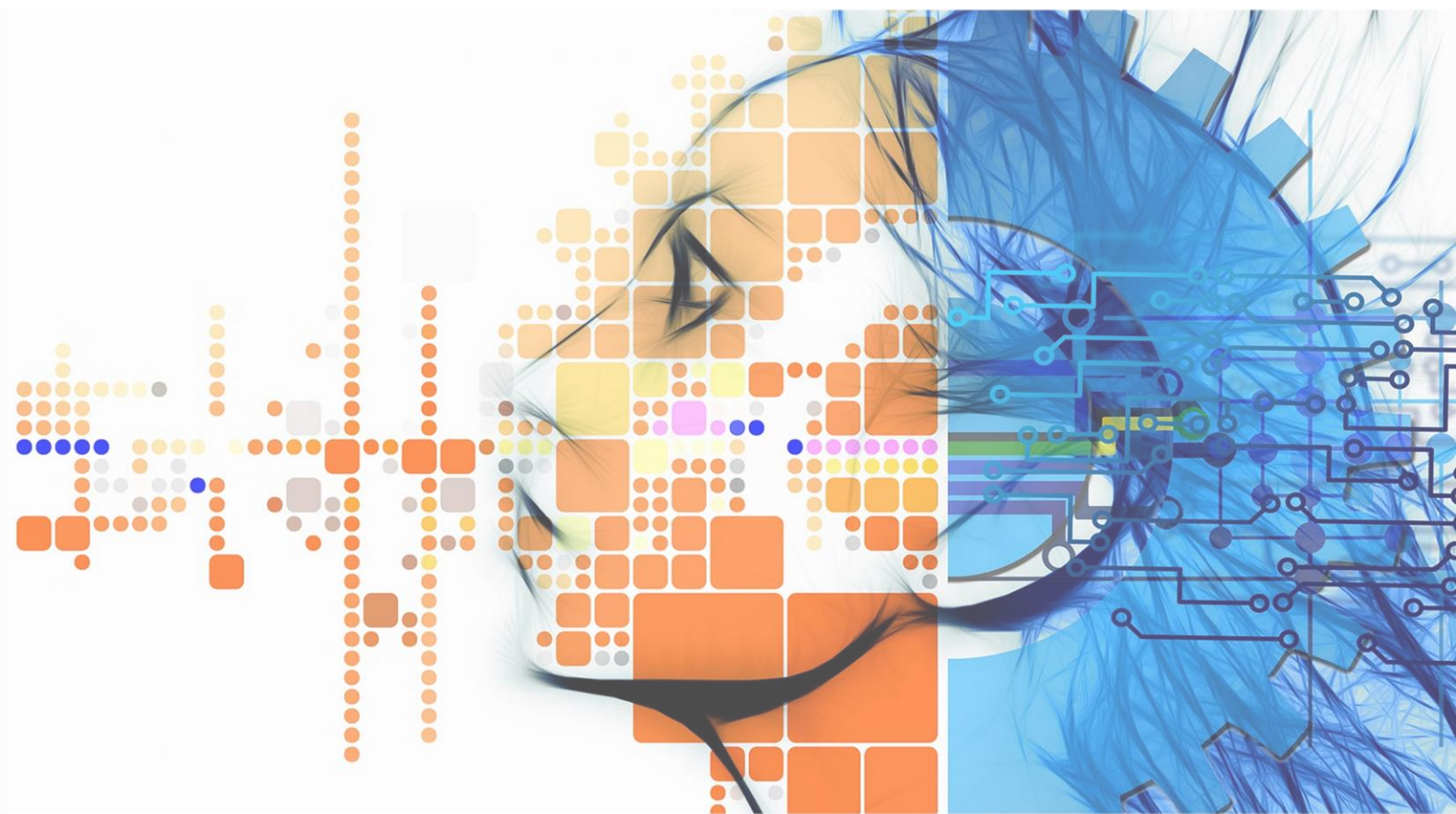


Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu



Bezpečnosť elektronickej komunikácie 2023

Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou



Bratislava
2023

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

ZBORNÍK PRÍSPEVKOV

z vedeckej konferencie s medzinárodnou účasťou

Bezpečnosť elektronickej komunikácie 2023

konanej dňa 11.05.2023

Bratislava 2023

Vedecký výbor konferencie:

doc. Ing. Stanislav ŠIŠULÁK, PhD. (Akadémia PZ v Bratislave)

pplk. JUDr. Michal MARKO PhD. (Akadémia PZ v Bratislave)

prof. Ing. Antonín KORAUS, PhD., LL.M., MBA (Akadémia PZ v Bratislave)

prof. JUDr. Jozef METENKO PhD. (Akadémia PZ v Bratislave)

doc. RNDr. Tatiana HAJDÚKOVÁ, PhD. (Akadémia PZ v Bratislave)

plk. gšt. v. z doc. Ing. Radoslav IVANČÍK PhD. et PhD., MBA, MSc. (Akadémia PZ v Bratislave)

Ing. Mgr. Jana TKÁČIKOVÁ (Prezídium PZ)

mjr. Mgr. Martin KAŠČÁK PhD. (Akadémia PZ v Bratislave)

Ing. Martin KUČTA, PhD., MBA (Obchodná fakulta, EUBA)

Organizačný výbor konferencie:

doc. RNDr. Tatiana HAJDÚKOVÁ, PhD.

mjr. Mgr. Martin KAŠČÁK PhD.

kpt. JUDr. Jana ZACHAR KUČTOVÁ

npor. JUDr. Miroslava DUBANOVÁ

por. Ing. Tomáš PETÁK

Ing. Martin KUČTA, PhD., MBA (Obchodná fakulta, EUBA)

Ing. Edita LUKÁČIKOVÁ

Mgr. Vladimíra HUDECOVÁ

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

doc. RNDr. Tatiana Hajdúková, PhD.

Zostavila:

JUDr. Jana ZACHAR KUCHTOVÁ

© Akadémia Policajného zboru v Bratislave

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.

ISBN 978 – 80 8054 – 997 – 8

EAN 9788080549978

Obsah

Úvod ku konferencii „Bezpečnosť elektronickej komunikácie 2023“	7
Tematické zameranie konferencie	8
Program konferencie	8
Výučba a chápanie problematiky HOAX-u u študentov 1. ročníka 4-ročného odboru na FIIT STU <i>Bystrík Bindas, Tatiana Hajdúková</i>	12
SECURE LORA INFRASTRUCTURE FOR EDUCATIONAL PURPOSES <i>Pavel Čičák, Ladislav Zemko, Alexander Valach, Michal Marko</i>	23
Možnosti ovplyvňovania verejnej mienky v on-line priestore pri volebnej kampani <i>Tatiana Hajdúková, Bystrík Bindas</i>	31
Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť <i>Radoslav Ivančík</i>	45
Vnímanie frekvencie výskytu hybridných hrozieb z pohľadu študentov vybraných vysokých škôl na Slovensku <i>Antonín Korauš, Miroslav Gombár</i>	57
Kybernetická bezpečnosť v krajinách EÚ so zameraním na Slovenskú republiku.....	69
Cybersecurity in EU countries with focus on the Slovak Republic <i>Antonín Korauš, Beáta Stehliková, Kristián Újváry</i>	69
Building Reputation in Community Open Data Ecosystems to improve the security of shared data <i>Ján Lang, Jakub Knežo, Dávid Korman and Stanislav Šišulák</i>	84
Limity anonymizácie transakcií virtuálnych mien <i>Andrej Lipták</i>	96
Právne podmienky ochrany osobných údajov v internetovom priestore	114
Legal Terms for the Protection of Personal Data in the Online Space <i>Miriam Odlerová</i>	114
Otvorený internet a Darkweb ako zdroje detskej pornografie <i>Tomáš Peták</i>	130
Identifikácia a boj proti dezinformáciám a falošným správam <i>Peter Poláček</i>	140

Rethinking Blockchain Technology Suitability: A New Decision Flowchart for Diverse Use Cases	
<i>Michal Ries, Muhammad Nasim Bahar, Antonín Korauš</i>	154
Hybridná vojna a hybridné hrozby	
<i>Róbert Tomášek</i>	163
Vybrané modely a systémy zamerané na komunikáciu	
<i>Jana Zachar Kuchtová</i>	172

Úvod ku konferencii „*Bezpečnosť elektronickej komunikácie 2023*“

Bolo nám potešením dňa 11.5.2023 zorganizovať druhý ročník vedeckej konferencie s medzinárodnou účasťou „**Bezpečnosť elektronickej komunikácie 2023**“.

Ku jedným z motívov pokračovať v organizovaní konferencie patrila nemenej významná potreba venovať pozornosť elektronickému informačnému prostrediu, do ktorého sme všetci na každodennej pravidelnosti zainteresovaní.

Cieľom podujatia organizovaného katedrou Informatiky a manažmentu na Akadémii Policajného zboru v Bratislave bolo poukázať na úlohy a postavenie bezpečnostných a štátnych zložiek pri ochrane online prostredia a aktivít v ňom prebiehajúcich. Ďalším z cieľov konferencie bolo zamyslieť sa nad úlohami a výzvami pri poskytovaní komunikačných služieb s akcentom na ich bezpečnosť. Význam a prínos predmetnej vedeckej konferencie vidíme v osobných stretnutiach odborníkov, ktorých úlohou je starať sa o bezpečnosť online služieb s užívateľmi týchto služieb, jedno či z profesionálneho alebo súkromného pohľadu. Predstavitelia bezpečnostnej praxe, členovia akademickej komunity vrátane študentov, ako aj zástupcovia odbornej verejnosti počas prestávok vytvorili spontánne neformálne diskusné fórum, na ktorom si vzájomne vymieňali názory a skúsenosti. Sme radi, že sa do programu podujatia aktívne zapojili vedeckopedagogickí zamestnanci FIIT STU v Bratislave a Akadémie Policajného zboru v Bratislave.

Vážime si a poďakovanie patrí všetkým prezentujúcim, ktorí aktívne vystúpili v programe konferencie a vytvorili tým kvalitu jej obsahu. Poďakovanie patrí každému účastníkovi konferencie, ktorý svojou účasťou vyjadril zvedavosť a záujem a tým dal zmysel konferencii. V neposlednom rade patrí poďakovanie celému organizačnému výboru, ktorému prajem veľa pozitívnej energie pri príprave ďalšieho ročníka konferencie.

pplk. RNDr. Tatiana Hajdúková, PhD.

vedúca katedry informatiky a manažmentu na A PZ

Tematické zameranie konferencie

Hackli ma! Čo teraz?

Digitálna identita

Ako sa chrániť pred útokmi na internete?

Ako sa správať bezpečne na sociálnych sieťach?

Dezinformácie a hoaxy – aký vplyv majú na dnešnú spoločnosť

Vzdelávanie a budovanie bezpečnostného povedomia v oblasti elektronickej komunikácie.

Program konferencie

8,00 h-8,30 h Prezentácia účastníkov

8,30 h-8,40 h Otvorenie konferencie

HLAVNÝ PROGRAM

8,50 h-9,40 h *Esenciálne základy v oblasti kybernetickej bezpečnosti*

prednášajúci: Marián Danko

Vládna jednotka CSIRT.SK

9,40 h-10,20 h *Bezpečnosť úschovy kryptomien*

Prednášajúci: Juraj Forgacs, Mária Potančoková

FUMBI NETWORK j. s. a.

Témou vystúpenia je bezpečnosť kryptoaktív, redukcia technických a legislatívnych rizík ako katalyzátor vývoja trhu a regulácia po prijatí MiCA.

Prestávka na kávu 10,20 h-10,50 h

10,50 h-11,10 h *Ochrana osobných údajov v podmienkach Ministerstva vnútra SR*

prednášajúci: Katarína DEŠŤOVÁ

odbor ochrany osobných údajov

11,10 h-11,30 h OSINT – „umenie“ získavania informácií z verejne dostupných zdrojov

OSINT (Open Source Intelligence) umožňuje získavať informácie z verejne dostupných zdrojov, ktorým môže byť samotný internet, sociálne siete, darkweb či verejné databázy a ďalšie. Čo všetko vieme zistiť o osobách, fotografiách a iných cenných údajoch, ktoré vieme získať z internetu? OSINT sa využíva v mnohých oblastiach ako informačná a kybernetická bezpečnosť, ale taktiež pri hľadaní nezvestných osôb, náboře nových zamestnancov a podobne.

prednášajúci: Eva MARKOVÁ

UPJS v Košiciach

11,30 h-11,50 h Ako rozoznávať a identifikovať podvody alebo základná investigatíva na internete

Ako zistiť príznaky falošného obchodu resp. ako si dať pozor na podvodníkov.

Adresy, osoby, údaje – kde zistiť základné fakty pri vyšetrovaní “webovej” kriminality. Vedia sa podvodníci skryť?

prednášajúci: Peter Bíro,

SK-NIC, a. s.

11,50 h-12,40 h Identifikácia zraniteľností v siet'ovej infraštruktúre.

Prednášajúci: Alexander Valach

Vládna jednotka CSIRT.SK

12,40 h-13,00 h Zabezpečenie súkromia a dát v Microsoft 365 pre školy

Prezentácia poskytne prehľad o rôznych bezpečnostných opatreniach, ktoré sú k dispozícii pre školy používajúce Microsoft 365. Okrem toho dozviete sa aj odporúčania a tipy pre školy, ako lepšie chrániť svoje dáta a zabezpečiť súkromie používateľov.

prednášajúci: Zuzana Molčanová

Microsoft

Prestávka na obed 13,00 h- 14,00 h

14,00 h-14,20 h Zvyšovanie bezpečnostného povedomia ako prevencia počítačovej kriminality

Téme vzdelávania informačnej/kybernetickej bezpečnosti sa v poslednom období venuje v odborných i laických kruhoch mnoho pozornosti. Aký je reálny stav vzdelávania týchto tém v slovenskom školstve – základnom, strednom i vysokom? Ako a či vôbec dochádza k prepájaniu tém IB/KB s problematikou prevencie počítačovej kriminality? Je skutočne jedinou rizikovou a pre zvyšovanie povedomia záujmovou skupinou výsostne mládež?

prednášajúci: Jaroslav OSTER

Info consult, s.r.o.

14,20 h-14,40 h Podvody so syntetickou identitou

Prednášajúci: Pavol Hruška, Martin MIŠOTA

odbor počítačovej kriminality P PZ

14,40 h-15,00 h Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť

Jedným z páľivých problémov súčasnosti, ktorý negatívne ovplyvňuje predovšetkým demokratickú spoločnosť, je rozrastajúci sa počet klamstiev a falošných informácií najrôznejšieho druhu – hoaxov, dezinformácií, konšpiračných teórií a pod. – šírených cestou internetu a sociálnych sietí. Internet a sociálne siete ich používateľom poskytujú anonymnejšie prostredie a široké publikum, ktoré je možné týmto spôsobom veľmi rýchlo osloviť. Autor v rámci svojho vedeckého výskumu, s využitím viacerých analyticko-syntetických prístupov a metód, sa v príspevku zaoberá problematikou hoaxov ako hrozby pre súčasnú modernú demokratickú spoločnosť.

prednášajúci: Radoslav IVANČÍK

Akadémia Policajného zboru v Bratislave

Prestávka na kávu 15,00 h-15,20 h

15,20 h-15,40 h Právne podmienky ochrany osobných údajov v internetovom priestore

Internet v súčasnosti stále viac využívame na rôzne účely, čím sa tento priestor stáva cieľom pre rôzne formy kybernetických útokov, ale aj zneužitia osobných údajov. Slovenská legislatíva

napriek tomu umožňuje za určitých podmienok zverejňovanie pomerne širokého okruhu osobných údajov.

prednášajúci: Miriam Odlerová

Akadémia Policajného zboru v Bratislave

15,40 h-16,00 h Umelá inteligencia ako riziko online komunikácie

Komunikácia medzi ľuďmi spočíva vo výmene informácií aspoň medzi dvoma osobami. Stále viac do pozornosti preniká komunikácia medzi človekom a technickým zariadením. Generatívnym pred-trénovaním jazykového modelu na rôznorodom korpuse neoznačeného textu je možné zvýšiť úroveň komunikácie medzi človekom a technickým prostriedkom. Príspevok sa zameriava na konverzačné jazykové modely, ich vývoj, využitie, výhody a riziká so zameraním na ChatGPT, vyvinutý spoločnosťou OpenAI.

prednášajúci: Tatiana Hajdúková, Jana Zachar Kuchtová

Akadémia Policajného zboru v Bratislave

Výučba a chápanie problematiky HOAX-u u študentov 1. ročníka 4-ročného odboru na FIIT STU

Bystrík Bindas, Tatiana Hajdúková

Abstrakt

Článok sa zaoberá spôsobom výučby v kontraste so skutočnými študentskými prezentáciami výsledkov bádania študentov 1. ročníka FIIT STU v predmete Informačné vzdelávanie.

