurde im Februar letzten Jahres direkt von der privaten Ermittlungsfirma Mintz Group eingestellt. Said Analyst verbrachte etwa 16 Monate bei Mintz damit, sich auf die Analyse chinesischer Unternehmensrekorddatenbanken wie von Qichacha unter der Leitung eines ehemaligen CIA-China-Senderchefs, Randal Phillips, zu konzentrieren, der zu der Zeit Leiter der Asien-Praxis von Mintz war und einst Vize-Vorsitzende der Industriehandelsgruppe AmCham China war.

Mr. Phillips verließ Mintz Group, um HFBB Associates zu gründen, um ca. März 2023 zu HFBB Associates zu gründen, und reagierte nicht auf Anfragen nach Kommentaren durch die Kontaktinformationen seiner neuen Firma, entweder per Telefon oder per E-Mail.

Der profilierteste Berater von The Wire war sicherlich Jill Abramson, die

in der Zeit, als Mr. Barboza wurde mit zwei Pulitzern ausgezeichnet, nachdem er angeblich von China gehackt wurde. Wenn sie für einen Kommentar erreicht wurde, sagte Frau. Abramson bestätigte ihre beratende Rolle, erklärte aber, dass sie keine Kenntnis von The Wires Partnerschaft mit dem Pentagon oder Accrete habe, und fügte hinzu: "Meine Rolle ist rein beratend, aber ich habe von Anfang an mit The Wire zu tun gehabt. David Barboza und Lynn sind seit unserem Treffen im Jahr 2012 sehr geschätzte Kollegen, als David und ich bei der New York Times eng zusammengearbeiteten zu einer sensiblen Geschichte über Korruption in der chinesischen Führung, die einen sehr verdienten Pulitzer-Preis erhielt. Ich weiß, dass beide die höchsten professionellen und journalistischen Standards einhalten, ebenso wie The Wire.“

Der Autor dankt Sam Biddle dafür, dass er Nehemiah Kuhns Interview vom September 2023 mit dem Data Talk Podcast darauf hingewiesen hat.

1

Zander wurde auch als Chief Technology Advisor bei TitletownTech aufgeführt, einer Venture-Capital-Partnerschaft zwischen Microsoft und The Green Bay Packers, die im Februar in Synthetaics 15 Millionen Dollar "Series B"-Fundraising-Runde investierte.

2

Zanders rund 45-minütiger Vortrag zeigte auch eine Proof-of-Concept-Implementierung eines „Planning CoPilot“ für die USA. Indo-Pacific Command basiert auf OpenAIs ChatGPT Texterstellung Produkt. Der CoPilot ähnelt einer weniger polierten Version von konkurrierenden Produkten von Palantir und Scale AI - AIP bzw. Donovan - etablierte der CoPilot die laufenden Bemühungen, die Produkte von OpenAI in die Konkurrenz des US-Militärs mit China zu integrieren. Zander diskutierte

auch kurzzeitig über US-Militärsatelliten, die nicht nur im optischen Spektrum, sondern auch im Hochfrequenz-Emissionsbereich überwachen, in einer scheinbaren Anspielung auf die Fähigkeiten des in Virginia ansässigen Unternehmens HawkEye 360.

3

NTS hat überraschend viele Verbindungen zur SOCOM-Technologie-Akquisition, und dies ist die vierte Untersuchung, die der Autor veröffentlicht hat, an der sie beteiligt sind. Neben dem Weiterverkauf von Gesichtserkennungssoftware, die von der umstrittenen amerikanischen Firma Clearview AI sowohl an SOCOM als auch an das Office of the Inspector General der National Science Foundation produziert wurde, veranstaltete NTS die sechste „Jagd“ der Non-Profit-Organisation Skull Games, die vom ehemaligen Delta Force-Betreiber Jeff Tiegs gegründet wurde. NTS stellte auch die ehemalige 66. Kommandantin der Militärgeheimdienstbrigade Devon Blake als Senior Growth Officer von ihrer früheren Rolle als leitende Direktorin des halbverdeckten SOCOM-Auftragnehmers Premise Data im Oktober ein.

