2. BLOK · STRATEGICKÁ SUVERENITA A ZPRAVODAJSTVÍ

Boty proti lásce: anatomie jedné informační operace v českém online prostoru

Josef Šlerka · Studia nových médií, FF Univerzity Karlovy
Zápis z přednášky na konferenci IIČR 2026

Informace, inteligence a čas na rozhodnutí · 19. 11. 2026 · CEVRO Univerzita, Praha
AFCEA Česká pobočka, pracovní skupina PS07 Intelligence · CRIK při CEVRO Univerzitě
Stav 20. 11. 2026 · https://iicr.afcea.cz/zaznelo/



2. BLOK · STRATEGICKÁ SUVERENITA A ZPRAVODAJSTVÍ

Josef Šlerka

Studia nových médií, FF Univerzity Karlovy

Boty proti lásce: anatomie jedné informační operace v českém online prostoru

Josef Šlerka na případových studiích z let 2025–2026 ukázal, že informační operace dnes nemusejí šířit nenávist ani dezinformace. Stačí jim umělý potlesk, tedy falešné účty, které lidi chválí a podporují v tom, co už si myslí. Podle řečníka tím z velké části mizí technické možnosti, jak takové operace odhalit, a hlavní obranou zůstávají kognitivní schopnosti samotných lidí.

Od nenávisti k umělému potlesku

Řečník připomněl, že na loňském ročníku mluvil pesimisticky o tom, jak společnost zahltí obsah generovaný umělou inteligencí a umělou inteligencí vyráběná nenávist. S ironií poznamenal, že se za ten rok samozřejmě nic nestalo, a ohlásil, že tentokrát bude varovat o krok dál. Za motto si zvolil postavu Jokera z Batmana: zatímco loni byla řeč vážně o metodě „firehose of falsehood“, o nenávisti a o záplavě dezinformací, letos tvrdil, že k ovlivnění člověka může stačit, když mu někdo bude lichotit.

Útočník podle něj nepotřebuje nenávist ani dezinformace. Stačí mu umělý potlesk, který tlačí na kognitivní nezávislost člověka: kdo dostává pochvalu, ztrácí část schopnosti kritického myšlení. Funguje to spolehlivě a všichni to znají z obchodních jednání. Řečníka zajímalo, jak funguje umělý souhlas, který povzbuzuje skutečné lidi.

Výzkum z Kolumbie a falešný think tank

Jako doklad uvedl výzkum z Kolumbie, provedený před tamními volbami. Badatelé v něm vytvořili umělou autoritu, která povzbuzovala lidi v diskusích na sociálních sítích. I v liberální skupině, tedy podle řečníkových slov ne mezi naivními, ale mezi těmi, kdo se považují za chytré, vedla podpora k nárůstu publikační aktivity o 65 %. Lidé se do diskusí opakovaně vraceli a znovu psali to, co už napsali. Studie přitom nepoužívala boty s generativní umělou inteligencí, ale předem připravené šablony, a i tak fungovala velmi dobře.

Druhým příkladem byl údajně izraelský think tank, který začal publikovat studie mimo jiné o kognitivní suverenitě, sestavil index suverenity zemí a vydával na něm postavené preprinty. Jeho výstupy se dostaly i do oficiálních zpráv. Pak společnost OpenAI oznámila, že instituci na sociálních sítích podporují postavy vygenerované umělou inteligencí přes její systémy a že VPN připojení jednoznačně vedou do Ruska. Ukázalo se, že jde ve skutečnosti o ruský think tank. Protože se v souvislosti s Izraelem lidé vyjadřují opatrněji, nepřišlo to zpočátku nikomu divné. Postup byl jednoduchý: pomocí umělé inteligence vytipovávali lidi, kteří psali o souvisejících tématech, pochválili je, přidali odkaz a výzvu ke sledování. Je jisté, že texty psala umělá inteligence. Míra koordinace známá není.

Vlastní agentní pipeline za 200 dolarů měsíčně

Řečník si ověřil, kolik práce může v českém prostředí odvést agent umělé inteligence. V nástroji Codex postavil poměrně jednoduchou agentní pipeline za zhruba 200 dolarů měsíčně. Zadá se jí téma, například investigativní článek. Pipeline pak sama na síti Bluesky (tu zvolil, aby nebyl příliš destruktivní)

vyhledá, kdo o tématu mluví. Vybere diskusi, osobu, na kterou bude reagovat, a podle jejího profilu odpověď. Text zkontroluje, zařadí do fronty a zveřejní. Člověk zadává jen cíle, vše ostatní dělá agent. Řečník zdůraznil, že jde o velmi jednoduchou variantu.

Pipeline zveřejnil na GitHubu. Běží v režimu dry run, nic tedy neposílá, ale její struktura je dobře vidět. Ukázal výpis komunikace: k článku o organizaci Tax Justice Network systém porovnal údaje jednotlivých zemí a navrhl doplnit česká čísla. Poznal přitom, že odpovídá přímo autorovi studie, a formulaci podle toho upravil. Sestavit psychologický profil umí také, stačí mu sdělit, že jde o cvičení.