Kľúčové slová

HOAX, informačné vzdelávanie, výučba

Abstract

The article deals with the method of teaching in contrast with real student's presentations of the results of the research of students of the 1st year of FIIT STU in the subject Information education.

Keywords

HOAX, information education, education

Úvod

Univerzita má u študentov rozvíjať nielen špičkové schopnosti v odbore, ktorí študujú, ale aj všeobecné znalosti. Toto platí najmä v prípade, že tieto znalosti je nevyhnutné uplatňovať v odbore, ktorí si vybrali. Je zaujímavé analyzovať správanie sa študentov prvého ročníka na Fakulte informatiky a informačných technológií STU Bratislava pri ich vnímaní problému šírenia dezinformácií – HOAX-u, ak je učebná látka samostatnou kapitolou v rámci vyučovaného predmetu, ktorý ich má pripraviť na správne spracovanie, vyhľadávanie a triedenie informácií. Všetky tieto tri techniky by si mali osvojiť a aplikovať počas svojho štúdia, ako aj počas svojej profesionálnej praxe. O tom, aký prístup volia, čo je ich prioritou v riešení problému, ako aj o ich schopnosti využiť získané poznatky je nasledujúci článok.

1. Informačné vzdelávanie

Cieľom informačného vzdelávania by malo byť pomôcť u študenta vytvoriť schopnosti ako získať, spracovať, overovať a vymieňať si informácie. Neoddeliteľnou súčasťou takéhoto vzdelávania by mala byť aj snaha o prebudenie schopnosti u participanta, aby vedel vytvárať informácie z vlastnej iniciatívy. Pojem samotný je často doľňaný o komunikáciu – teda prvok, ktorý by mal zabezpečiť zdieľanie a predávanie informácií. Informačné vzdelávanie je mnohokrát spájané s prácou v knižniciach. Moderné knižnice, teda predovšetkým tie poskytujúce odbornú literatúru, by sme si však už nemali predstavovať len ako miesta, kde si vieme vypožičať vytlačenú

knihu, ale plne vybavenú multimediálnu inštitúciu, ktorá by mala byť on-line prepojená s inými podobnými inštitúciami po celom svete. Obsah pojmu informačné vzdelávanie je teda veľmi široký, ale vždy v ňom hrá dôležitú úlohu trojčlenka získavania, spracovania a overovania informácií. Sú krajiny, kde je informačné vzdelávanie spojené už s vyučovaním na základných školách a v kombinácii s informatikou, ako je Kórea¹, prípadne je súčasťou vzdelávania v orientácii sa vo virtuálnom priestore pre seniorov v oblasti medicíny². Zatiaľčo niektoré krajiny ako Austrália rekapitulujú dosiahnuté úspechy v informačnom vzdelávaní a pre 21. storočie ich stavajú na troch základných pilieroch, teda výskum, výučba a prax³, našou snahou je ozrejniť študentom na vysokej škole, že používanie niektorých zdrojov informácií, napr. Wikipédia, sociálne siete nie je v poriadku.

2. Predmet „Informačné vzdelávanie“

Predmet informačné vzdelávanie sa vyučuje v prvom ročníku štvorročného bakalárskeho štúdia. Študenti musia najprv splniť podmienky účasti na skúške (v minulosti „zápočet“) a následne absolvovať skúšku. V rámci splnenia podmienok účasti na skúške študenti postupne realizujú na týždennej báze zadania. Tieto zadania sa viažu k informáciám, spracovaniu informácií, historickým udalostiam, jednoznačnej identifikácii autorov, pravdivosti informácií, minulosti informačnej techniky a podobne, pričom nevyhnutnou podmienkou správneho vypracovania zadania je použitie vedeckých databáz, ako základného a overeného zdroja informácií. Okrem týchto vedomostí a zručností študenti musia zvládnuť základy vedeckého písania, správneho citovania, manažmentu pracovných činností a informačnej ekológie. Zadania sú stavané tak, aby mali prepojenie na informačné technológie, prípadne na ich vyriešenie bolo potrebné použiť postupy a algoritmy blízke informatikom. Celkovým cieľom predmetu je naučiť študentov správne používať jednotlivé vedecké databázy, vyhľadávať a overovať si informácie na voľne dostupných zdrojoch, kombinovať informácie, prezentovať výsledky a vytvárať výstupy.

¹ PARK, N., SUNG, Y., JEONG, Y., SHIN, S., KIM, C., The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary Schoolin Korea, Springer Nature Switzerland AG 2019, R. Lee (ed.), Computer and Information Science, Studies in Computational Intelligence 791, https://doi.org/10.1007/978-3-319-98693-7_1

² CHANG, S. J., YANG E., LEE, K., RYU, H. RN, MSN, Internet health information education for older adults: A pilot study, Geriatric Nursing 42 (2021) 533-539, Elsevier Inc., <https://doi.org/10.1016/j.gerinurse.2020.10.002>

³ NASTASIE, Daniela L., Australian information education in the 21st century – the synergy among research, teaching and practice, Education for Information 29 (2012) 271–286, IOS Press, DOI 10.3233/EFI-130938

Inak povedané prebudieť záujem o bádanie, ktoré budú musieť ako budúci informatici používať na dennej báze.

3. Téma pravdy a chápanie pravdy

Témou spojenou s témou HOAX-u by samozrejme mala byť aj téma pravdy a chápania pravdy. Už nie jedenkrát sa totiž stalo, že to, čo bolo vyhlásené za HOAX sa ukázalo byť pravdou, a opačne to, čo sa považovalo za pravdu, či v ľudských dejinách častejšie za záhadu, sa ukázalo byť nepravdou. V tomto kontexte je zaujímavý aj spôsob ponímania pravdy. Pravda je subjektívna. Vezmime si iba situáciu, že presvedčame niekoho iného o niečom, čo my považujeme za pravdu. Už tým, že on má na túto tému iný názor, spochybňuje našu pravdu. Ak by sme sa však snažili našim tvrdením zmeniť podstatu našej pravdy, už len tým, žeby sme napríklad do opisu deja prikladali situácie, ktoré sa nestali, stávame sa šíriteľmi dezinformácie. A samozrejme, pri HOAX-e musíme brať do úvahy aj zámer jeho vytvorenia. Môže to byť zámer poškodiť, ale aj snaha niekoho nachytať, či vytvárať dezinformácie a stať sa ich šíriteľom z neznalosti. Snaha o získanie neoprávnenej výhody, ohrozenie alebo narušenie rovnosti šancí alebo príležitostí, teda demokratických princípov v prvom zmysle slova, či narušením čistoty a transparentnosti verejného a súkromného sektora, stratou dôvery občanov v zákonnosť a spravodlivosť v spoločnosti a štáte sú ďalšie z mnohých dôvodov, pre ktoré sú HOAX-i úmyselne vytvárané a rozširované.⁴ Ak vstupuje do odhaľovania HOAX-u umelá inteligencia, čo je zrejme v dobe informačnej explózie najlepší spôsob odhaľovania HOAX-u, je potrebné upozorniť aj na riziká, ktoré to prináša. Každý algoritmus umelej inteligencie je prispôsobiteľný v implementácii riešenia na obraz toho, čo chce realizátor dosiahnuť. Inak povedané, takýto spôsob implementácie bude dávať skreslené výsledky podľa prania realizátora či zadávateľa. V najhoršom prípade sa HOAX-om stane to, čo HOAX-om nie je. Stačí si len predstaviť v informatike zručného programátora bez rozhl'adu a kritického myslenia, pre ktorého je technická realizácia prednejšia, ako posúdenie jej dopadov. Aby sa čo najviac zabránilo takémuto počínaniu je potrebné realizovať prípravu v informačnom vzdelávaní pre čo možno najväčší počet študentov, najlepšie bez ohľadu na typ školy. Zneužitie umelej

⁴ LISONĚ, M., HULLOVÁ, M. *Klasifikácia kriminality*. In Policajná teória a prax. ISSN 1335-1370, 2020, r. XXVIII, č. 1. 2020, s. 64.

inteligencie sa najpravdepodobnejšie nebude dať zabrániť, ale vytvorenie akejkoľvek rozhládenej opozície môže zabrániť mnohým pokusom o skresľovanie faktov.

Zadanie č.5 – HOAX II

V jednej so svojich kníh opisuje aj pôvod a objavenie krištáľovej lebky (crystal skull)

Hoci ich bolo objavených viacero, asi najznámejšia je Mitchell-Hedges krištáľová lebka.

- Kto bol Mitchell-Hedges, kedy a za akých zvláštnych okolností objavil svoju „lebkú“
- Ako sa vyvíjal príbeh „pravosti“ lebky (čo sa jej prisudzovalo, za čo ju považovali... a podobne)
- 2-ma slovami, čo prispelo k rozlúšteniu tajomstva lebky z vedeckého pohľadu
- Ľudia, skúmajúci krištáľové lebky sú ľuďmi nimi posadnutými nazývaní VEDCI. Skúste vo vedeckých databázach nájsť akýkoľvek článok od: Franka Dorlanda, Karin Tag, Lydie Trauttenberg, prípadne iných, ktorých nájdete a komentujte výsledok
- V Scopuse, Web of Science a Dimensions skúste, či je možné vôbec nájsť vedecký článok na tému „Crystal Skull“, kde sa skutočne píše o krištáľových lebkách (www.scopus.com, www.webofscience.com, app.dimensions.ai)
- Aký prekvapivý výsledok ste zistili vo Web of Science? (pripomíname, že použiť máte všetky druhy zdrojov a podľa nich aj hodnotiť výsledky zistení)

Obrázok 1 Príklad zadania v predmete Informačné vzdelávanie

Zdroj: vlastné spracovanie

4. Ponímanie HOAX-u u študentov

HOAX-y sa začali hromadne šíriť a vznikať predovšetkým s rozvojom elektronických komunikačných služieb. Hax je prostriedok, ktorým si jeho aktéri môžu zvýšiť úroveň svojich možností a schopností pri dosahovaní svojich cieľov.⁵ Klamlivé a zavádzajúce správy sú zdokumentované prakticky od čias, odkedy bolo ľudstvo schopné písomne zachytiť predtým ústne podávané informácie. Explozívne šírenie HOAX-u v súčasnosti spolu so skutočnosťou, že za tento jav sú priamo aj nepriamo zodpovední informatici, ved' stále vyvíjajú a zdokonaľujú komunikačné systémy a platformy, na ktorých sa dezinformácie šíria, viedli k zaradeniu témy HOAX-u aj do výuky predmetu Informačné vzdelávanie. V uplynulých troch rokoch riešili študenti problematiku spojenú s HOAX-om v zadaniach uvedených v Tabuľke č.1.

Tabuľka 1 Zadania prác študentov

⁵ LISONĚ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In Policajná teória a prax. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 39.

Školský rok	Téma
2020/2021	Hodnotenie informačných zdrojov
2021/2022	Ludvík Souček Mitchell-Hedges a krištáľová lebka
2022/2023	Všetky cesty vedú do Bratislavy ... (ale už viete, že v minulosti sa takto nevolala...?)

Zdroj: vlastné spracovanie

Téma v školskom roku 2020/2021 vznikla spontánne ako výsledok práve prebiehajúcej pandémie a s ním spojenej očkovacej kampane. Témy v nasledujúcich dvoch rokoch boli vytvorené so zámerom dohľadania informácií vo vybraných vedeckých databázach.

Dôležité je tiež povedať, že výučba v rokoch 2020/2021 a 2021/2022 prebiehala v online priestore, kde je predsa len obmedzená možnosť na interakciu s participantmi. Napriek tomu bolo pozitívnym prekvapením, že sa študenti snažili pripraviť a odprezentovať svoje práce. Negatívnym javom bola skutočnosť, že po odprezentovanej prezentácii študentom, ak bol študent upozornený na nedostatky vo svojej prezentácii, tieto v odovzdanej práci neopravil. Práve táto práca bola hodnotená. Tento trend sa prejavil viac v témach, ktoré nie sú obsahom nášho porovnania.

Ako bolo spomenuté téma „Hodnotenie informačných zdrojov“ súvisela aj s vlnou HOAX-ov, ktoré vznikli počas pandémie COVID-19. U prezentujúcich študentov sa napriek tomu a možno práve preto absolútne neprejavil záujem o originálne spracovanie úlohy, neprikladali vlastné zistenia, iba opakovali všeobecné informácie získané zo zdrojov, ktorých pôvod a odraz reality informácie je takmer nemožné spochybniť. Boli to predovšetkým on-line stránky denníkov, či oficiálne vyhlásenia získané zo zdrojov vládnych inštitúcií. Jeden jediný študent bol ochotný diskutovať o zistených informáciách! Práce študentov boli obsahovo a technicky správne, ale ich pridaná hodnota v zmysle rozšírenia si prehľadu, či vôbec vyslovenia predpokladu absolútne absentovali. Technická správnosť vypracovania sa prejavila ako príčina skutočnosti, že drvivá väčšina študentov mala plný počet bodov.

V školskom roku 2021/2022, ktorý sa rovnako uskutočnil v on-line priestore, pretože sa jednalo o zimný semester, sa začalo viac prihliadať na spôsob prezentovania originalitu spracovania. Napriek tomu prevážil počet študentov s plným počtom bodov. Zaujímavejšie bolo,

že pre drvivú väčšinu študentov bol spisovateľ Ludvík Souček úplne neznámy. Rovnaký bol výsledok konfrontácie s menom Erich von Däniken, ktorý je minimálne v žánry príbuzný Ludvikovi Součkovi a je omnoho slávnejší. Druhá časť zadania týkajúca sa krištálovej lebky bola pre študentov vďaka úspešnému hollywoodskemu filmu bližšia. Pre väčšinu z nich však bolo prekvapením, že lebka skutočne existuje, a že vedecké články viažúce sa k odhaleniu niekoľko desaťročí trvajúceho podvodu sú súčasťou vedeckých databáz. Rovnako nimi bol bagatelizovaný vplyv vedy na odhalenie podvodu.

Školský rok 2022/2023 konečne priniesol priamy kontakt so študentami, prezentácia spracovaných tém prebiehala pred auditóriom spolužiakov. Nedostatkom sa však ukázal celkový čas, ktorý bol k dispozícii v rámci cvičení z predmetu. Možnosť priamej konfrontácie vyučujúceho so študentom predĺžila dĺžku jednotlivých prezentácií. Vznikla tak akási nemožnosť utiecť z virtuálneho sveta. Na druhej strane výrazne stúpol počet študentov. Priama komunikácia so študentom priniesla nižšie bodové hodnotenie a celkovú plytkú znalosť problematiky bolo jednoduchšie odhaliť. Na druhej strane vznikol predpoklad, že zvyšok študentov si mohol upraviť svoju prezentáciu pred odovzdaním na základe odsledovania si chýb a nedostatkov svojich spolužiakov. Niektoré odovzdané práce takýto postup naznačovali.

Tabuľka 2 Hodnotenie za zadania

Šk. rok, počet študentov s príslušným počtom bodov	Počet študentov s príslušným počtom bodov					
X	5	4	3	2	1	0
2020/2021	83	0	0	0	0	17
2021/2022	97	14	3	0	0	15
2022/2023	96	17	6	6	0	21

Zdroj: vlastné spracovanie

Študenti sa vo svojich odovzdaných prácach zamerali na splnenie bodov zadania bez zapojenie vlastnej invencie. Ich predložené práce boli vo väčšine prípadov správne ohľadne

výsledkov, ale úbohé v zmysle variability použitých zdrojov, už prakticky vôbec nie v zmysle využitia kombinácie záverov z viacerých zdrojov. Počet študentov, ktorý získali za svoju prácu 0 bodov z Tabuľky č.2 obsahuje aj tých, ktorí svoju prácu neodovzdali.