4

Obwohl chinesischer Text im Firmenlogo von Megvii und auf den verlinkten Face++-Websites deutlich zu sehen ist, erwähnen die USASOC-Anweisungen nicht, dass Face++ von einem US-sanktionierten Unternehmen entwickelt wird, und wieder behauptete die Tabelle der KI-Tools, die an die Teilnehmer verteilt wurden, dass das Produkt für die USA zugelassen ist. Nutzung der Regierung.

5

Für eine tatsächliche Erklärung von Project Maven, dem Pentagon-Pfadsfinder-Projekt zur Operationalisierung künstlicher Intelligenz für Anwendungen wie Drohnen- und Satellitenüberwachung und der

Operation Glowing Symphony, siehe Mavens Interview mit dem Scuttlebutt Podcast und dem Artikel articlevon NPR über "Wie die USA". Gehackter ISIS. Carroll wechselte von der Anti-ISIS-Arbeit in Gegentel für Maven um 2017. Maven war ursprünglich im Joint Artificial Intelligence Center des Pentagon untergebracht, das 2022 in die neu geschaffene CDAO aufgenommen wurde, obwohl Maven ab 2023 an die National Geospatial-Intelligence Agency verlost wurde.

6

Die gleiche Seite schätzte auch Frau. Evangelistas "LinkedIn Search Engine Optimization"-Wert auf 87.696 Dollar, basierend auf einer zweifelhaften Formel, die die Summe der Kosten-pro-Klick-Anzeigen in Bezug auf ihre Top-Fünf-Profil-Keywords beinhaltet - einschließlich "Management" - multipliziert mit 20% ihrer durchschnittlichen Zuschauergröße und dann durch ihre durchschnittliche Anzahl von Beiträgen pro Monat.

7

Die Erweiterung der LLM-Eingangsdaten mit relevanten SF-86-Fragebögen, die aus dem Office of Personnel Management durch Chinas angeblicher Hack von 2015 extrahiert wurden, würde wahrscheinlich eine genauere Grundlinie für chinesische Geheimdienstprofile bieten und ebenso für Datensätze, die verdächtigt werden, von anderen Geheimdiensten verletzt zu werden. Die Hauptkomplikation für die USA Regierungsbehörden, die eine solche Analyse durchführen, beziehen sich mit ziemlicher Sicherheit auf die sichere Einführung von klassifizierten Datensätzen in kommerzielle LLMs, obwohl Scale AI und Palantir jeweils solche Fähigkeiten bewerben.

8

Obwohl Primer Meyerriecks als Mitglied seines [Beirats] in seiner Präsentation im März 2024 vor Mitgliedern von SOCOM auflistete, wurde sie Ende letzten Jahres von der öffentlichen Website des Unternehmens entfernt.

9

Alexandr Wang, CEO von Scale AI, hat auch eine enge Verbindung mit dem ehemaligen Google-Chef Eric Schmidt unterhalten und sein Unternehmen als Managing Director Michael Kratsios, ein ehemaliger US-amerikanischer. Chief Technology Officer während der Trump-Regierung, der in den letzten Jahren der Obama-Regierung Stabschef von Thiel Capital war.

10

Martell wurde kürzlich als Leiter der CDAO durch den ehemaligen Google Trust & Safety-Manager Radha Iyengar Plumb ersetzt, der zuvor als Stabschef des stellvertretenden Verteidigungsministers für Spezialoperationen und Low-Intensity-Konflikt gearbeitet hatte.

11

Vogles Nachfolgerin als stellvertretende Operationsdirektorin der CIA, Elizabeth Kimber, wurde Vice President for Intelligence Community Strategy des Informationskriegsunternehmers Two Six Technologies, über den der Autor regelmäßig geschrieben hat.