Gli sconvolgenti abissi dell'intelligenza artificiale

geopolitika.ru/it/article/gli-sconvolgenti-abissi-dellintelligenza-artificiale

15 settembre 2024

16.09.2024

Leonid Savin

Sostituzione della realtà e sua analisi approfondita: i nuovi programmi sono in grado di farlo.

L'intelligenza artificiale è una di quelle tecnologie critiche che si stanno sviluppando rapidamente e la cui applicazione viene implementata in un'ampia varietà di campi. Tuttavia, ci sono casi in cui queste innovazioni non sono chiaramente benefiche, ma piuttosto utilizzate per scopi distruttivi.

Il primo esempio è legato alla sostituzione della realtà in Venezuela. Poiché c'è la possibilità concreta di essere condannati a una pena detentiva per aver incitato alle proteste, gli strateghi dell'opposizione hanno imparato un nuovo trucco per la manipolazione dei media: hanno creato presentatori virtuali di notizie come “Bestie” e “Buddy” per pubblicare rapporti critici nei confronti del governo sui social network. Questo approccio innovativo con avatar virtuali, che fa parte del progetto “Operation Retweet”, permette loro di dire quasi tutto, evitando le responsabilità. “Operation Retweet”, a sua volta, fa parte delle iniziative #VenezuelaVota e #LaHoradeVenezuela.

Per la prima volta, le informazioni al riguardo sono apparse il 16 agosto sulla CNN, che è il portavoce dei globalisti.

I video dell'“Operation Retweet” vengono pubblicati su piattaforme di social media come X (ex Twitter), YouTube, TikTok, Facebook e Instagram. Su queste piattaforme digitali, gli avatar dell'intelligenza artificiale condividono informazioni su argomenti di attualità in Venezuela. Il primo episodio, pubblicato il 14 agosto, è stato dedicato al numero di detenuti dopo le elezioni presidenziali e a come la crisi politica del Paese influisce sull'economia.

Ovviamente, tutto questo viene mostrato non dalla posizione dello Stato di diritto e della sovranità, ma dal punto di vista dell'opposizione e degli interessi del principale istigatore della crisi attuale: gli Stati Uniti. È molto probabile che il metodo stesso sia stato suggerito da sponsor del Dipartimento di Stato americano.

La strategia, in generale, è piuttosto innovativa, anche per quanto riguarda l'elusione delle responsabilità. Dopotutto, se un normale presentatore può essere perseguito penalmente per dichiarazioni chiaramente illegali, che dire di un avatar virtuale? Bisogna cercare il suo creatore, i giornalisti, i reporter e gli editori, il che complica chiaramente le azioni investigative.

Una situazione simile, ma con una dimensione leggermente diversa, è in aumento in Corea del Sud. Lì vi è un boom di *deepfake* erotici e pornografici generati dalle IA.

In un recente reato, diversi studenti delle scuole superiori di Busan hanno creato falsi pornografici di compagni e insegnanti della loro scuola e li hanno pubblicati in una chat di gruppo su KakaoTalk. Casi simili si sono verificati in circa 150 scuole medie e superiori in tutto il Paese. Secondo i post sui social media, casi simili si sono verificati in circa 150 scuole medie e superiori a livello nazionale. Ciò suggerisce un problema diffuso di crimini deepfake perpetrati da adolescenti abituati IA contenuti digitali.

Secondo le indagini di Hankyoreh, i crimini che coinvolgono i deepfake nelle unità militari hanno raggiunto livelli gravi. Si è appreso che alcuni dei deepfake che coinvolgevano le donne soldato utilizzavano fotografie di documenti d'identità e certificazioni ufficiali del Governo a cui si poteva

accedere solo sull'intranet dell'esercito. Poiché tale intranet è accessibile solo agli addetti IA lavori, ciò suggerisce che la portata di tali crimini è davvero ampia.

Ma il governo può fare ben poco, ed è per questo che il gruppo coreano per i diritti delle donne Womenlink ha affermato che le donne continuano a “vivere senza uno Stato”, perché non sentono più che il loro Paese fornirà loro la protezione necessaria.

Tuttavia, la realtà non fallisce solo a causa di teppisti, come in Corea del Sud, o di attivisti politicamente motivati, come in Venezuela.

Nell'agosto 2024, i principali funzionari elettorali di Michigan, Minnesota, New Mexico, Pennsylvania e Washington hanno inviato una lettera a Elon Musk, lamentando il fatto che il chatbot IA della piattaforma X, Grok, ha prodotto informazioni false sulle scadenze elettorali statali, poco dopo che il Presidente Joe Biden si era ritirato dalla corsa presidenziale del 2024.