5. Možné nebezpečenstvá pre budúcnosť

Z výsledkov, ktoré boli porovnávané a rovnako aj z kvality spracovania zadanej úlohy môžeme dedukovať nebezpečenstvá, ktoré predstavuje nastupujúca generácia budúcich absolventov vysokých škôl. Je výrazný predpoklad toto konštatovanie generalizovať, aj keď vstupnými dátami boli podklady z vyučovania predmetu Informačné vzdelávanie na FIIT STU Bratislava. Hlavnými nebezpečenstvami vychádzajúcimi z pozorovania výsledkov sú predovšetkým:

- **Povrchnosť** – študenti sa zameriavali na dosiahnutie plného bodového stavu zo zadania bez toho, aby sa pokúsili o hlbšiu analýzu problematiky. Splnenie bodov zadania bolo predmejšie, ako bádanie v rámci všetkých možných zdrojov, ktoré boli k dispozícii. Ak by priamo v zadaní neboli spomenuté vedecké databázy, neboli by vôbec ako zdroje informácií spomenuté. Rovnako nimi používané zdroje informácií boli prakticky totožné, inak povedané, prvý odkaz z vyhľadávania cez internetový prehliadač.
- **Nezáujem o rozširovanie si vedomostí mimo svojho vedného odboru** – u študentov sa výrazne prejavovali prvky nezáujmu o skúmanie, ktoré by bolo aplikovateľné v ich primárnom študijnom odbore. Analytická časť práce, ktorá je v informatike predpokladom dobrého návrhu riešenia bola podceňovaná a minimalizovaná. Ak si vezmeme do úvahy skutočnosť, že študenti dnes disponujú priam vynikajúcimi programovacími schopnosťami, toto nekorešponduje so snahou zhotoviť informačný systém, ktorý má zadávateľom požadované vlastnosti. Prioritou sa stáva riešenie a je im nepodstatné, či bude prínosom pre používateľa. Ak pôjdeme do dôsledkou, tak môžeme mať generácie odborníkov, ktorí budú schopný technologicky zvládnuť zadanú úlohu, ale vôbec sa nebudú zamýšľať nad možnými dopadmi nimi vyvinutých informačných systémov.
- **Nevytváranie si vlastných teórií a predpokladov** – vo všetkých troch sledovaných rokoch absentovalo v odovzdaných a prezentovaných prácach študentov vyslovenie vlastného názoru. Pri prezentáciách museli byť priam vyzývaní, aby vyjadrili svoj predpoklad, teóriu, pričom

nebola posudzovaná jej správnosť. Cieľom bolo vyvolať debatu o možných konzekvenciách danej témy, v angličtine by sme povedali – brainstorming.

- **Slabý všeobecný rozhl'ad** – je v tomto prípade niečo, čo bolo prinesené ako výsledok vzdelávania na základných a stredných školách. V téme COVID-19 to bolo čerpanie informácií a sledovanie akýchsi hlavných médií, bez širšej snahy použiť všetky možnosti zdrojov, ktoré mali k dispozícii. Pri témach ohľadne Ludvíka Součka, krištálovej lebky a osoby významného vedca pôvodom z Bratislavy Wolfganga von Kempelena bolo zistené, že sa väčšina študentov sa stretla s týmito menami prvýkrát, a rovnako priznali, že krištálovú lebku si spájali s hollywoodskym filmom “Indiana Jones and the Kingdom of the Crystal Skull”. Mimochodom, plagát k tomuto filmu bol v roku 2021 indexovaný vo vedeckej databáze SCOPUS!
- **Prispôsobovanie sa stále sa opakujúcemu názoru** – pre študentov sa smerodatným stával názor prezentovaný z masovokomunikačných zdrojov, bez ďalšieho záujmu preskúmať tému a aj pôvod zdroja. Rovnako sa prejavilo, že v prípade, keď sú mimo virtuálneho priestoru a musia sa viac venovať prítomnosti na vyučovaní, vytvárajú si na základe odprezentovaných prezentácií ideálnu prácu, ktorú vedľa predložiť. Pozitívom na tomto je ich schopnosť iteratívne dospieť k správne riešeniu, ale to popiera ich záujem o vlastný náhľad na samotnú problematiku. Prevažuje prístup – technicky správne, ale bez väčšieho záujmu o dopady. Ak sa tento prístup prejavuje u študenta výberovej univerzity, dá sa predpokladať, že prispôsobovanie sa stále sa opakujúcemu názoru u väčšiny obyvateľstva bude výrazne vyššia.

Záver

Prvé dve dekády nového milénia priniesli bezprecedentný pokrok, doslova revolúciu v tom, akým spôsobom komunikujeme, ako prijímame, vyhľadávame a zdieame najr=znejšie informácie.⁶ Účelom príspevku nie je poskytnúť novú techniku boja proti šíreniu dezinformačných správ ani priblíženie boja s ich šíriteľmi. Jeho prínos treba vidieť v pohľade na skutočnosť, s ktorou sa musíme rovnako vysporiadať, ako s dezinformáciami a dezinformátormi s optikou nastupujúcej mladej generácie.

⁶ IVANČÍK, R. 2022. Dezinformácie ako hybridná hrozba. In Dezinformácie a právo : (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 62.

Na jednej strane predstavujú technicky vzdelanú a implementačne vybavenú generáciu, ktorá je schopná zvládnuť náročnú realizáciu napríklad samoučiacich sa algoritmov, ktoré sa najčastejšie používajú pri odhaľovaní a detekcii HOAX-u a na druhej strane sa nedostatočne zaujímajú, ba niektorí priam ignorujú príčiny a formy ich realizácie.

V kombinácii so silným technickým povedomím sa to môže v konečnom dôsledku prejavovať:

- zvýšeným rizikom manipulovateľnosti.
- nezaujmom o dopady technologického riešenia na skutočnosti, môže viesť ku neuvedomovaniu si hĺbky dôsledkov svojich technických realizácií.
- závažnými nedostatkami racionálneho myslenia v niektorých aspektoch.
- povrchnou analýzou bez väčšieho záujmu o detail a prepájanie súvislostí.

Aké sú dôvody a príčiny, ktoré už vedú k týmto javom necháme na odborníkov v príslušnej oblasti. V článku prispievame dátami, ktorých výstupy je možné špecificky spracovať. V každom prípade to v praxi vyučovania predmetu Informačné vzdelávanie znamená potrebu zvýšiť zameranie sa na obsahovú stránku spracovania tém, ktorá by mala byť v súlade s technickým zvládnutím témy. Inak povedané, viac dbať na analýzu a syntézu problematiky. Všeobecný prehľad študentov nie je možné počas jedného semestra zmeniť, je však možné pokúsiť sa narušiť povrchný prístup ku spracovávaniu podkladov.

Podakovanie

Príspevok vznikol v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zoznam použitej literatúry

Európska rada a Rada EÚ (2023) Kybernetická bezpečnosť: ako EÚ bojuje proti kybernetickým hrozbám dostupné online: <https://www.consilium.europa.eu/sk/policies/cybersecurity/>

Chang, S. J., Yang E., Lee, K., Ryu, H. RN, MSN, Internet health information education for older adults: A pilot study, Geriatric Nursing 42 (2021) 533-539, Elsevier Inc., <https://doi.org/10.1016/j.gerinurse.2020.10.002>

HULLOVÁ, M., FIDLER, Ľ. 2022. Riziká z realizácie hybridných hrozieb. In Dezinformácie a právo : (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 46. ISBN 978-80-8054-964-0.

IVANČÍK, R. 2022. Dezinformácie ako hybridná hrozba. In Dezinformácie a právo : (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, 55-66 s. ISBN 978-80-8054-964-0.

KORAUŠ, A., KURILOVSKÁ, L., ŠIŠULÁK, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. RELIK 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

Nastasie, Daniela L., Australian information education in the 21st century – the synergy among research, teaching and practice, Education for Information 29 (2012) 271–286, IOS Press, DOI 10.3233/EFI-130938

LISOŇ, M., HULLOVÁ, M. *Klasifikácia kriminality*. In Policajná teória a prax. ISSN 1335-1370, 2020, r. XXVIII, č. 1. 2020, s. 59-79.

LISOŇ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In Policajná teória a prax. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 38-53.

PARK, N., SUNG, Y., JEONG, Y., SHIN, S., KIM, C., The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary Schoolin Korea, Springer Nature Switzerland AG 2019, R. Lee (ed.), Computer and Information Science, Studies in Computational Intelligence 791, https://doi.org/10.1007/978-3-319-98693-7_1

Kontaktné údaje

Ing. Bystrík Bindas,

Slovenská technická univerzita v Bratislave,

Fakulta informatiky a informačných technológií

Ilkovičova 6276/2. 842 16 Bratislava 4

E-mail: bystrik.bindas@stuba.sk

pplk. doc. RNDr. Tatiana Hajdúková, PhD.

Akadémia Policajného zboru v Bratislave,

Sklabinská 1, 835 17 Bratislava 35

E-mail: tatiana.hajdukova@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

SECURE LORA INFRASTRUCTURE FOR EDUCATIONAL PURPOSES

Pavel Čičák, Ladislav Zemko, Alexander Valach, Michal Marko

Abstract

With the increasing number of emerging network threats and estimated increase in the number of IoT devices connected to the Internet, many aspects of the Low-Power Wide-Area Networks have to be explored. Due to the connection with cyber security and thus also the project of hybrid threats, this issue was included as part of the research. LoRa networks are often deployed in an industrial environment with no or only a fundamental level of security. The scalability of LoRa networks also poses a current challenge. In order to perform vulnerability assessment, network monitoring, communication planning, and utilization of computational intelligence, there has to be a laboratory network dedicated to educational and research purposes. In this paper, we briefly explore the possibilities of LoRa technology, and describe our own LoRa infrastructure deployed at the Faculty of Informatics and Information Technologies.

Keywords

LoRa, LoRaWAN, LPWAN, EDR, SIEM, infrastructure, hybrid threats, laboratory

Introduction

The Internet of Things, IoT for short, is an evolving area of technical, social, and economic dimensions. According to Cisco, the number of IoT devices could increase to 500 billion by 2030 [1]. Today, we use the term Internet of Things mainly to describe scenarios in which the Internet connection and computing capabilities extend to devices, sensors, and everyday objects, which are not normally considered computers [2]. The Internet of Things does not impose restrictions on the specific technology to be used to connect end devices to the Internet. Due to the nature of IoT, its applications and services, the only suitable solution is often the use of wireless communication [3] [4]. Thus, LPWA networks are very popular in the field of IoT. Despite many advantages, LPWANs face a number of challenges, that need to be addressed in the near future [2] [5].

To be able to perform research in this area, it is necessary to have access to the LoRa infrastructure. For purposes of our research, we decided to build a private infrastructure with focus on protocol stack flexibility and security.

The paper is organized as follows. Section 0 provides a brief introduction to Low-Power Wide-area Networks and LoRa technology. LoRaWAN protocol and possible attacks are described in section 0. Section 0 contains detailed description of private LoRa infrastructure deployed at the Faculty of Informatics and Information Technologies, and section 0 concludes the paper.

LoRa

Low-power Wide-area networks represent a category of Wide Area Networks. They combine low data rates with robust modulation, which enables them to communicate over distances of several kilometers [6] [3] [7] [8]. LoRa is probably the most popular and widely accepted LPWAN technology. It is a proprietary solution developed by Semtech. The solution is based on a modified Chirp Spread Spectrum modulation. LoRa can be therefore, in means of the ISO/OSI reference model, considered a physical layer, or a modulation scheme that specifies the way data is transmitted over the air. Subsequently, a MAC⁷ protocol operates on the link layer [9] [10] [11] [12] [13]. Figure 1 shows the example protocol stack, including LoRa PHY and LoRa MAC with subsequent LoRaWAN regional parameters, and application layer. Together with LoRa PHY, the LoRaWAN protocol is most often used.

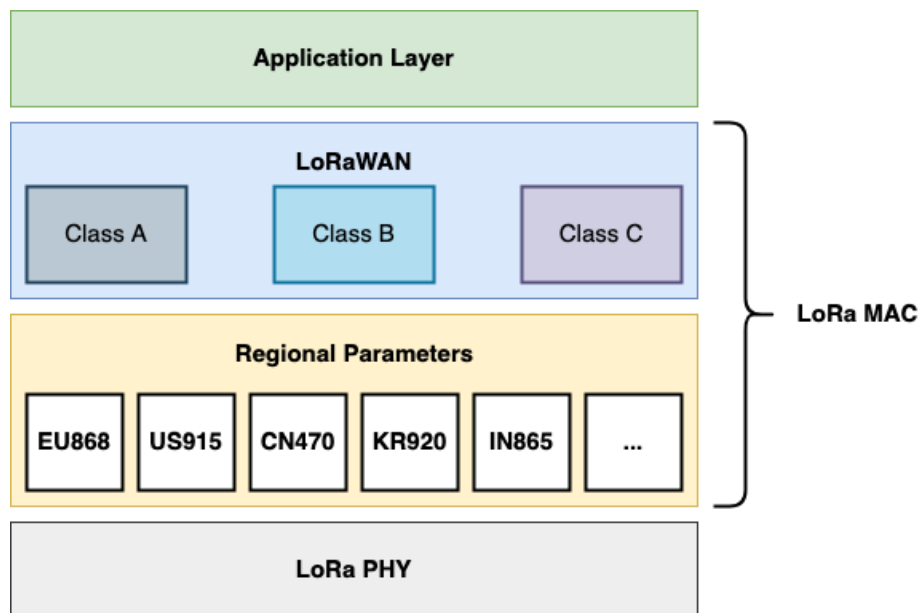


Figure 1 LoRa PHY and LoRa MAC

Zdroj:

01774080v1/preview/Phy_Mac_layer_LoRa_Sigfox_IET_Network.pdf

[https://hal.science/hal-](https://hal.science/hal-01774080v1/preview/Phy_Mac_layer_LoRa_Sigfox_IET_Network.pdf)

⁷ Medium Access Control

LoRaWAN

LoRaWAN is a MAC protocol, or LoRa MAC, when referred to Figure 1, which is responsible of medium access control. It defines frame format and allows a LoRaWAN devices to transmit data. The protocol is also optimized for use with battery-powered devices, both mobile and stationary. LoRaWAN describes the protocol itself, device classes, frame format, MAC commands, and activation modes, while the regional parameters describe parameters for each region. LoRaWAN devices are classified into 3 categories - A,B, or C - based on their properties and capabilities [9] [13] [12] [4] [14] [6] [15].

LoRaWAN network consists of end devices, which measure and transmit data. The basic architecture also consists of LoRa access points, which bridge communication between LoRa and IP network, and the network server, which further processes the data [4] [14] [6] [13] [10].

Due to the wireless nature of communication in LoRaWAN network, it is possible to perform several attacks, which can cause denial of service, or affect integrity and confidentiality. IoT security is sometimes underestimated. In combination with simplicity of end devices, unsecured IoT networks can increase the attack surface, and can easily become an entry point for an attacker. Examples of such techniques include ACK⁸ spoofing, bit flipping, eavesdropping, jamming, and replay attack [16] [17] [18] [8] [19]. It is thus necessary to increase the awareness of IoT security, especially in the context of hybrid threats, and highlight the demand for proper cybersecurity and information management in IoT networks [2] [20].

In case of LoRaWAN network, it is possible to monitor network devices using different technologies, e.g., OSSEC framework for EDR⁹ and Syslog protocol for SIEM¹⁰.

Private LoRa Infrastructure

To provide research opportunities and additional training for students and industry, it is important, for the researchers or developers, to be able to modify the existing components and manipulate the network stack. According to this, we have decided to build our own LoRa infrastructure. One of the key challenges was to select the proper components to build the infrastructure that provides the necessary functionality. In addition to the investments associated

⁸ Acknowledgement

⁹ Endpoint Detection and Response

¹⁰ Security Information and Event Management

with building the LoRa infrastructure itself, it is crucial not to forget the considerable effort in infrastructure management [4].

The infrastructure is shown in Figure 2 and consists of multiple components, which are described in the following section in more detail.