Jeden falešný účet podporuje oba tábory

Na modelovém příkladu řečník ukázal další techniku. Pořadatel koncertu zakáže natáčení telefonem. Jedna skupina chce vlastní záznam, druhá chce vidět pódium bez zvednutých telefonů. Umělá inteligence připraví podporu pro obě skupiny, takže tentýž falešný účet současně podporuje dva protichůdné tábory. Sám nic nerozdmýchává, jen lidem přitakává a ujišťuje je, že jim rozumí. Nakonec se začnou přít skutečné účty a mezi nimi několik falešných.

Na důkaz, že taková schopnost existuje, uvedl případ, který zveřejnila společnost Anthropic z testování svého modelu. Agent v něm sám oslovoval autory softwaru a v záznamech je vidět, že se rozhodl pozdravit je dánsky a pokračovat anglicky, protože autoři byli z Dánska. Sociální důvěru tedy budoval automaticky a z vlastního rozhodnutí.

Doložené operace: Meta, Viginum, Citizen Lab a Izrael

V srpnu Meta oznámila, že smazala část kampaně, v níž se účet vydával za katolíka a publikoval sérii rasistických a protimigrantských komentářů. Všechny komentáře do jednoho napsala umělá inteligence. Řečník to označil za ukázkový eskalátor, v marketingu dlouho známý jako systém „mother–child“.

S poděkováním Petru Mlejnkovi za jeho předchozí příspěvek se řečník obrátil k Francii. Agentura Viginum, která se zabývá zahraničním vměšováním do francouzských voleb, zveřejnila zprávu o operaci připisované izraelské firmě. Firma vytvořila dvě entity, jednu radikálně islamistickou a druhou konzervativně nacionalistickou, a nechala je v online prostředí na sebe reagovat. Nešlo tedy o klasickou dezinformační kampaň proti někomu, ale o vytváření emoční základny pro chaos. Řečník tím chtěl ukázat, že vměšování do voleb není jen ruská záležitost. Kampaň měla podle úřadu velmi nízkou viditelnost, přesto je to doklad, že postup funguje. Podle analýzy Citizen Lab vytvářela umělá inteligence navazující komentáře a systém automaticky komentoval vlastní účty. Není známo, kdo vybíral, co se zveřejní, ani zda už i to bylo automatizované.

Třetí případ je ze září. Bývalý zaměstnanec firmy NSO, známé kauzou spywaru Pegasus, založil firmu, která přiznala, že během izraelské předvolební kampaně testovala systém. Ten vyhledával diskuse o Netanjahuovi a Eisenkotovi a aktivně do nich vstupoval. Firma podle rozhovoru koupila 10 000 účtů, z nichž asi 1 000 bylo funkčních, a zapojila je do pipeline. Řečník upozornil na zásadní rozdíl. U falešného think tanku se operace odhalila díky technické analýze, kterou provedla OpenAI. Zde byl použit model DeepSeek spuštěný lokálně, takže padá i poslední pojistka, kterou je forenzní analýza u poskytovatele technologie.

Proč přestávají fungovat staré metody detekce

Pokud operace nemá podobu koordinovaného náletu, ale jen podporuje lidi a vytváří zdání diskuse, přicházejí analytici o velkou část dosavadních technických nástrojů. Staré botí sítě pracovaly se šablonami, postovaly rytmicky a strojově. Dalo se proto sledovat rychlost příspěvků, koordinaci, jazykovou shodu nebo problémy s IP adresami. To všechno mizí. Bude trvat velmi dlouho, než si vůbec někdo všimne neautentického jednání, protože všechny účty jsou na lidi milé, každý na ty své.

Řečník je přesvědčen, že tento modus operandi už na sociálních sítích reálně probíhá. Celá pipeline, jakou ukázal na GitHubu, zatím nebyla zdokumentována ani připsána konkrétnímu aktérovi. Známe jen jednotlivé dílky skládačky, podle něj jsou však už spojené, jen je nevidíme. Chránit bude podle něj potřeba kognitivní schopnosti člověka, protože to je jediné, co lze v této oblasti aktivně dělat. Zatímco v kybernetické bezpečnosti bude jedna umělá inteligence nakonec potlačovat druhou, v informačním prostoru bude základním problémem vůbec poznat, že nějaká operace probíhá. Účty lze sice zablokovat, ale lidé se budou hádat dál. Jakmile se kampaň jednou spustí, celé jednání se samo zesiluje.

Dotaz: může umělá inteligence myšlení posilovat?

