

Šokující propasti umělé inteligence

 zvedavec.news/komentare/2024/09/10218-sokujici-propasti-umele-inteligence.htm

Leonid Savin

10.9.2024 Komentáře Témata: AI 1039 slov

Umělá inteligence je jednou z těch kritických technologií, které se rychle rozvíjejí a uplatňují se v nejrůznějších oblastech. V některých případech však tyto inovace zjevně nejsou přijímány, ale spíše využívány k destruktivním účelům.

První příklad se týká nahrazování reality ve Venezuele. Vzhledem k tomu, že riziko uvěznění za podněcování k protestům je reálné, opoziční stratégové si osvojili nový trik manipulace s médii, a to vytvořením virtuálních zpravodajů, jako jsou Bestie a Buddy, kteří na sociálních sítích zveřejňují zprávy kritické vůči vládě. Tento inovativní přístup k virtuálním avatarům, který je součástí projektu „Operace Retweet“, jim umožňuje říkat téměř cokoli, a přitom se vyhnout odpovědnosti. Operace Retweet je součástí iniciativ #VenezuelaVota a #LaHoradeVenezuela.

Poprvé o ní informovala 16. srpna CNN, hlásná trouba globalistů.

Epizody Operace Retweet jsou vysílány na různých digitálních platformách, včetně X (dříve Twitter), YouTube, TikTok, Facebook a Instagram. Na těchto kanálech avataři umělé inteligence sdílejí informace o aktuálních tématech ve Venezuele. První epizoda, vysílaná 14. srpna, se zaměřila na počet zadržených osob po prezidentských volbách a na to, jak politická krize v zemi ovlivňuje ekonomiku.

To vše bylo samozřejmě ukázáno nikoli z hlediska právního státu a suverenity, ale z pohledu opozice a zájmů hlavních strůjců současné krize, tedy Spojených států.

Je pravděpodobné, že samotnou metodu navrhli sponzoři z amerického ministerstva zahraničí.

Strategie jako celek je poměrně novátorská, a to i z hlediska vyhýbání se odpovědnosti. Koneckonců, pokud může být za zjevně nezákonné výroky stíhán běžný moderátor, co teprve virtuální avatar? Je třeba vypátrat jeho tvůrce a vydavatele, což samozřejmě komplikuje vyšetřování.

Podobná situace, ale s trochu jiným rozměrem, nastala v Jižní Koreji. Dipfakes erotických a pornografických videí tam zažívají boom.

V jednom z nedávných případů několik žáků střední školy v Pusanu vytvořilo falešné pornografické snímky žáků a učitelů své školy a zveřejnilo je ve skupinové chatovací místnosti na KakaoTalk. Podobné případy se vyskytly na přibližně 150 středních školách po celé zemi. To naznačuje rozšířený problém krádeží identity teenagerů zvyklých na digitální obsah.

Podle vyšetřování, které provedl Hankyoreh, byly trestné činy padělání dokladů spáchány také ve vojenských jednotkách po celé zemi. Některé z těchto padělků, do nichž byly zapojeny vojákyně, využívaly průkazové fotografie a oficiální vládní dokumenty, do nichž bylo možné nahlížet pouze v interní armádní síti. Vzhledem k tomu, že přístup do této interní sítě mají pouze zasvěcené osoby, naznačuje to, že rozsah těchto trestných činů je velmi široký.

Vláda však může udělat jen málo, což vedlo korejskou skupinu pro práva žen Womenlink k prohlášení, že ženy „žijí bez státu“, protože již nemají pocit, že by jim jejich země poskytla potřebnou ochranu.

Realita však nesehává jen kvůli šikaně, jako v Jižní Koreji, nebo politicky motivovaným aktivistům, jako ve Venezuele.

V srpnu 2024 poslali vysocí úředníci v Michiganu, Minnesotě, Novém Mexiku, Pensylvánii a Washingtonu dopis Elonu Muskovi, v němž si stěžovali, že Grok, chatbot poháněný platformou umělé inteligence sociální sítě X (zablokované v Ruské federaci), poskytl nepravdivé informace o termínech hlasování ve státech krátce poté, co prezident Joe Biden odstoupil z prezidentského klání v roce 2024.

Státní tajemníci požádali, aby chatbot uživatele s dotazy týkajícími se voleb odkázal na webovou stránku s informacemi o volbách.