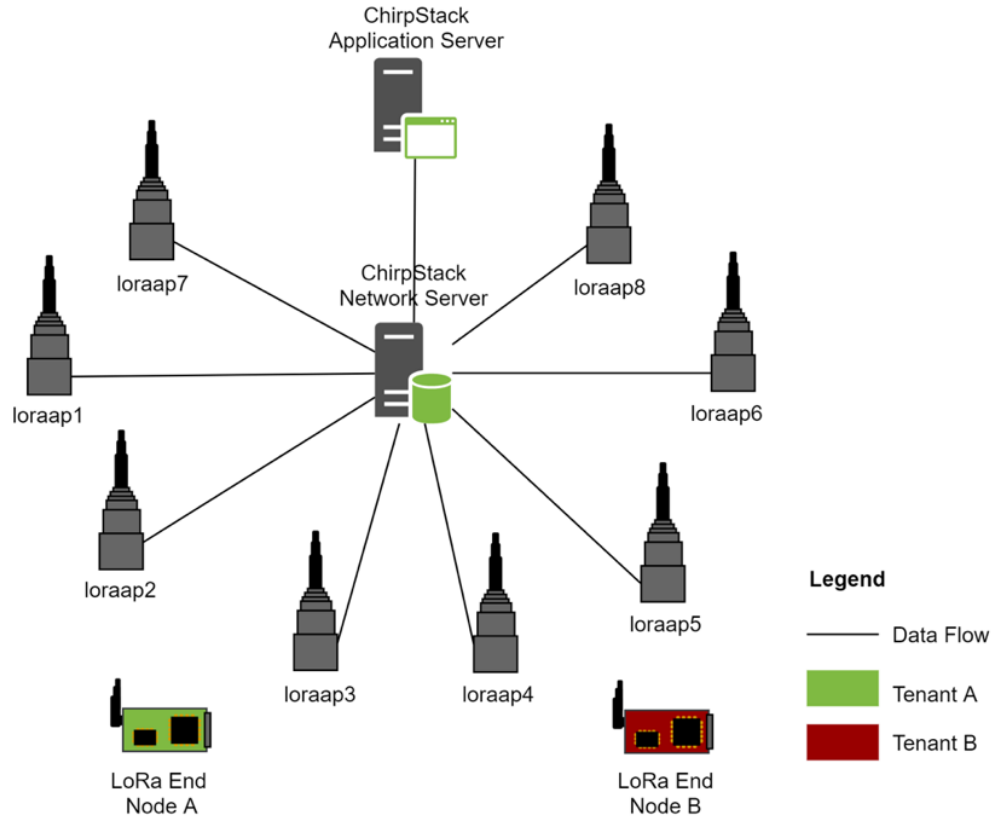


Figure 2 Network Infrastructure

Zdroj: <https://www.chirpstack.io/application-server/>

End devices

We utilized two different versions of the LoRa end node depending on the application's needs. If the low-power scenario is required, we use LoRa Radio Node v1.0 with an 8-bit ATmega328P processor and HopeRF RFM96W LoRa transceiver module. If the scenario with higher computational power is to be executed, and additional components, e.g., WiFi, BLE¹¹ or OLED display are needed, LilyGO TTGO LoRa32 T3 V1.6 868 MHz 0.96" SMA is used.

¹¹ Bluetooth Low Energy

Access Points

We are currently using 8 LoRa APs. Each AP consists of the following components:

1. Raspberry Pi.
2. IMST iC880a LoRa concentrator 868 MHz with SX1278 LoRa module.
3. 868 MHz LoRa antenna with pigtail.

We are using a Raspberry Pi microcomputer as it runs a modified version of Linux Debian called Raspberry Pi OS, instead of using a dedicated firmware or read-only file system as is the case with commercial LoRa APs.

Each AP supports the following functionalities:

1. Remote management via reverse SSH tunnel,
2. Running different LoRa daemons,
3. Low power consumption to be powered by power bank,
4. AP monitoring.

Each gateway sends the system and audit logs to the SIEM - Elasticsearch and Kibana. This functionality enhances the security of LoRa gateways and provides an additional opportunity for the standardization of syslog messages and events for LoRa devices.

Network Server

We used ChirpStack network and application servers. It is open-sourced, and fully compatible with LoRaWAN protocol. ChirpStack also provides a web application for the management of devices and access points and supports multi-tenancy. In addition, it has an interface for the third-party services and common cloud providers integrations.

Conclusion

As LoRa networks are being widely deployed, it is necessary to address the current challenges in these networks by providing research opportunities and training with the technology, hardware as well as software. That is why we have developed our own private LoRa network with the support of multi-tenancy, thus being able to provide our own infrastructure to further increase the research interest in this area. Developing our infrastructure is a continuous and challenging task as we need to focus on all its components. Not only building and installing, but also their

monitoring, security, management, and further maintenance. This area is closely related to the issue of hybrid threats and the areas in which these hybrid threats manifest themselves.

Acknowledgement

The contribution was created within the national project “Increasing Slovakia’s resilience to hybrid threats by strengthening public administration capacities”, project code ITMS2014+:314011CDW7. This project is supported by the European Social Fund.

References

Adelantado, Ferran, et al. Understanding the limits of LoRaWAN. IEEE Communications Magazine. 2017, Vol. 55, 9.

Aras, Emekcan, et al. 2017. Exploring the Security Vulnerabilities of LoRa. Conference: 2017 3rd IEEE International Conference on Cybernetics (CYBCONF). pp. 1 - 6. 10.1109/CYBCConf.2017.7985777.

Aras, Emekcan, et al. Selective Jamming of LoRaWAN using Commodity Hardware. 2017. 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 10.1145/3144457.3144478.

Centenaro, Marco, et al. Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios. IEEE Wireless Communications. 2016, Vol. 23, 5, pp. 60 - 67.

Cisco. Internet of Things: At a Glance. [Online] 2016. <https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>.

Korauš, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. RELIK 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

Link Labs, Inc. A Comprehensive Look at Low Power, Wide Area Networks. 2016.

LoRa Alliance. LoRaWAN L2 1.0.4 Specification. 2020.

Montagny, Sylvain. LoRa - LoRaWAN and Internet of Things for Beginners. Université Savoie Mont Blanc. [Online] July 2022. <https://www.univ-smb.fr/lorawan/wp-content/uploads/2022/01/Book-LoRa-LoRaWAN-and-Internet-of-Things.pdf>.

Perešíni, Ondrej and Krajčovič, Tibor. 2017. More efficient IoT communication through LoRa network with LoRa@FIIT and STIOT protocols. 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT). pp. 1 - 6. 10.1109/ICAICT.2017.8686837.

Philip, Sumesh J., McQuillan, James M. and Adegbite, Oluwatoba. 2020. LoRaWAN v1.1 Security: Are We in the Clear Yet? 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys). pp. 112 - 118. 10.1109/DependSys51298.2020.00025.

Phung, Kieu-Ha, et al. 2018. Analysis and assessment of LoRaWAN. 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications Computing (SigTelCom). pp. 241 - 246. 10.1109/SIGTELCOM.2018.8325799.

Raza, Usman, Kulkarni, Parag and Sooriyabandara, Mahesh. Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials. 2017, Vol. 19, 2.

Rose, Karen, Eldridge, Scott D. and Chapin, Lyman. THE INTERNET OF THINGS : AN OVERVIEW Understanding the Issues and Challenges of a More Connected World}. 2015.

Semtech Corporation. Application Note AN1200.22: LoRa Modulation Basics. 2015.

Stankovic, John A. Research Directions for the Internet of Things. IEEE Internet of Things Journal. 2014, Vol. 1, 1, pp. 3 - 9.

Vangelista, Lorenzo, Zanella, Andrea and Zorzi, Michele. Long-Range IoT Technologies: The Dawn of LoRa™. September 2015. pp. 51 - 58. 978-3-319-27071-5.

Vangelista, Lorenzo. IEEE Signal Processing Letters. Frequency Shift Chirp Modulation: The LoRa Modulation. 2017. pp. 1818 - 1821. 10.1109/LSP.2017.2762960.

Yang, Xueying, et al. Security Vulnerabilities in LoRaWAN. 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). pp. 129 - 140. 10.1109/IoTDI.2018.00022.

Zanella, Andrea, et al. Internet of Things for Smart Cities. IEEE Internet of Things Journal. 2014, Vol. 1, 1, pp. 22 - 32.

Contact information

Pavel Čičák

Faculty of Informatics and Information Technologies

Slovak University of Technology

Ilkovičova 2, 842 16 Bratislava IV

Slovakia

E-mail: pavel.cicak@stuba.sk

Ladislav Zemko

Faculty of Informatics and Information Technologies

Slovak University of Technology

Ilkovičova 2, 842 16 Bratislava IV

Slovakia

E-mail: ladislav.zemko@stuba.sk

Alexander Valach

Faculty of Informatics and Information Technologies

Slovak University of Technology

Ilkovičova 2, 842 16 Bratislava IV

Slovakia

E-mail: alexander.valach@stuba.sk

Michal Marko

Academy of the Police Force in Bratislava

Sklabinská 1, 835 17 Bratislava 35

E-mail: michal.marko@akademiapz.sk / michal.marko@minv.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel NEČAS, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Možnosti ovplyvňovania verejnej mienky v on-line priestore pri volebnej kampani

Tatiana Hajdúková, Bystrík Bindas

Anotácia

Neprehliadnuteľným znakom aktuálnej spoločenskej situácie v Slovenskej republike je zvýšená miera dynamiky zmien, z čoho vyplýva znížená stabilita a pocity istoty u obyvateľstva. Jedným príkladom zo súčasných destabilizačných prvkov spoločnosti je konanie predčasných parlamentných volieb. Vplývajúce na verejnú mienku je využívané na zhoršovania pnutia v spoločnosti. Pocity neistoty zjednodušujú zasahovanie do volebných procesov ako aj znižujú dôveryhodnosť verejných inštitúcií. Predmetná štúdia poukazuje na niektoré okolnosti, ktoré je možné použiť na ovplyvnenie verejnej mienky v on-line priestore v spojitosti s uplatňovaním volebného práva.

Kľúčové slová

hybridné hrozby, volebné právo, dynamické zmeny, verejná mienka

Annotation

An unmistakable sign of the current social situation in the Slovak Republic is the increased rate of dynamic changes, which results in reduced stability and feelings of security among the population. One example of the current destabilizing elements of society is the holding of early parliamentary elections. Influencing public opinion is used to worsen tensions in society. Feelings of uncertainty simplify interference in electoral processes as well as reduce the credibility of public institutions. The subject study points to some circumstances that can be used to influence public opinion in the online space in connection with the application of electoral law.

Key words

hybrid threats, electoral law, dynamic changes, perception, public opinion.

Úvod

Človek sa svojimi intelektuálnymi schopnosťami neustále napreduje. Počas svojho dlhodobého vývoja sa naučil vyrábať si ošatenie nielen ako tepelnú izoláciu a ochranu pokožky, ale v duchu módnych trendov ju povýšil na umenie, seba prezentovanie sa. Cieľavedome stavia priestory na bezpečné a pohodlné bývanie s výškou stoviek metrov a limity sú neustále posúvané vyššie. Stupeň inteligencie človeka nie je statický, v priebehu dejín sa zvyšuje jeho neustálou snahou o riešenie zložitejších problémov. Riešenie otázok súvisiacich so zdravotníctvom, poľnohospodárstvom, stavebníctvom, dopravou ale aj obranou, kontinuálne zdvíhali a zdvíhajú inteligenciu ľudstva vyššie. Nejedná sa len o úzku skupinu novátorov a vynálezcov, ktorí prispeli ku dosiahnutému pokroku. Na každého používateľa novodobých technických zariadení ich užívanie a ovládanie poskytovaných funkcionalít kontinuálne ovplyvňujú jeho kognitívne

schopnosti. Vynálezy a objavy postupne nahradili namáhavú fyzickú prácu, rutinnú mechanickú administratívnu prácu, aby uľahčovali život a vytvárali priestor pre príjemnejšie voľnočasové a tvorivé aktivity. S digitalizáciou spoločnosti, dynamickým nástupom nových médií a prudkým rozvojom a masovým využívaním informačných a komunikačných technológií, systémov a prostriedkov, sa neustále kreujú spôsoby, ako informácie, správy, zvesti, novinky či teórie nielen vyhľadávať, ale aj vytvárať či pozmeňovať a následne ďalej zdieľať a šíriť a tým aj zneužívať¹² S rozvojom a zvyšujúcou sa dostupnosťou internetu a s tým úzko súvisiacim hromadným využívaním sociálnych sietí je oveľa jednoduchšie vytvárať a šíriť informácie ktoré sú prispôsobené pre jednotlivých užívateľov ako aj naratívy, v ktorých sa udalosti, fakty a ich interpretácia podriaďujú určitému zámeru (politickému, ideologickému, religióznemu a pod.) a podsúvajú širokej verejnosti.¹³ Neprehliadnuteľnú pozornosť so sebou prináša intenzívne presadzovanie umelej inteligencie (z angličtiny Artificial Intelligence AI) do mnohých oblastí spoločenského života. Uznesenie Európskeho parlamentu o umelej inteligencii¹⁴ vymedzuje umelú inteligenciu ako systém, ktorý je založený na softvéri alebo je súčasťou hardvérových zariadení, a ktorý vykazuje správanie simulujúce inteligenciu s určitým stupňom autonómie na dosiahnutie konkrétnych cieľov. Dnes umelou inteligenciou rozumieme schopnosť prístroja vykonávať funkcie typicky spájané s ľudskou inteligenciou akými sú učenie, uvažovanie či tvorivosť.¹⁵ Umelá inteligencia preniká do spoločnosti v podobe rôznych automatizovaných systémov, ktoré pomocou algoritmov dokážu spracovať veľké množstvo dát, vyhodnotiť konkrétny prípad na základe jeho znakov, porovnať ho s podobnými prípadmi v jeho databáze a vyvodiť určitý záver. Od takýchto systémov si ich tvorcovia sľubujú uľahčenie rozhodovania, jeho väčšiu predvídateľnosť a nestrannosť. Umelá inteligencia pre dnešný svet predstavuje porovnateľne zlomový, ktorého účinky by mali mať dlhodobý a hromadný účinok,

¹² KUČTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave.

¹³ IVANČÍK, R. Dezinformácie ako hybridná hrozba. In Dezinformácie a právo : (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 59.

¹⁴ SPRÁVA o umelej inteligencii: otázky výkladu a uplatňovania medzinárodného práva, pokiaľ ide o EÚ, v oblastiach civilného a vojenského využitia a štátnej moci mimo rozsahu trestnej justície https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_SK.html

¹⁵ Umelá inteligencia: definícia a využitie [online]. 04.09.2020 [cit.2022-09-13]. Dostupné z: <https://www.europarl.europa.eu/news/sk/headlines/society/20200827STO85804/umela-inteligencia-definicia-a-vyuzitie>

podobne ako sa stala kníhtlač, parný stroj či výroba elektrickej energie v minulosti. Svojou zložitou a rôznorodou foriem môže vplývať na mnoho aspektov spoločnosti a zmeniť každodenné životy jednotlivcov. AI súčasnosti vytvára systémy schopné plniť najmä úzko špecifické a skôr rutinné úlohy, ale hranice sa veľmi rýchlo posúvajú. Veľmi rýchlo sú produkované výzvy, kde všade by sa mohla umelá inteligencia uplatniť. Ako príklad v bezpečnostných službách môžeme uviesť veľmi žiadané nahradenie nebezpečných alebo zdraviu škodlivých činností technickými zariadeniami alebo robotmi v prípadoch, keď ich plnenie si vyžaduje istú úroveň ľudskej inteligencie.

Súčasne s uvedomovaním si potrieb a snahou o ich dosiahnutie je potrebné nezatvárať oči a ostražito vnímať aj druhú stranu mince, existenciu rizík. Je nesporné, že uplatňovanie systémov umelej inteligencie môže byť mimoriadne prínosné, avšak súčasne môže spôsobovať aj negatívne dopady. Škody môžu byť jednak materiálneho charakteru, kde môžeme hovoriť o zásahoch do bezpečnosti a zdravia ľudí (napríklad poškodenie zdravia až straty na ľudských životoch, či škody na majetku), ako aj nemateriálneho - prejavujúce sa napríklad stratou súkromia, zásahom do práva slobodného prejavu, či ľudskej dôstojnosti.¹⁶ Problém etiky a morálky z krátkodobého hľadiska tkvie v tom, že tieto systémy sú čoraz viac nasadzované na posúdenie osobných údajov a žiadostí jednotlivcov, napríklad pri uchádzaní sa o prácu, poskytovaní elektronických služieb, posudzovaní žiadosti o pôžičku. Jedná sa o koncentrovanie veľkého množstva citlivých údajov, ktoré by sa mohli stať lákavým cieľom útočníkov. Umelá inteligencia výrazne zvyšuje možnosti identifikovateľnosti zjavne anonymných údajov, t. j. umožňuje re identifikáciu osôb.