I Segretari di Stato hanno chiesto che il chatbot indirizzi gli utenti che fanno domande relative alle elezioni a un sito web di informazioni sul voto. Elon Musk ha fatto delle anticipazioni alle richieste dei funzionari. È interessante notare che anche l'Alabama, l'Indiana, l'Ohio e il Texas sono stati citati nella diffusione di informazioni inaffidabili sui tempi del voto, sebbene non siano state ricevute lettere dalla leadership di questi Stati. Le false informazioni hanno continuato ad essere ripetute per 10 giorni. Il motivo per cui sono state fornite tali informazioni è sconosciuto.

Se questi casi illustrano una distorsione della realtà e la sua sostituzione, esiste anche l'approccio opposto: un'analisi approfondita e accurata dei dati. Teoricamente, può essere utilizzata in vari campi, ma ora viene sfruttata attivamente dall'esercito e dall'intelligence degli Stati Uniti.

Il direttore dei dati e dell'innovazione digitale presso la National Geospatial Intelligence Agency, Mark Munsell, ha dichiarato che la NGA ha recentemente iniziato ad addestrare gli algoritmi di intelligenza artificiale sul suo patrimonio unico di dati visivi e testuali. Nel corso di decenni, l'agenzia di intelligence statunitense ha accumulato grandi quantità di dati ben etichettati, ben organizzati e accuratamente controllati, compreso un archivio di immagini satellitari senza pari. Per elaborarli, l'agenzia ha dovuto dedicare molto tempo e coinvolgere un gran numero di persone. Ma ora questi archivi stanno cercando di combinarsi con i resoconti di persone accuratamente selezionate su ciò che vedono in queste immagini.

Esistono modelli linguistici di grandi dimensioni che operano esclusivamente sul testo: si addestrano sul testo, ricevono input nel testo e producono risposte come testo. Altre forme di intelligenza artificiale generativa possono correlare testo e immagini abbastanza bene da trasformare le richieste scritte degli utenti in immagini o addirittura in video.

E ora l'esercito e la comunità di intelligence degli Stati Uniti annunciano un nuovo approccio e la prossima frontiera: l'IA multimodale. La capacità cruciale consiste nell'incrociare diversi tipi di informazioni sulla stessa cosa, come un'immagine o un video con la relativa didascalia che lo descrive a parole, proprio come il cervello umano può associare un'idea o un ricordo alle informazioni provenienti da tutti i sensi.

Il responsabile del programma DARPA William Corvey, intervenuto al panel Intelligence and National Security Alliance (INSA), ha anche sottolineato che l'IA multimodale può funzionare anche con sensi che gli esseri umani non hanno, come le immagini a infrarossi, i segnali radio e radar o i sonar: “Immaginate sistemi cross-modali che possano conciliare informazioni visive e linguistiche e altri tipi di modalità di sensori che potrebbero essere disponibili per un robot ma non per un essere umano”, ha detto Corvey con ammirazione.

I moderni algoritmi di IA hanno dimostrato di essere perfettamente in grado di lavorare con immagini, video e tutti i tipi di dati dei sensori, non solo con il testo, perché possono astrarre tutti i dati nelle stesse rappresentazioni matematiche.

Pertanto, l'esercito americano sta cercando di utilizzarlo per portare i vari dati a un denominatore comune e a un targeting più chiaro. E questo approccio viene utilizzato ovunque.

L'FBI sta utilizzando la tecnologia abilitata all'IA per valutare le soffiate e garantire che siano identificate in modo accurato, classificate come prioritarie ed elaborate in modo tempestivo. L'Open Source Enterprise della CIA ha lanciato uno strumento interno di IA “in stile Chat-GPT” per consentire agli analisti di avere “un migliore accesso all'intelligence open-source”, e l'NSA ha aperto un “Centro di Sicurezza per l'Intelligenza Artificiale”, focalizzato sulla difesa “dell'IA della Nazione attraverso la collaborazione Intel-Driven con l'industria, il mondo accademico, l'Intelligence Community (IC) e altri partner governativi”.

Anche se le nuove tecnologie daranno presumibilmente un vantaggio alle forze di sicurezza americane, bisogna ricordare l'altra faccia della medaglia: tutte queste informazioni saranno utilizzate contro i potenziali avversari, che a Washington includono Cina, Russia e una serie di altri Paesi. E dal loro punto di vista, tale applicazione dell'intelligenza artificiale è anche distruttiva.

Articolo originale di Leonid Savin:

https://orientalreview.su/

Traduzione di Costantino Ceoldo