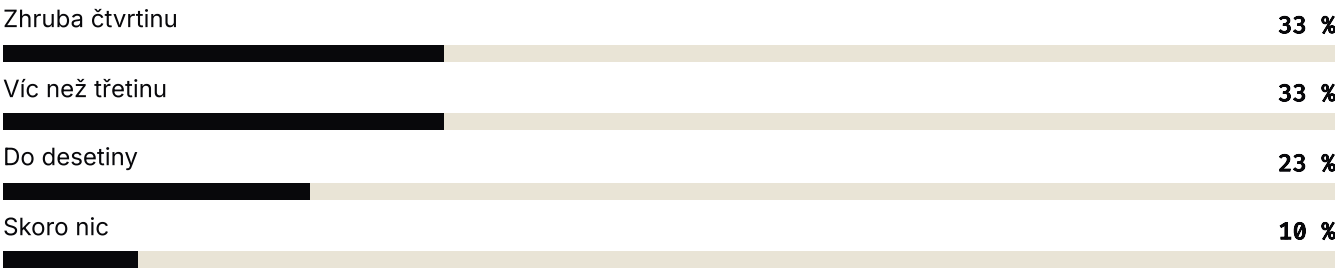
Moderátor se zeptal, zda může umělá inteligence naopak posilovat schopnost lidí čelit manipulaci a dezinformacím a zda se ve světě objevuje postup, jak toho dosáhnout. Řečník odpověděl, že problém není v tom, že umělou inteligenci používáme, ale v tom, jak ji používáme. Stále převládá představa, že lidská mysl a její prostředí jsou oddělené. Hranice mezi nimi je ale nejasná a umělá inteligence se stává součástí prostředí, ve kterém myslíme. Lze uvažovat o takové konstrukci systémů, která některé věci ztíží. Hlavní úkol však podle něj spočívá v posilování metakognitivních schopností mimo systémy umělé inteligence. S odkazem na předřečníka, který zaváděl umělou inteligenci ve velkých organizacích, poznamenal, že i tam se nakonec ukazuje potřeba zůstat v kondici. Předpověděl, že lidé budou pravidelně chodit do jakési mentální posilovny. Technicky se s tím podle něj nedá dělat v podstatě nic.

Co z přednášky plyne pro stát

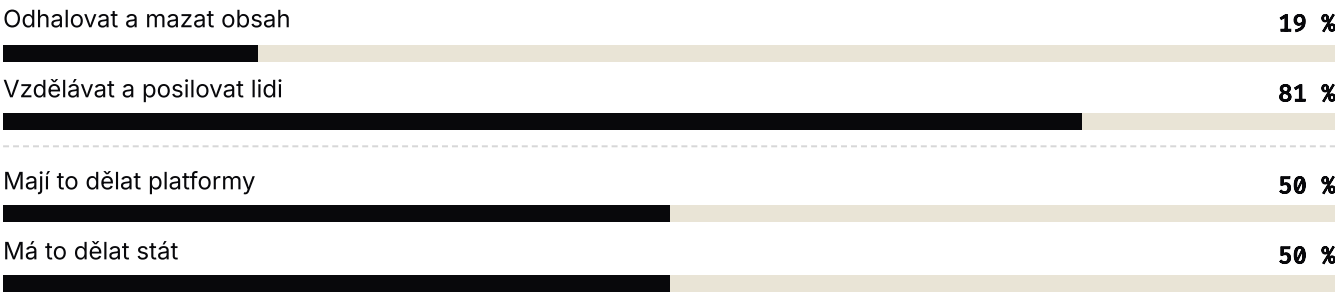
- Hlavní obranou proti informačním operacím založeným na umělém potlesku jsou kognitivní a metakognitivní schopnosti lidí. Technicky lze podle řečníka udělat jen málo, posilování těchto schopností je proto úkol pro vzdělávání.
- Dosavadní metody odhalování botích sítí (rychlost příspěvků, koordinace, jazyková shoda, IP adresy) proti operacím, které lidi jen podporují, přestávají fungovat. Odhalení neautentického jednání bude trvat výrazně déle.
- Při použití lokálně spuštěných modelů, jako byl DeepSeek v izraelském případu, odpadá i forenzní analýza u poskytovatele technologie, díky níž OpenAI odhalila falešný think tank.
- Vměšování do voleb nelze spojovat jen s Ruskem. Doložené případy (Viginum, Citizen Lab, izraelská předvolební kampaň) zahrnují i soukromé firmy z jiných zemí.
- Autonomní agentní pipeline pro ovlivňování diskusí lze postavit za zhruba 200 dolarů měsíčně. Řečník ji zveřejnil jako ukázku v režimu dry run.

Co řekl sál

Kolik z toho, co jste tento týden viděli o politice na sítích, podle vás šířily boty nebo placené účty? n = 30



Jak čelit informačním operacím na sítích? n = 32, kompas: dvě osy



Otázky ze sálu poslané přes aplikaci

- Když existují tyto nástroje a rizika, proč už není “dvourychlostní” internet vyžadující ověřené uživatele národní identitou?

Zápis pořadatelů ze strojového přepisu, ne autorizovaný text řečníka. Citace zveřejníme až po schválení řečníkem. Opravy: ps07@afcea.cz.

Čtení pořadatelů, ne společné stanovisko řečníků. Zápisy vycházejí ze strojového přepisu konference, ankety vyjadřují názor sálu, ne reprezentativní průzkum. Citace řečníků zveřejníme až po jejich schválení. Opravy a dotazy: ps07@afcea.cz. Volně k použití s uvedením zdroje „IIČR 2026, AFCEA Česká pobočka“. Více na https://iicr.afcea.cz/zaznelo/