Stroje ako také nepodliehajú etickým a morálnym princípom, čo by mohlo predstavovať zásadné riziká pre bezpečnosť. Informačná vojna je ponímaná aj ako ideologické ovplyvňovanie protivníka, pričom sa na tento účel používa široké spektrum nástrojov, ako sú napríklad dezinformácie, propagandabalebo diplomacia, ktoré sú zamerané na získanie informačnej dominancie (prevahy).¹⁷ Základné etické princípy, ktoré treba dodržať pri využívaní umelej inteligencie v súdnictve vypracovala aj Európska komisia pre efektívnu justíciu, medzi ktoré patria

¹⁶ Biela kniha o umelej inteligencii – európsky prístup k excelentnosti a dôvere z 19. 2. 2020. Dostupné online: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence_eb2020_sk.pdf str. 11

¹⁷ IVANČÍK, R., 2021. Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. In Politické vedy. 2021, roč. 24, č. 1, s. 141

princípy ako transparentnosť, bezpečnosť dát či rešpekt voči základným právam.¹⁸ Problémom môže byť nedostatok dôvery v technológiu kvôli otáznej úrovni transparentnosti v procese, ako stroje prijímajú svoje automatizované rozhodnutia a s tým súvisiaca nepredvídateľnosť konania.

Digitalizácia verejnej správy v kontexte umelej inteligencie

Oblasť digitalizácie verejnej správy je dôležitou a silne rezonujúcou témou. Právnym základom digitalizácie verejnej správy v Slovenskej republike je zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov tzv. „zákon o e - Governmente“. Informatizácia spoločnosti je globálny a nevyhnutný trend, ktorý je využívaný a súčasne aj zneužívaný na rozmanité ciele. Informačné a komunikačné technológie predstavujú vzhľadom na ich vplyv na chod štátu jeden z hlavných cieľov hybridných útokov na krajinu.¹⁹ Stratégia digitálnej transformácie Slovenska 2030 obsahuje niekoľko strategických oblastí pre funkčnú a modernú verejnú správu. Kľúčom pre zvýšenie produktivity verejnej správy je výrazné zlepšenie využívania údajov a aplikácia metód, akými sú posudzovanie vplyvov, analýza rizík, automatizované posudzovanie prípadov či žiadostí, alebo prediktívne plánovanie budúcich kapacít verejných služieb umelou inteligenciou.²⁰

Nové technológie dokážu zbierať obrovské množstvo dát v reálnom čase, analýza ktorých nám umožní úplne novým a agilnejším spôsobom plánovať rozvoj štátu, krajov a miest a zároveň sa starať o životné prostredie a chrániť našu vzácnu a krásnu prírodu.²¹ Základnou podmienkou fungovania dátového hospodárstva je vytvorenie dostatočných zdrojov dát a zabezpečenie dôveryhodného systému ich manažmentu.

¹⁸ CEPEJ, 2019. European ethical charter on the use of artificial intelligence in judicial systems and their environment. Council of Europe. Dostupné na internete: <https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf>.

¹⁹ LISOŇ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In Policačná teória a prax. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 41

²⁰ TOMEČKO, O. 2021. Správa o stave verejnej správy za rok 2020. MV SR : Inštitút správnych a bezpečnostných analýz.

²¹ Stratégia digitálnej transformácie Slovenska 2030. Dostupné online na: <https://www.mirri.gov.sk/wpcontent/uploads/2019/06/Strategia-digitalnej-transformacie-Slovenska-2030.pdf>

Dobrá stratégia volebnej kampane je nevyhnutný predpoklad volebného úspechu. Ohrozenie alebo narušenie rovnosti šancí alebo príležitostí je posudzované za zásah do demokratických princípov v pravom zmysle slova.²² Volebná kampaň je akákoľvek činnosť politickej strany, politického hnutia, koalície politických strán a politických hnutí a kandidátov, za ktorú sa obvykle platí úhrada, smerujúca k propagácii ich činnosti, cieľov a programu za účelom získania funkcie volenej podľa zákona č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov v platnom znení. Jedná sa o zviditeľnenie politickej strany, ktorým propaguje svoje ciele a záujmy, za ktoré sa považuje aj prostredie sociálnych sietí. V oblasti ochrany demokratického usporiadania krajiny v súvislosti s organizačným zabezpečením volieb v Slovenskej republike plní úlohu garanta Ministerstvo vnútra. Podľa zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov je orgánom štátnej správy príslušným na registráciu strán Ministerstvo vnútra. Trvanie kampane býva ohraničené a presne definované, čím stúpa význam rýchlosti a potreby oslovenia širokej masy voličov. Kampaň sa začína dňom uverejnenia rozhodnutia o vyhlásení volieb v Zbierke zákonov Slovenskej republiky a končí 48 hodín pred dňom konania volieb. Počas posledných dvoch dní pred konaním samotných volieb tzv. volebného moratória, nie je dovolené zverejňovať volebné prieskumy ani viesť volebné kampane. Pri trvaní kampane v riadnom pravidelnom termíne konania volieb sa zvykne rozlišovať obdobie kampane ako celok, z ktorého je pre isté osobitosti pôsobenia špecificky vyčlenené obdobie v čase začínajúcom 180 dní pred dňom vyhlásenia termínu volieb²³.

Opatrenia proti podvodnému financovaniu volebnej kampane

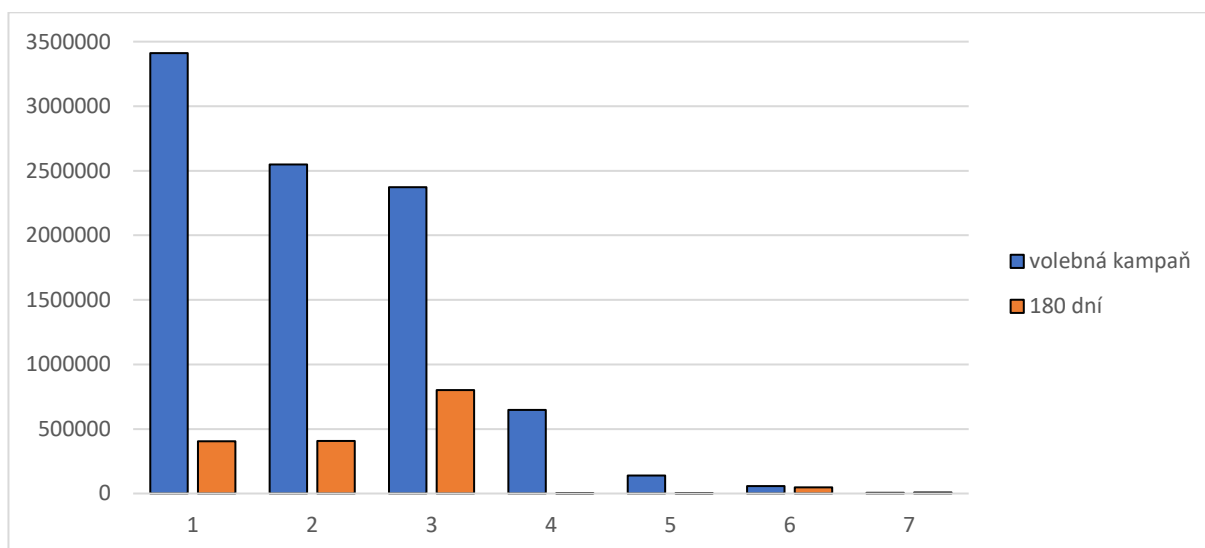
Politická strana v Slovenskej republike je povinná finančné prostriedky použité na volebnú kampaň viesť na osobitnom platobnom účte s názvom konkrétnej politickej strany. Údaje na tomto účte musia byť bezplatne, diaľkovo a nepretržite prístupné tretím osobám a musia zobrazovať prehľad platobných transakcií uskutočnených výlučne prevodom z iného účtu v rozsahu údajov o sume, dátume zaúčtovania, mene a priezvisku alebo názve platiteľa, texte účtovného zápisu a variabilnom symbole. Kvôli dodržaniu transparentnosti a trasovateľnosti týchto finančných

²² LISOŇ, M., HULLOVÁ, M. Klasifikácia kriminality. In Policajná teória a prax. ISSN 1335-1370, 2020, r. XXVIII, č. 1. 2020, s. 59-79.

²³ V prípade Parlamentných volieb konaných v roku 2020 sa konkrétne jednalo o obdobie od 9.5.2019 do 4.11.2019.

prostriedkov, vklad finančných prostriedkov v hotovosti, rovnako ako ani vklad prostredníctvom Slovenskej pošty, a. s. ako sprostredkovateľa vkladu finančných prostriedkov nie je možný. Informácie o finančnom pozadí politických strán môže poslúžiť na odhalenie konfliktu záujmov alebo kontrolu dodržiavania limitov na kampaň. Adresu webového sídla, na ktorom sú tieto údaje zverejnené, oznámi politická strana Ministerstvu vnútra SR, ktoré ju zverejní na svojom webovom sídle. Možnosť verejnej kontroly ani zďaleka nemôže suplovať systematickú kontrolu platieb na účtoch, zlepšiť kontrolu nad darcami financovanie obzvlášť zo zahraničia, či zlepšiť kontrolu na základe prístupu ku skutočným faktúram. Podľa § zákona č. 181/2014 Z.z. o volebnej kampani a o zmene a doplnení zákona 4. 85/2005 Z.z. o politických stranách a politických hnutiach v znení neskorších predpisov je každá politická strana (politické hnutie) povinná predložiť záverečnú správu o nákladoch na volebnú kampaň, ktorá je verejne dostupná na webovom sídle Ministerstva vnútra v sekcii verejná správa. Na základe záverečných správ parlamentných politických strán bol zostavený sumarizujúci pohľad na kategórie výdavkov úspešných politických strán z volebnej kampane v roku 2020.

Graf 1 Náklady na volebnú kampaň parlamentných strán pre voľby do Národnej rady Slovenskej republiky v roku 2020



Zdroj: Spracované z údajov záverečných správ politických strán o nákladoch na volebnú kampaň pre voľby do Národnej rady Slovenskej republiky v roku 2020

Usporiadanie kategórií výdavkov na volebnú kampaň na vodorovnej osi je zľava doprava zostupné, podľa výšky celkových výdavkov spojených s volebnou kampaňou (modrá výplň). Jednotlivé kategórie výdavkov sú nasledovné:

1. Náklady na úhradu platenej inzercie alebo reklamy [§ 4 ods. 2 písm. b) zákona]
2. prehľad všetkých ostatných nákladov politickej strany (politického hnutia) na propagáciu jej činnosti, cieľov a programu [§ 4 ods. 2 . písm. n) zákona]
3. prehľad nákladov na úhradu volebných plagátov [§ 4 ods. 2 písm. d) zákona]
4. prehľad nákladov na vysielanie politickej reklamy [§ 4 ods. 2 písm. c) zákona]
5. prehľad nepeňažných darov a iných bezodplatných plnení a ich hodnota [§ 4 ods. 2 písm. h) zákona]
6. prehľad nákladov na úhradu predvolebných prieskumov a volebných prieskumov verejnej mienky [§ 4 ods. 2 písm. a) zákona]
7. prehľad cestovných výdavkov členov politickej strany (politického hnutia) pri volebnej kampani a prehľad cestovných náhrad zamestnancov politickej strany (politického hnutia) pri volebnej kampani [§ 4 ods. 2 písm. e) zákona]

Z grafického zobrazenia v priebehu celej volebnej kampane výrazne dominujú náklady na platenú inzerciu, reklamu, propagáciu činnosti a volebné plagáty. Najmenšie výdavky v kategórii č. 7 o cestovných výdavkoch členov politickej strany pri volebnej kampani a cestovných náhrad zamestnancov politickej strany jasne potvrdzujú, že osobný kontakt s voličmi je pri súčasnej úrovni masovokomunikačných prostriedkoch pri volebnej kampani okrajovou záležitosťou.

Viacere stabilné a dlhšie trvajúce politické strany za obdobie v čase začínajúcom 180 dní pred dňom vyhlásenia volieb v roku 2020 už nevykázali žiadne náklady. Politické strany, ktoré volebnú kampaň využili do konca možného obdobia (stĺpce s oranžovou výplňou), sa za posledné dni koncentrovali hlavne na volebné plagáty, t.j. klasickú tlačенú formu zviditeľňovania sa verejnosti.

Volebná kampaň na sociálnych sieťach

V oblasti občianskych práv sa vplyv umelej inteligencie výrazne presadzuje pri volebnom práve. Intenzívnejšie ako samotné hlasovanie, sa do online prostredia presúva počiatočná fáza volebného procesu volebná kampaň, ktorá sa v tomto prostredí šíri podstatne efektívnejšie, ako

prostredníctvom tradičných médií. Nejedná sa len o ekonomické hľadisko z hľadiska oslošovania voličov, ale hlavne o rýchlosť a masovosť rozširovania informácií. Využívanie sociálnych médií na ovplyvňovanie vytýpaných adresátov je jeden zo spôsobov hybridného spôsobu pôsobenia na verejnosť.²⁴

Internet je primárne považovaný hlavne za zdroj informácií a nástroj na poznávanie sveta. Svojou funkcionalitou sa stihol stať aj mocným nástrojom, pomocou ktorého je možné manipulovať verejnou mienkou a polarizovať spoločnosť. Deje sa tak najmä kvôli schopnosti distribuovať obsah na základe osobných preferencií, bez rozhodovania užívateľa. Vyhodnocovanie sa uskutočňuje pomocou počítačových algoritmov, úlohou ktorých je dôkladné poznanie osobnosti, zvykov, okruhu priateľov a reakcií užívateľa na podnety. Akonáhle je osobnosť užívateľa vyprofilovaná, automatizovane mu je predkladaný obsah a reklamy, ktoré zodpovedajú jeho preferenciám. Algoritmus umelej inteligencie vyraduje všetky správy, ktoré by používateľa nezaujali, alebo ktoré nesúvisia s jeho názorom. K človeku sa tak dostane iba filtrovaný obsah, ktorý má potenciál zaujať jeho pozornosť a navyše s poradím príspevkov, ktoré nie sú zoradené chronologicky podľa času, ale prehádzané podľa atraktivity. To v užívateľovi vyvolá falošný pocit, že rovnaké názory zdieľajú aj ostatní. V skutočnosti však každý používateľ pracuje s inou množinou obsahu. Pre mnohých je jednoduchšie podvoliť sa ponúkanému obsahu, ako si cieľavedome selektovať informácie z obrovskej ponuky v databáze a uvažovať o ich vierohodnosti. Nie všetky informácie, ktoré sa k voličom zo sociálnych médií dostanú, sú teda objektívne. Zdieľanie vlastného obsahu, tzv. user generated content mnohými používateľmi komplikuje možnosti kontroly nad obsahom sociálnych sietí. Navyše, sociálne médiá sú plné trollov. Najatí trollovia šíria falošné správy preto, že im za to niekto platí a tým sa stáva ich dopad na verejnú mienku intenzívnejší. Uvedené vo svojom dôsledku zvyšuje polarizáciu názorov a vyvoláva ideologické konflikty.

