MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Artificial Intelligence: A European Perspective

(Umělá inteligence: Evropská perspektiva)

Zdroj:https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/artificial-intelligence-european-perspective

Autor: Společné výzkumné centrum (JRC) Evropské komise

Zpráva se obecně zabývá současnou situací a budoucím vývojem a dopady umělé inteligence (UI). Část práce je o právním a bezpečnostním hledisku. Tyto dvě části jsou v následujícím textu shrnuty.

Bezpečnostní hledisko

UI a kybernetická bezpečnost

Nejstarším a nejklasičtějším je využívání UI pro bezpečnost v kyberprostoru, kde je UI součástí ochrany informačních systémů. UI například filtruje spamy nebo identifikuje potencionální útoky na systémy. Tyto systémy UI jsou většinou založené na metodách supervizovaného strojového učení. Do budoucna se dá očekávat pokračování trendu, kdy UI bude asistovat lidským operátorům, proti kterým budou stát kybernetické hrozby, které budou také využívat UI.

UI a boj proti kriminalitě

V oblasti boje proti kriminalitě se používání UI bude i nadále rozšiřovat. UI plní svoje úkoly například v boji proti kybernetické kriminalitě. Donucovací orgány se do využívání UI zapojují čím dál více pro její vyšetřovací schopnosti a k posílení digitálních důkazů u soudu.

Výzkum a vývoj UI pro potřeby donucovacích orgánů hraje a bude hrát důležitou roli v moderním boji proti kriminalitě. UI má schopnost podpořit donucovací orgány nejen v boji proti kybernetické kriminalitě, ale i v případech klasické kriminality. Většina současného bezpečnostního výzkumu UI se zaměřuje na tři cíle:

- lokalizace zločinu;
- identifikace obětí a pachatelů;
- stanovení obsahu trestné činnosti.

Forenzní věda je další oblast, kde donucovací orgány benefitují z využívání UI, například:

- biometrické systémy UI mohou napomáhat vyšetřování;
- UI asistuje při forenzním vyšetřování pevných disků;
- UI analyzuje databáze pro detekci podvodů;
- UI vyhledává důkazy o proliferaci digitálního obsahu;
- UI analyzuje zvukové, obrazové a textové média.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Zranitelnosti a hrozby plynoucí z používání UI

Používání UI však přinese nové a dosud ne zcela pochopené zranitelnosti. Je potřeba přihlédnout ke skutečnosti, že ochrana současných algoritmů je fundamentálně odlišná od ochrany systémů UI, které jsou mnohem komplexnější. Například UI v samo-učící fázi je vysoce náchylná na přesnost dat. Tudíž se samotná data stávají zranitelností.

Mezi hrozby ze strany UI patří například nezamýšlené důsledky, jako například sociální inženýrství na sociálních sítích, kde UI pomáhá šířit falešné zprávy a propagandu. Devastující by mohly být potencionálně kybernetické útoky na systémy, jako autonomní vozidla nebo dokonce autonomní zbraňové systémy. S tím jak bude UI rozšířenější a dostupnější, nebude sloužit jen k ochraně, ale bude bezpochyby využita i při škodlivých kybernetických útocích.

Závěry zprávy

Zpráva došla k následujícím závěrům pro UI v oblasti bezpečnosti:

- V nejbližší době UI nenahradí člověka v kybernetické bezpečnosti, ale spíše posílí jeho schopnosti.
- UI přinese jasné výhody pro kybernetickou bezpečnost a boj proti kriminalitě, ale přinese i nové výzvy v oblasti ochrany těchto nových systémů.
- Systémy založené na principu strojového učení často nejsou odolné proti škodlivým útokům.
- Je třeba zajisti dostupnost aktuálních a vysoce kvalitních datových souborů pro účely strojového učení.
- Je důležité mít na paměti, že v oblasti bezpečnosti je UI dvojité ostří.
- Implementace UI v bezpečnosti vyžaduje multidisciplinární přístup.

Co bude následovat

Zpráva nevyjadřuje politické pozice Evropské komise a slouží pouze jako vědecká podpora pro tvůrce politiky.