Elon Musk se vydal na schůzku s úředníky. Zajímavé je, že zavádějící informace o termínech hlasování se týkaly také Alabamy, Indiany, Ohia a Texasu, ačkoli žádný dopis od představitelů těchto států neexistoval.

Celkem byly nepravdivé informace vysílány deset dní. Není známo, proč byly tyto informace šířeny.

Zatímco ve výše uvedených případech jde o zkreslování a nahrazování reality, existuje i opačný přístup, který spočívá v hloubkové analýze údajů. Teoreticky jej lze použít v různých oblastech, ale v současné době jej aktivně využívá americká armáda a zpravodajské služby.

Mark Mansell, ředitel pro data a digitální inovace v Národní geoprostorové zpravodajské agentuře, nedávno oznámil, že agentura začala trénovat algoritmy umělé inteligence na základě svého jedinečného souboru vizuálních a textových dat. Americké zpravodajské služby za desítky let nashromáždily obrovské množství dat, z nichž velká část pochází ze satelitních snímků z vesmíru. Zpracování těchto dat vyžaduje mnoho času a velký počet pracovníků. Dnes se však objevují pokusy spojit tyto archivy s výpověďmi pečlivě vybraných osob o tom, co na těchto snímcích vidí.

Existují jazykové modely, které pracují výhradně s textem: trénují se na textu, přijímají data a vytvářejí odpovědi ve formě textu. Jiné formy generativní umělé inteligence dokážou text a obrázky propojit natolik dobře, že písemné dotazy uživatelů převádějí na obrázky nebo dokonce na videa.

Dnes se americká armáda a zpravodajská komunita hlásí k novému přístupu, který posouvá věci na další úroveň: multimodální umělá inteligence. Její nejdůležitější schopností je spojit různé typy informací o stejném objektu, například obrázků nebo video, s odpovídajícím popiskem popisujícím objekt, a to stejným způsobem, jakým lidský mozek dokáže spojit myšlenku nebo vzpomínku s informacemi ze všech smyslů.

William Corvey, ředitel programu DARPA, který vystoupil na konferenci US Intelligence and National Security Alliance, rovněž poznamenal, že multimodální umělá inteligence by mohla pracovat i se smysly, které člověk nemá k dispozici, jako jsou infračervené obrazy, rádiové a radarové signály nebo sonar. „Představte si multimodální systémy, které dokážou koordinovat vizuální a jazykové informace a další typy senzorů, které mohou být dostupné robotovi, ale nejsou dostupné člověku,“ říká s obdivem Corvey.

Moderní algoritmy umělé inteligence již prokázaly, že jsou schopny zpracovávat obrázky, videa a všechny druhy smyslových dat, nejen text, protože je dokáží převést do stejných matematických reprezentací.

Americká armáda se je proto snaží využít k tomu, aby různá data svedla na společného jmenovatele a poskytla jasnější zaměření. Tento přístup se používá všude.

Také FBI využívá technologie založené na umělé inteligenci k vyhodnocování stop, aby zajistila jejich správnou identifikaci, stanovení priorit a včasné zpracování. Oddělení CIA pro otevřené zdroje spustilo interní nástroj Chat-GPT AI, který má analytikům

poskytnout „lepší přístup k otevřeným zdrojům informací“, a NSA otevřela „Centrum pro bezpečnost umělé inteligence“, jehož úkolem je chránit „národní umělou inteligenci prostřednictvím spolupráce s průmyslem, akademickou obcí, zpravodajskou komunitou a dalšími vládními partnery“.

I když nové technologie pravděpodobně poskytnou bezpečnostním složkám USA výhodu, nesmíme zapomínat na druhou stranu mince: všechny tyto informace budou použity proti potenciálním protivníkům, mezi něž podle názoru Washingtonu patří Čína, Rusko a řada dalších zemí. A z jejich pohledu je takové využití umělé inteligence rovněž destruktivní.

Les abîmes choquants de l'intelligence artificielle vyšel 8.9.2024 na euro-synergies.hautetfort.com. Překlad v ceně 548 Kč Zvědavec.

Známka 1.3 (hodnotilo 26)

Oznámkuje kvalitu článku jako ve škole
(1-výborný, 5-hrozný)

1 2 3 4 5

Diskuze

4 příspěvků

(4 nové)

odeslat jako odkaz

odeslat text článku

vytisknout

uložit jako PDF