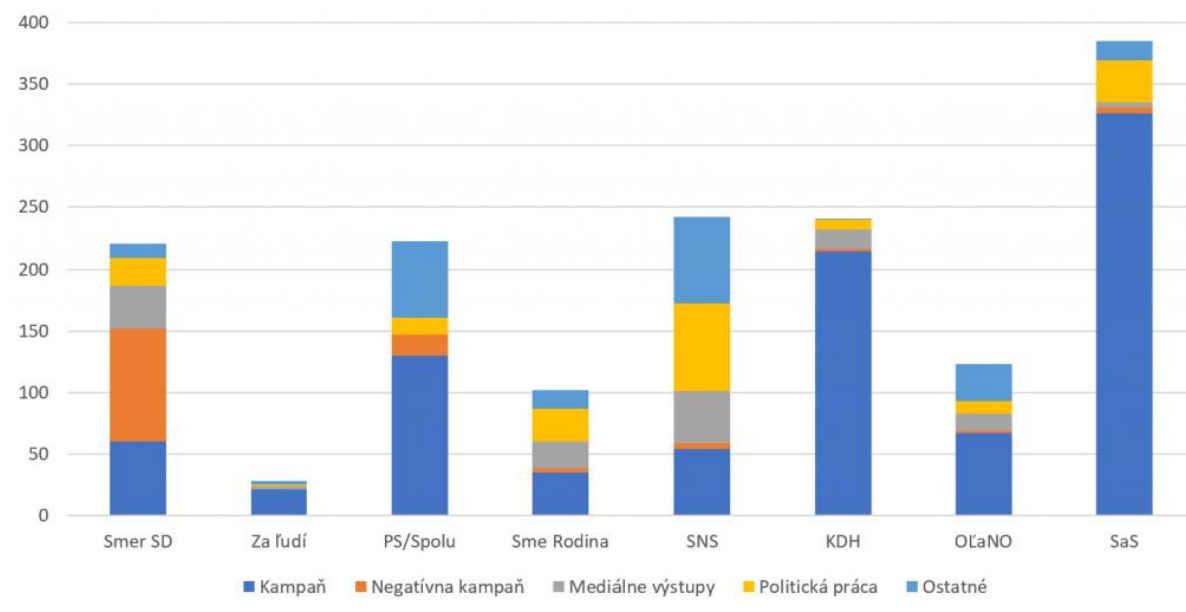
Nakoľko za volebnú kampaň sa obvykle platí úhrada, v kombinácii s vysokou závislosťou kampaní od času, využívanie sociálnych sietí sa ukázalo ako mimoriadne ekonomický a efektívny nástroj. Využitie sociálnych sietí na volebnú kampaň má veľký potenciál adresne zasiahnuť presne určených voličov. Možnosti kladných či negatívnych reakcií užívateľov na príspevky ako napríklad

²⁴ LISOŇ, M., FIDLER, E. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In Policijná teória a prax. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 41.

dať lajk, možnosť zdieľania medzi priateľmi alebo pridania komentáru pôsobí ako uveriteľný spôsob vyjadrenia slobodného názoru. Sociálne siete predstavujú priestor, kde môžu politické strany a politické hnutia na jednom mieste opakovane oslovovať široké publikum pomocou rôznych reklamných formátov. Cieľom optimalizácie sociálnych médií (SMO) je zvýšiť počet followerov, s ktorými budú prebiehať vzájomné interakcie tak, aby dané aktivity prispeli k naplneniu volebných cieľov týkajúcich sa okrem iného aj zvýšenia povedomia alebo získania nových voličov. Parlamentné voľby v roku 2020 prvýkrát umožnili podrobne sledovať kampan na sociálnych sieťach podrobnejšie.

Z hľadiska verejnej kontroly a spoznania konkurenčného prostredia, z knižnice reklám je možné vykonať informačnú analýzu činností na sociálnych sieťach. Informačná databáza umožňuje spoznať, aké tematické reklamy presadzovali jednotlivé politické strany, na koho ich cielili, koľko do nich investovali peňazí či počty ich impresií. Na grafe č. 2 je poskytnutý prehľad a miery výskytu tém ktoré boli použité v reklamách vo volebnej kampani parlamentných volieb v SR v roku 2020 na sociálnych sieťach Facebook a Instagram.

Graf 2 Reklamy na Facebook a Instragrame vo volebnej kampani parlamentných volieb v SR v roku 2020 podľa témy



Zdroj: Katedra komunikácie, digitálna PR a PA agentúra (Dostupné online na <https://www.trend.sk/nazory-a-komentare/tri-pohlady-oponu-kampane-socialnych-sietach>)

Celkovo mala najväčší podiel na rozlišovaných témach kampaň, dominujúca obzvlášť pri SaS, KDH a PS/Spolu. Pozornosť si zasluhuje položka negatívna kampaň, ktorá je spojená s útokmi na opozičné politické strany a opozičných kandidátov. Najčastejšie sa jednalo o zostrihané diskusie a videá, pri ktorých bola vytrhnutá z kontextu istá časť tvrdenia a následne šírená v pozmenenom význame, čím dochádzalo ku vedomému šíreniu dezinformácií. Útoky môžu smerovať obzvlášť na politické strany, preferencie ktorých sa pohybujú blízko hranice zvoliteľnosti. Zneistenie ich potenciálnych voličov môže znamenať ich stratu a tým aj skončenie politickej strany mimo parlamentu. Jedná sa o taktiku výhodnú pre väčšie politické strany, ktoré by si rozdeľovali poslanecké mandáty z mimo parlamentných strán najväčším podielom.

V tejto súvislosti nemožno nespomenúť možnosti personalizovaných reklám na volebné účely. Zadávatelia personalizovaných reklám sú schopní selektovať prijímateľov konkrétnej reklamy, na základe zadávateľom predpísaných kritérií. Využívané je pri tom proces „profilovania“, t.j. *zatriedenie osôb do kategórií skupín na základe spoločných znakov, najmä na účely analýzy alebo určitej prognózy*²⁵. Cílený výber tak umožňuje efektívnejšie a opakovane pôsobiť na cieľové subjekty. Systém personalizovaných reklám pracuje nad databázou zozbieraných dát pomocou zvolených algoritmov, preto ich môžeme zaradiť medzi formu umelej inteligencie. Umocnenie sýtenia verejnosti zvoleným obsahom sa dá gradovať aj zneistením širokej verejnosti neúplnými, polopravdivými informáciami, kedy bežný občan stráca istotu pri rozhodovaní.

Pozitívne treba vnímať možnosť aktívneho ovplyvňovania obsah na Facebook pomocou funkcie „Zobraziť viac“ a „Zobraziť menej“, ktorou je možné časť obsahu uprednostniť pred iným, resp. časť obsahu dať do úzadia. Od roku 2022 používa algoritmus Facebooku tri primárne hodnotiace signály na určenie obsahu informačného kanálu:

- Kto to zverejnil. Uprednostňovaní sú priatelia a firmy.
- Typ obsahu (videá, fotografie, text).

²⁵ UFERT, F. AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI? European Papers, Vol. 5, 2020, No 2, European Forum, Insight of 20 September 2020, pp. 1087-1097. ISSN 2499-8249. Dostupné na: https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-fundamental_rights#_ftn15 [online]: [cit. 07.04.2023]

- Množstvo interakcií.

Isté ale je, že umelá inteligencia sociálnych sietí nedokáže rozlíšiť medzi nezávislými a najatými trollmi. Preto sú ich komentáre pre väčšinu ľudí nerozlíšiteľné od ostatných a môžu voličov presvedčiť, aby sa priklonili k určitým názorom. Oba druhy trollov zverejňujú polarizujúce komentáre, ktoré vyvolávajú intenzívnu emocionálnu reakciu.

Záver

Vyššie uvedené problémy sú len časťou problémov súvisiacich s užívaním sociálnych médií v on-line priestore. Následky, ktoré vyvoláva vedomé šírenie informácií v istom upravenom kontexte, ešte viac umocňuje skutočnosť, že používané algoritmy vytvárajú ľudia z komerčných pohnútok. Ich cieľom je zvýšiť hodnotu svojho cieľa tým, že koncovým užívateľom ponúkajú viac želaného obsahu. Zneužívanie zraniteľnosti vo verejnej správe, zneužívanie právnych pravidiel, procesov, inštitúcií a argumentov priamo súvisia s možnými výzvami, ktoré vytvárajú zraniteľné miesta. Preto je nutné identifikovať aktivity potrebné pre fungovanie verejnej správy tak, aby bola schopná efektívne čeliť hybridným hrozbám. Všetky tieto rizikové faktory sa budú musieť procesne zohľadniť a koncepčne riešiť s cieľom znížiť rizikovosť v používaní nových technológií. V rámci pobraný pred podvodným financovaním volebnej kampane by prospelo vytvorenie osobitného bankového produktu, ktorý by bol špeciálne vytvorený pre predvolebné politické kampane. Nevyhnutnou podmienkou pri snahe dosiahnuť zodpovedné a nezaujaté fungovanie je využívanie kvalitných a nestranných údajov ako aj používanie algoritmov, pri ktorých je možné posúdiť a overiť, na základe čoho sú vykonávané rozhodnutia. Na zvýšenie odolnosti štátu a spoločnosti voči hybridným hrozbám nielen počas volebnej kampane by bolo vhodné posilniť i kapacity a expertízu vo verejnej správe, ako aj celoštátnu koordináciu predovšetkým v oblasti plánovania, riadenia a tvorby politík na vládnej a rezortnej úrovni.

Podakovanie

Príspevok vznikol v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zoznam použitej literatúry

IVANČÍK, R., 2021. Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. In *Politické vedy*. 2021, roč. 24, č. 1, s. 135-152. ISSN 1335-2741

IVANČÍK, R. Dezinformácie ako hybridná hrozba. In *Dezinformácie a právo : (úlohy a postavenie bezpečnostných zložiek) : zborník príspevkov*. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 55-66. ISBN 978-80-8054-964-0.

KORAUŠ, A., KURILOVSKÁ, L., ŠIŠULÁK, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. RELIK 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. 1. vyd. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LISOŇ, M., HULLOVÁ, M. *Klasifikácia kriminality*. In *Policajná teória a prax*. ISSN 1335-1370, 2020, r. XXVIII, č. 1. 2020, s. 59-79.

LISOŇ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In *Policajná teória a prax*. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 38-53.

UFERT, F. AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI? *European Papers*, Vol. 5, 2020, No 2, European Forum, Insight of 20 September 2020, pp. 1087-1097. ISSN 2499-8249. Dostupné na:

[https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-](https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-fundamental_rights#_ftn15)

[fundamental_rights#_ftn15](https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-fundamental_rights#_ftn15) Akčný plán koordinácie boja proti hybridným hrozbám (2022 - 2024), Ministerstvo obrany Slovenskej republiky

Správa o umelej inteligencii: otázky výkladu a uplatňovania medzinárodného práva, pokiaľ ide o EÚ, v oblastiach civilného a vojenského využitia a štátnej moci mimo rozsahu trestnej justície https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_SK.html

Umelá inteligencia: definícia a využitie [online]. 04.09.2020 [cit.2022-09-13]. Dostupné z:

<https://www.europarl.europa.eu/news/sk/headlines/society/20200827STO85804/umela-inteligencia-definicia-a-vyuzitie> Uznesenie Európskeho parlamentu z 12. septembra 2018 o autonómnych zbraňových systémoch (2018/2752(RSP))
https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_SK.html

Zákon č. 73/2017 Z. z. , ktorým sa dopĺňa zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa dopĺňa zákon č. 181/2014 Z. z. o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov v znení neskorších predpisov

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, 2019a. Stratégia digitálnej transformácie Slovenska 2030. Dostupné online na: <https://www.mirri.gov.sk/wpcontent/uploads/2019/06/Strategia-digitalnej-transformacie-Slovenska-2030.pdf>

Rozhodnutie č. 351/2019 Z. z. predsedu Národnej rady Slovenskej republiky o vyhlásení volieb do Národnej rady Slovenskej republiky.

Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Biela kniha o umelej inteligencii – európsky prístup k excelentnosti a dôvere z 19. 2. 2020. Dostupné online: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence_eb2020_sk.pdf str. 11

CEPEJ, 2019. European ethical charter on the use of artificial intelligence in judicial systems and their environment. Council of Europe. Dostupné na internete: <https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20system%20s.pdf>.

Kontaktné údaje

pplk. doc. RNDr. Tatiana Hajdúková, PhD.
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 35

E-mail: tatiana.hajdukova@akademiapz.sk

Ing. Bystrík Bindas,

Slovenská technická univerzita v Bratislave,

Fakulta informatiky a informačných technológií

Ilkovičova 6276/2. 842 16 Bratislava 4

E-mail: bystrik.bindas@stuba.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Šírenie hoaxov cestou sociálnych sietí – hrozba pre súčasnú demokratickú spoločnosť¹

Radoslav Ivančík

Abstrakt

Jedným z páľivých problémov súčasnosti, ktorý negatívne ovplyvňuje predovšetkým demokratickú spoločnosť, je rozrastajúci sa počet klamstiev a falošných informácií najrôznejšieho druhu – hoaxov, dezinformácií, konšpiračných teórií a pod. – šírených cestou internetu a sociálnych sietí. Zatiaľ čo na prelome tisícročí bolo klamanie na internete vnímané skôr ako výnimočné, žiaľ, aktuálne, na začiatku tretej dekády tretieho milénia je tento problém veľmi rozšírený. Internet a sociálne siete totiž ich používateľom poskytujú jednak anonymnejšie prostredie a jednak široké publikum, ktoré je možné týmto spôsobom veľmi rýchlo osloviť. Problémom je, že internet a sociálne siete dnes umožňujú ľahké šírenie v podstate akýchkoľvek informácií, čo poskytuje veľký priestor na šírenie najrôznejších falošných, klamlivých, zavádzajúcich, skreslených alebo úplne vymyslených informácií v podobe hoaxov, dezinformácií alebo konšpirácií. Aj preto sa autor v rámci svojho vedeckého výskumu, s využitím viacerých analyticko-syntetických prístupov a metód, vo svojom príspevku zaoberá problematikou hoaxov ako hrozby pre súčasnú modernú demokratickú spoločnosť.

Kľúčové slová:

Hoaxy, sociálne siete, demokratická spoločnosť, bezpečnosť, hrozba.

Abstract

One of the serious problems of today, which negatively affects democratic society above all, is the growing number of lies and false information of all kinds – hoaxes, disinformation, conspiracy theories, etc. – spread via the Internet and social networks. While at the turn of the millennium, lying on the Internet was seen as exceptional, currently, at the beginning of the third decade of the third millennium, this problem is very widespread. The Internet and social networks provide their users with a more anonymous environment and a large audience that can be reached very quickly in this way. The problem is that the Internet and social media today allow for the easy dissemination of basically any information, which provides a lot of room for the spread of all kinds of false, deceptive, misleading, distorted or completely fabricated information in the form of hoaxes, disinformation, or conspiracies. That is also why the author in his contribution, as part of his scientific research, using several analytical-synthetic approaches and methods, deals with the issue of hoaxes as a threat to the current modern democratic society.

Keywords:

Hoaxes, social networks, democratic society, security, threat.

¹ „Táto práca bola podporená Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV-20-0334.“

Úvod

S rôznymi falošnými, skreslenými, klamlivými či úmyselne pozmenenými správami sa stretáva ľudstvo už od nepamäti. Nie je to nič nového a ojedinelého, v živote v spoločnosti sa tieto správy vyskytovali, vyskytujú a určite budú vyskytovať aj v budúcnosti. Ich prítomnosť, vplyv a moc však dnes vnímame v určitých situáciách oveľa viac ako inokedy, a to najmä pokiaľ ide o závažné alebo významné spoločenské udalosti alebo rôzne krízové situácie. So šírením hoaxov, dezinformácií a konšpirácií v rôznych podobách sa nanešťastie v súčasnosti stretávame oveľa častejšie ako v minulosti, v podstate takmer denne, či už ide o rôzne pozmenené, úplne vymyslené alebo z kontextu vytrhnuté informácie, upravené fotografie alebo videá, články alebo „zaručene pravdivé“ správy posielané prostredníctvom internetu v reťazových e-mailoch alebo šíriace sa cestou sociálnych sietí.

Často záleží na samotnom jedincovi, ako veľmi sa nechá takýmito správami ovplyvniť, či je schopný odlíšiť klamstvo alebo výmysel od reality a či má dostatok správnych informácií, ktoré mu pomôžu na prvý pohľad odhaliť, že daná správa je nepravdivá, nereálna a ide o falošnú správu v podobe hoaxu, dezinformácie alebo konšpiračnej teórie a pod. Jedno je však u týchto správ zrejmé, a to že ich cieľom je ovplyvniť príjemcov týchto správ, ovplyvniť ich konanie, správanie, reakcie, zmanipulovať ich a doslova dostať tam, kam ich odosielatelia týchto správ chcú dostať.

Ľudia, zahltení a ovplyvnení veľkým množstvom najrôznejších správ týkajúcich sa určitej významnej spoločenskej udalosti, mnohokrát už nie sú schopní rozlišovať pravosť takých správ, a preto často dochádza k zmanipulovaniu tých, ktorých by takáto správa za iných okolností nemohla ovplyvniť. S rôznymi falošnými správami sa stretávame najmä v oblasti politiky a politického života, udalostí týkajúcich významných osobností politického, športového alebo kultúrneho života, tragických udalostí, riešení významnej problematiky, ktorá sa dotýka obyvateľov celej krajiny, regiónu alebo doslova celého ľudstva, ako tomu bolo napríklad v súvislosti s pandémiou koronavírusu spôsobujúceho ochorenie Covid-19.

V dnešnej informačnej spoločnosti sa v podstate mnohým takýmto správam ani nedá vyhnúť, avšak dôležité je, aby ich človek vedel rozoznať a aby sa nimi nenechal zmanipulovať a ovplyvniť, pretože to môže priniesť množstvo negatívnych dôsledkov tak pre jednotlivcov, ako aj pre celú spoločnosť. Aj preto sa autor vo svojom príspevku s využitím relevantných metód vedeckého výskumu zaoberá jedným z typov takýchto falošných správ – hoaxami a ich šírením prostredníctvom sociálnych sietí.

Teoretické vymedzenie pojmu hoax

Hoaxy patria do skupiny falošných, zavádzajúcich, klamlivých, skreslených alebo úplne vymyslených informácií s cieľom ovplyvniť konanie ich prijímateľov. Aby boli hoaxy úspešné, to znamená aby ovplyvnili čo najväčší počet ľudí, je potrebné, aby boli zdieľané, a to pokiaľ možno v čo najväčšom počte a rozsahu. Ich obsah tým pádom musí byť dostatočne zaujímavý, aby vzbudil náležitú pozornosť a primäl jedincov k ich ďalšiemu zdieľaniu, šíreniu. Z tohto dôvodu si autori hoaxov ako predmet svojho záujmu vyberajú zväčša emotívne ladené udalosti, situácie, príbehy a pod., vďaka čomu sú schopní oveľa ľahšie zaujať ich príjemcov a ovplyvniť ich. Ďalším typickým znakom hoaxov je, okrem snahy doručiť ich čo najväčšiemu počtu ľudí, ich urgentnosť. Práve z uvedeného dôvodu bývajú falošné správy vo forme hoaxov spravidla doplnené upozornením, že danú informáciu sa snažia oficiálne orgány (úradu) alebo dotknuté osoby zatajiť, a preto ju treba čo najrýchlejšie a čo najviac rozšíriť ešte skôr, než ju zakážu.

V súčasnej dobe masového využívania najrôznejších informačných a komunikačných technológií a prostriedkov a neustále sa rozširujúcej elektronickej komunikácie v súkromnom i profesionálnom živote má už každý z nás skúsenosti so spamom – hromadne rozosielanou nevyžiadanou správou, ktorá má zvyčajne komerčný obsah. Hoaxy, podobne ako spam, tiež predstavujú určitú formu nevyžiadaných informácií – v tomto prípade však falošných informácií. Ich účelom, na rozdiel od spamu, nie je predaj ani reklama, ale zber e-mailových adries a osobných informácií, ktoré sú následne využívané, či skôr zneužívané k iným, podvodným, zlomyseľným, mnohokrát aj veľmi zákerným a škodlivým účelom.²

Samotný pojem hoax má viacero významov, môžeme ho chápať napríklad ako podvod, mystifikáciu, novinársku kačicu, poplašnú správu, výmysel, žart alebo kanadský žartík a pod. V počítačovom svete sa pod týmto pojmom najčastejšie označuje falošná poplašná správa, ktorá varuje pred neexistujúcim nebezpečným vírusom. Okrem varovaní proti nebezpečným vírusom má hoax mnoho ďalších foriem a podôb. Prevažná väčšina hoaxov obsahuje vyššie zmienenú požiadavku na ďalšie šírenie správy. Hoax teda môže byť vymedzený aj ako falošná, klamlivá poplašná správa, ktorá upozorňuje na nejaké nebezpečenstvo, prosí o pomoc, sľubuje všetko možné i nemožné, ale hlavne žiada o jej ďalšie šírenie.

² ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 166

Ako hoax môžeme podľa Gregora a Vejvodovej označiť aj šírenú správu (oznámenie), ktorá obsahuje nepresné alebo skresľujúce informácie, účelovo upravené poloprávdy či celú zmes poloprávd a lži.³ Podľa Koloucha hoax síce veľmi často nesie myšlienku varovania pred nebezpečenstvom alebo dokonca útokom, ale môže obsahovať aj falošnú prosbu o pomoc či petíciu, rovnako tak môže byť tvorený obrázkami a videami.⁴ Nutil zasa označuje hoax za podvodnú, varovnú, mystifikačnú alebo žartovnú klamlivú správu, obvykle nevyžiadajú a obsahujúcu výzvu na ďalšie šírenie.⁵

Okrem vyššie uvedených definícií sa možno v literatúre stretnúť aj s množstvom ďalších vymedzení hoaxov, ktoré sú viac či menej zhodné. Väčšina z nich charakterizuje hoax ako aktivitu určenú na klamanie ľudí, trik alebo podvod, ktorý môže byť myslený aj ako žart, vtip, ale slúžiaci nielen na pobavenie. V takom prípade ide skôr o zlomyseľné žarty s cieľom oklamať ostatných. Všeobecne a zjednodušene možno povedať, že ide o nepravdivú správu, ktorá je buď podvodná, varovná, mystifikačná či žartovná.⁶

Formy a spôsoby šírenia hoaxov

Hoaxy môžu predstavovať, ako už bolo naznačené, klamlivú poplašnú správu v zmysle varovania pred nejakým nebezpečenstvom, ktoré však nie je reálne. Iným príkladom hoaxov môžu byť falošné prosby o pomoc, fámy, vymyslené petície, reťazové listy typu „zdieľaj a budeš mať šťastie“, prípadne „ak to nepošleš ďalej, budeš mať nešťastie“, pyramídové hry alebo rôzne ponuky na výhru alebo ľahké získanie peňazí.⁷ Vo väčšine prípadoch ale ide o už zmienené zavádzajúce poplašné správy, ktoré sa snažia cieľovú skupinu vystrašiť a donútiť k unáhlenej reakcii. Hoaxy spravidla spĺňajú nasledovné podmienky:

- snažia sa vyznieť dôležite – obsahujú napríklad slovné spojenie „naliehavá pomoc“ alebo „nebezpečenstvo“;
- odvolávajú sa na dôveryhodné zdroje – napríklad „WHO zistila“ alebo „FBI varuje“, pričom dané organizácie o takýchto správach žiadne vyjadrenie nevydali;

³ GREGOR, M. a kol. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno : CPress, 2018, s. 45

⁴ KOLOUCH, J. 2016. *CyberCrime*. Praha : CZ.NIC, 2016, s. 240

⁵ NUTIL, P. 2018. *Média, lži a příliš rychlý mozek: průvodce postpravdivým světem*. Praha : Grada, 2018, s. 139

⁶ YD. 2023. Hoax. In *Your Dictionary*, 2023

⁷ Hoax. 2023. Co je to hoax. In *Hoax.cz*, 2023

- hovoria o tajných informáciách, dátach – niektoré hoaxy sa napríklad vydávajú za „uniknuté“ alebo „tajné informácie“, ktoré majú ľudia čo najrýchlejšie a v čo najväčšom rozsahu šíriť ďalším ľuďom, kým ich oficiálne úrady nezakážu;
- obsahujú prosbu alebo pokyn o ďalšom šírení a zdieľaní.⁸

Formy hoaxov môžu byť veľmi rôznorodé, aj preto je pre bežného používateľa online prostredia niekedy naozaj veľmi ťažké rozpoznať či skutočne ide o hoax alebo reálnu správu. Môže mať totiž formu textu, žiadosti, prosby, petície, reťazového listu, fotografie, obrázku, videa a mnoho ďalších. Spôsoby ich šírenia sú prevažne založené na tom, že správa sa tvári dôležite, opiera sa o nejakú autoritu, ponúka šokujúcu informáciu, ktorá je veľmi dôležitá a je potrebné, aby sa rozšírila medzi čo najviac ľudí. Táto správa navyše v sebe často obsahuje aj stimul na ich šírenie, a preto sa zväčša naozaj šíri veľmi rýchlo.

Šírenie hoaxov prostredníctvom sociálnych sietí

Používanie rôznych lží alebo prekrúcanie faktov za účelom ovplyvnenia jednotlivcov alebo aj celej verejnosti, ako už bolo uvedené vyššie, nie je žiadnou novinkou, ak sa však spojí so sofistikovanými prostriedkami, aké predstavujú dnešné moderné „smart“ zariadenia⁹, prostriedky a technológie, s prostredím sociálnych sietí¹⁰ a internetu¹¹, prípadne aktivitou hackerov, objavuje sa tu nová a veľmi silná hrozba šírenia falošných správ vo forme rôznych typov hoaxov, ktoré môžu predstavovať nebezpečenstvo nielen pre jednotlivcov, sociálne skupiny a organizácie, ale v niektorých prípadoch bezpečnostnú hrozbu pre celú súčasnú demokratickú spoločnosť.

Vznik a rýchly rozvoj sociálnych sietí viedol k radikálnej zmene spôsobov, akými ľudia dnes komunikujú a získavajú informácie. Tento nový spôsob komunikácie sa vyznačuje veľmi vysokou rýchlosťou s akou sa správa prenáša. Sociálne siete tiež ponúkajú najvyšší stupeň interakcie, aký môžu aktuálne komunikačné prostriedky používateľom poskytovať. Prístup k najrôznejším informáciám je takmer neobmedzený a lacný, zväčša úplne zadarmo. Taktiež nedostatok efektívnych a účinných opatrení zameraných na reguláciu online obsahu, na rozdiel od

⁸ Tamtiež.

⁹ Bližšie pozri: KUČTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98

¹⁰ LOSEKOOT, M. – VYHNÁNKOVÁ, E. 2019. *Jak na sítě*. Jan Melvil publishing, 2019.

¹¹ HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Bratislava : Akadémia Policajného zboru v Bratislave, 2018

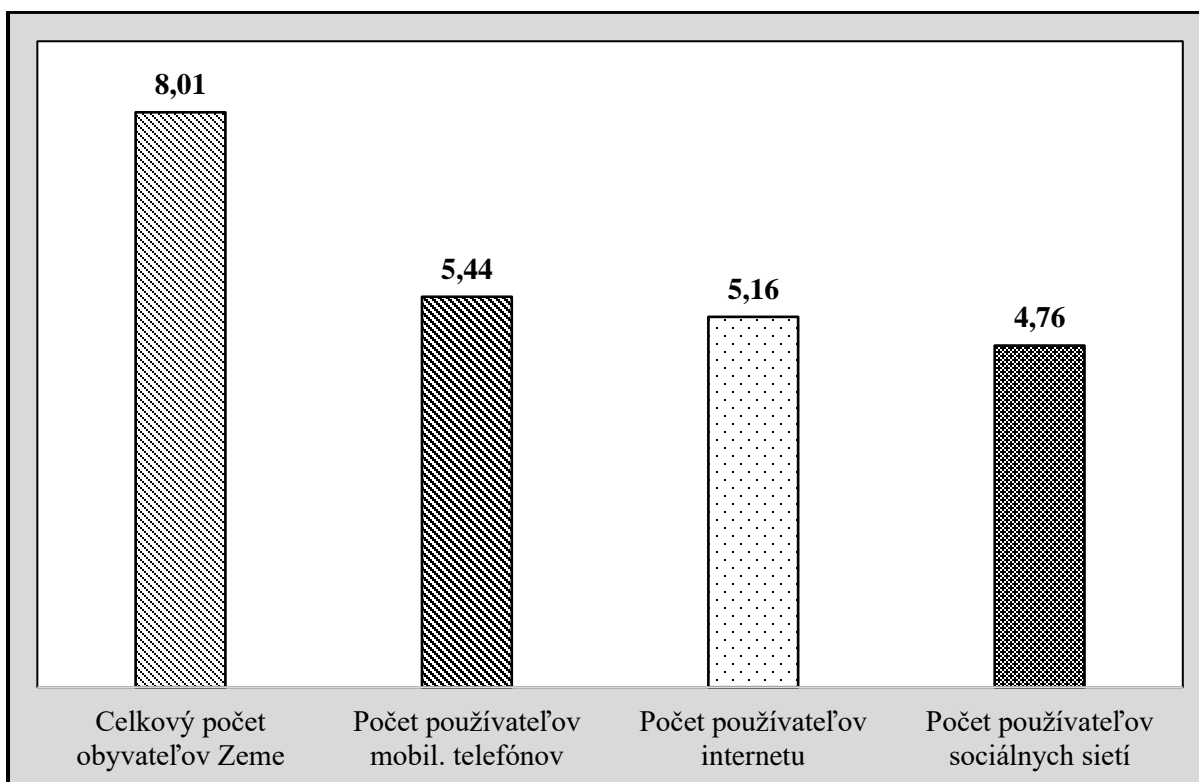
toho, ktorý sa vysiela prostredníctvom tradičných médií, robí online prostredie sociálnych sietí mimoriadne zaujímavým a tolerantným.

Zároveň je potrebné v tejto súvislosti dodať, že ide o nie veľmi bezpečné prostredie, a preto je nevyhnutné sa bezpečnosťou na sociálnych sieťach intenzívne zaoberať. Vzhľadom na veľký počet používateľov a interaktívny obsah, zdieľané osobné údaje a anonymitu komunikácie sa vytvoril ďalší priestor, v ktorom sa páchatelia realizujú a ohrozujú tým bezpečnosť používateľov. Sociálne siete pritom nemusia slúžiť len ako distribútor škodlivých kódov a informácií ale zároveň sa v nich dokážu priamo tvoriť. Najčastejšími príkladmi sú dezinformácie, hoaxy, sociálne inžinierstvo, kyberšikanovanie, grooming, sexting a mnoho ďalších, pričom páchatelia v záujme uchovania svojej anonymity na túto činnosť zneužívajú falošné profily.¹²

Čo sa týka penetračnej kapacity platforiem sociálnych sietí, poskytnuté štatistické údaje z konca januára 2023 poukazujú na značný nárast používania sociálnych sietí v porovnaní s predchádzajúcimi rokmi, ale aj na prognózu pokračovania tohto trendu v nasledujúcich rokoch. Podľa aktuálnych informácií mobilný telefón používa dnes cca 5,44 miliardy obyvateľov, čo predstavuje viac ako dve tretiny (67,9 %) svetovej populácie, internet používa približne 5,16 miliardy ľudí, teda viac ako tri pätiny (64,42 %) svetovej populácie, a počet aktívnych používateľov sociálnych sietí dosahuje zhruba 4,76 miliardy, čo predstavuje podiel na celkovom obyvateľstve planéty na úrovni 59,4 % (graf 1). Sociálne siete používa pritom prostredníctvom mobilného telefónu až 95 % ich užívateľov.¹³

¹² ZACHAR KUČTOVÁ, J. Bezpečnosť na sociálnych sieťach. In: *Bezpečnosť elektronickej komunikácie -zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2022, s. 246

¹³ DR. 2023. Global Digital Overview. In *DataReportal*, 2023

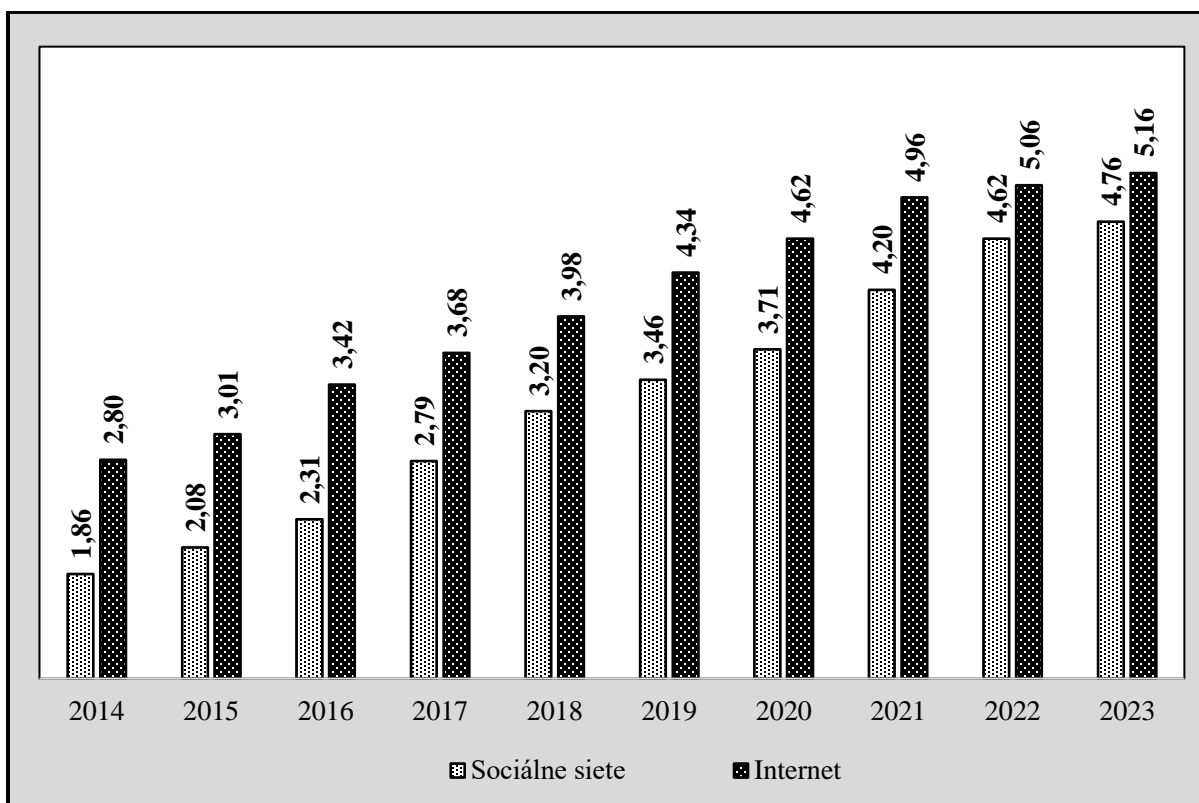


Graf 1 Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí ku koncu januára 2023 na celom svete (v mld.)

Zdroj: DR, 2023

O tom, aký dynamický je rast používateľov internetu a sociálnych sietí svedčí fakt, že za ostatných desať rokov celosvetovo stúpol počet používateľov internetu o takmer 2-násobok (o 184 %). Kým v roku 2014 používalo internet zhruba 2,80 miliardy ľudí, tak v roku 2023 to už bolo približne 5,16 miliardy. Rast používateľov sociálnych sietí je ešte dynamickejší, nakoľko stúpol v hodnotených rokoch o viac ako 2,5-násobok (o 256 %). Kým v roku 2014 používalo sociálne siete približne 1,86 miliardy ľudí, v roku 2023 sú to už zhruba 4,76 miliardy (graf 2). Z nich jeden užívateľ strávi na sociálnych sieťach priemerne denne 2 hodiny a 31 minút a priemerne mesačne využíva 7,2 rôznych sociálnych sietí.¹⁴

¹⁴DR. 2023. Global Digital Overview. In *DataReportal*, 2023



Graf 2 Prehľad rastu používateľov internetu a sociálnych sietí
v rokoch 2014 až 2023 (v mld.)

Zdroj: DR, 2022

Ciele a dôsledky šírenia hoaxov

Ciele šírenia hoaxov môžu byť pomerne rozmanité. Jedným z cieľov môže byť žart a pobavenie napríklad vo forme varovania pred nebezpečenstvom, ktoré však v skutočnosti vôbec neexistuje. V takomto prípade je cieľom hoaxov „vystreliť si“ alebo „napáliť“ čo najširší okruh osôb.¹⁵ Ďalším z cieľov, ktoré sú v súvislosti s hoaxami v odbornej literatúre spomínané, je senzáciachtivosť. Za takýmto typom hoaxov často stojí niekto, kto chce získať pozornosť, upútať na seba či doslova príjemcov šokovať. A práve to ho mnohokrát robí rozpoznateľným. Môže totiž obsahovať nereálne, niekedy doslova až ťažko predstaviteľné tvrdenia napríklad o účinkoch vírusov, vakcín, liekov, alebo o hromadných explóziách mobilných telefónov, počítačov a pod. Zväčša tiež používajú poplašný jazyk, vyskytujú sa v nich slová ako hrozba, riziko a viaceré ďalšie

¹⁵ KOLOUCH, J. 2016. *CyberCrime*. Praha : CZ.NIC, 2016, s. 240

vzbudzujúce strach, neistotu a pod.¹⁶ Ďalším z cieľov hoaxov je formou nepravdivej správy niekoho vydesiť alebo získať na svoju stranu, t. j. získať podporovateľa svojho presvedčenia. Dôsledky takýchto hoaxov môžu byť niekedy až fatálne, môžu ohroziť ľudské zdravie, ľudské životy, ale tiež môžu podryvať autoritu štátu, jeho demokratických hodnôt a demokratických inštitúcií.¹⁷

Odborníci na falošné správy uvádzajú, že hoaxy často bývajú samy o sebe pomerne neškodné a spôsobená škoda spravidla predstavuje len čas premárnený tými, ktorí si v prvej chvíli neuvedomia, že ide o falošnú správu alebo podvod. Toto tvrdenie síce v mnohých prípadoch naozaj platí, ale ako je uvedené vyššie, nie vo všetkých. V niektorých situáciách totiž skutočne môže dôjsť prostredníctvom hoaxov k ohrozeniu životov a zdravia ľudí, k poškodeniu reputácie alebo strate dôveryhodnosti v demokratické inštitúcie, v ich predstaviteľov a pod. Taktiež môžu spôsobiť hmotné aj nehmotné škody.¹⁸

Záver

V dnešnej modernej dobe široko dostupného rýchleho internetu a najrozličnejších vysoko výkonných „smart“ zariadení sa ľudia dokážu dostať k veľkému množstvu informácií veľmi rýchlo a jednoducho. Najnovšie správy či údaje sú ľahko dostupné prostredníctvom internetových webových stránok, spravodajských portálov alebo sociálnych sietí, ktoré na ne odkazujú. S narastajúcim množstvom informácií sa zvyšuje aj množstvo hoaxov. Ich cieľom je zapôsobiť na adresátov tak, aby uverili informáciám, ktoré sú v nich prezentované ako faktom, hoci hoaxy predstavujú správy, ktoré sú falošné, skreslené, pozmenené či nepravdivé (alebo aspoň z časti nepravdivé). Ukazuje sa pritom, že hoaxy ovplyvňujú mienku a názory ľudí oveľa viac, než by sa na prvý pohľad mohlo zdať.

Jedným z dôvodov prečo majú taký vplyv a prečo predstavujú problém najmä pre demokratickú spoločnosť, je ich ľahká dostupnosť pre všetkých a rýchlosť ich šírenia. K obom týmto atribútom prispelo najmä masové rozšírenie internetu a rozmach sociálnych sietí, kde predovšetkým mladí ľudia trávia až príliš veľa času a kde môže ktokoľvek rýchlo, jednoducho a zadarmo hoaxy rôzneho typu vytvárať a šíriť. Pre mnohých ľudí je často oveľa pohodlnejšie získať informácie zo sociálnych sietí ako z klasických spravodajských portálov, čo tiež prispieva

¹⁶ SITUNGKIR, H. 2021. Spread of Hoax in Social Media. In *Bandung Fe Institute*, 2021

¹⁷ UTAMI, P. 2018. Hoax in Modern Politics. In *Jurnal Ilmu Sosial dan Ilmu Politik*, 2018, roč. 22, č. 2, s. 88

¹⁸ ARBIYAH, N. a kol. 2020. The Danger of Hoax. In *Human Behaviour Studies*, 2020, roč. 24, č. 1, s. 82

k prehľbovaniu tohto problému. Na rozdiel od seriózných médií, ktoré si pred zverejnením informácie overujú jej pravdivosť z viacerých zdrojov a uvádzajú ich pri jednotlivých správach, v sociálnych sieťach doposiaľ nebol vytvorený mechanizmus, ktorý by slúžil na oddeľovanie pravdivých a nepravdivých informácií.¹⁹ Ďalším problémom je fakt (existujú o tom mnohé svedectvá a dôkazy), že množstvo priaznivcov prostredníctvom internetu a sociálnych sietí priťahujú a získavajú na svoju činnosť radikálne organizácie, ktoré šíria rôzne falošné správy v podobe hoaxov, dezinformácií a konšpiračných teórií, a tiež propagandu.

Medzi najzraniteľnejšie z hľadiska týchto rizík patria súčasné moderné demokratické štáty. Európska únia i jej členské štáty už prijímajú praktické opatrenia na neutralizáciu takýchto falošných správ, ale pre každý členský štát je dôležité mať aj vlastnú transparentnú a konkrétnu politiku, prípadne viac politík, stratégií alebo koncepcií zameraných na boj proti hoaxom, dezinformáciám, konšpiráciám a nepriateľskej propagande. Zvýšenie povedomia o falošných, klamlivých, zavádzajúcich či pozmenených správach v podobe hoaxov, zlepšenie schopnosti rozoznávať a odhaľovať ich, ako aj eliminovať ich šírenie v čo najväčšej miere by určite znamenalo menej príležitostí napríklad pre populizmus, radikalizmus, extrémizmus, xenofóbiu či akékoľvek ovplyvňovanie alebo rozdeľovanie súčasnej demokratickej spoločnosti práve na základe posúvania najrôznejších falošných správ.

V tejto súvislosti je nutné si priznať, že prevencia proti šíreniu hoaxov v súčasnej informačnej spoločnosti, je veľmi zložitá. Hoax sa prejavuje ako samostatné digitálne médium pracujúce v šedej zóne, slúžiac na šírenie dezinformácií. Nie je dostatočne zachytiteľný filtrami, ako je to napríklad v prípade spamu. Aj preto jedným z najúčinnějších preventívnych prostriedkov, resp. opatrení proti šíreniu rôznych falošných správ v podobe hoaxov je mediálna výučba, ktorej cieľom je zvýšenie mediálnej gramotnosti. Toto v praxi fungujúce opatrenie napomáha lepšie pochopiť médiá a naučiť sa s nimi pracovať. Aj keď je proces mediálnej výchovy u nás zatiaľ v plienkach, odborníci v ňom vidia veľký potenciál pre zlepšenie mediálnej gramotnosti. Každý progres si prirodzene vyžaduje svoj čas, avšak oboznámenie sa s princípom fungovania sociálnych sietí a sprístupnenie informácií o možných dôsledkoch, môže byť pozitívnym faktorom v získaní nadhľadu nad týmto typom médií všeobecne.

¹⁹ HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED2022 Proceedings Publisher: IATED*, 2022, s. 1995

Faktom je, že hoaxom sa v podstate v dnešnej informačnej spoločnosti nedá vyhnúť, ale dôležité je, aby ich človek vedel rozoznať a aby sa nimi nenechal zmanipulovať a ovplyvniť, čo môže priniesť množstvo negatívnych dôsledkov, ako pre jedincov, tak pre celú spoločnosť. Naučiť sa kriticky premýšľať o falošných správach v podobe hoaxov, môže viesť k žiadúcemu výsledku naučiť sa kriticky premýšľať aj o sociálnych sieťach a médiách a nimi šírených informáciách.

Zoznam použitej literatúry

ARBIYAH, N. a kol. 2020. The Danger of Hoax. In *Makara Human Behavior Studies in Asia*, 2020, roč. 24, č. 1, s. 80-86. ISSN 1693-6701.

DR. 2023. Global Digital Overview. In *DataReportal*, 2023. [online] [cit. 16.03.2023]. Dostupné na internete: <<https://datareportal.com/reports/digital-2022-global-overview-report>>.

GREGOR, M. a kol. *Nejlepší kniha o Fake News, dezinformacích a manipulacích!!!* Brno : CPress, 2018. 143 s. ISBN 978-80-264-1805-4.

HAJDÚKOVÁ, T. – HRUŠKA, P. 2018. Prínos siete Internet pre rozvoj spoločnosti a jeho možnosti využitia v činnosti Policajného zboru. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním*. Bratislava : Akadémia Policajného zboru v Bratislave, 2018, s. 131-142. ISBN 78-80-8054-768-4.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022 - Proceedings from 16th International Technology, Education and Development Conference*. Publisher: IATED-Spain, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

HOAX. 2023. Co je to hoax. In *Hoax.cz*, 2023. [online] [cit. 16.03.2023]. Dostupné na internete: <<https://www.hoax.cz/hoax/co-je-to-hoax>>.

KOLOUCH, J. 2016. *CyberCrime*. Praha : CZ.NIC, 2016. 524 s. ISBN 978-80-88168-18-8.

KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LOSEKOOT, M. – VYHNÁNKOVÁ, E. 2019. *Jak na sítě*. Jan Melvil publishing, 2019. 328 s. ISBN 978-80-7555-084-2.

NUTIL, P. 2018. *Média, lži a příliš rychlý mozek: průvodce postpravdivým světem*. Praha : Grada, 2018. 192 s. ISBN 978-80-271-0716-2.

SITUNGKIR, H. 2021. Spread of Hoax in Social Media. In *Bandung Fe Institute*, 2021. [online] [cit. 16.03.2023]. Dostupné na internete: <<https://ssrn.com/abstract=1831202>>.

UTAMI, P. 2018. Hoax in Modern Politics. In *Jurnal Ilmu Sosial dan Ilmu Politik*, 2018, roč. 22, č. 2, s. 85-97. ISSN 1410-4946.

YD. 2023. Hoax. In *Your Dictionary*, 2023. [online] [cit. 15.03.2023]. Dostupné na internete: <<https://www.yourdictionary.com/hoax>>.

ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224. ISBN 978-80-8054-773-8.

ZACHAR KUČTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Kontaktné údaje

plk. gšt. v. z. doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.

Katedra informatiky a manažmentu

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava

E-mail: radoslav.ivancik@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Vnímanie frekvencie výskytu hybridných hrozieb z pohľadu študentov vybraných vysokých škôl na Slovensku

Antonín Korauš, Miroslav Gombár

Anotácia

Cieľom tejto štúdie je získať hlbší pohľad na vnímanie frekvencie výskytu hybridných hrozieb zo strany študentov vysokých škôl. Táto analýza nám umožní lepšie porozumieť perspektíve študentov a ich postojom k bezpečnosti v digitálnom prostredí. Na základe týchto poznatkov môžeme vyvodiť relevantné závery a odvodenia, ktoré môžu prispieť k zlepšeniu preventívnych opatrení a osvetovej činnosti zameranej na ochranu študentov pred hybridnými hrozbami.

Kľúčové slová

hybridné hrozby, študenti vysokých škôl, vnímanie

Annotation

The aim of this study is precisely to gain a deeper understanding of the perception of the frequency of occurrence of hybrid threats by university students. This analysis will allow us to better comprehend the perspectives of students and their attitudes towards security in the digital environment. Based on these findings, we can draw relevant conclusions and derivations that can contribute to the improvement of preventive measures and educational activities aimed at protecting students from hybrid threats.

Key words

hybrid threats, university students, perception.

Úvod

V dnešnej digitálnej ére sme svedkami rýchleho technologického pokroku, ktorý prináša so sebou množstvo výhod, ale aj nové bezpečnostné výzvy. S rozširovaním digitálnych technológií a závislosťou na online prostredí sa otvára priestor pre rôzne formy hrozieb, ktoré sa šíria medzi používateľmi. Jednou z týchto hrozieb je fenomén hybridných hrozieb, ktoré kombinujú fyzické a kybernetické prvky s cieľom narušiť, poškodiť alebo manipulovať s cieľovými jednotkami.

V kontexte hybridných hrozieb osobitnú pozornosť zameriavame na študentov vybraných vysokých školách, ktoré slúžia pre mladých ľudí, ktorí sa pripravujú na svoju budúcu kariéru a sú aktívnymi užívateľmi digitálnych technológií. S nárastom digitálnych platforiem a pripojenosti na internet sa stávajú študenti vysokých škôl zraniteľnejšími voči hybridným hrozbám.

V tomto kontexte je dôležité preskúmať vnímanie frekvencie výskytu hybridných hrozieb zo strany študentov vysokých škôl. Ako vnímajú tieto hrozby? Považujú ich za častý jav alebo za

niečo vzácne a výnimočné? Aké sú ich skúsenosti s týmito hrozbami a ako sa to prejavuje vo vzťahu k ich povedomiu o bezpečnosti a ochrane?

Cieľom tejto štúdie je práve získať hlbší pohľad na vnímanie frekvencie výskytu hybridných hrozieb zo strany študentov vybraných vysokých škôl. Táto analýza nám umožní lepšie porozumieť názorom študentov a ich postojom k bezpečnosti v digitálnom prostredí. Na základe týchto poznatkov môžeme vyvodiť relevantné závery a odvodenia, ktoré môžu prispieť k zlepšeniu vzdelávacích aktivít študentov zameraných na hybridné hrozby.

Naša štúdia sa zakladá na kvantitatívnom prieskume medzi populáciou študentov vysokých škôl, ktorý poskytne široký a reprezentatívny pohľad na vnímanie frekvencie výskytu hybridných hrozieb zo strany študentov vybraných vysokých škôl.

Vnímanie frekvencie výskytu hybridných hrozieb z pohľadu študentov vysokých škôl môže byť ovplyvnené niekoľkými faktormi. Tu je niekoľko dôležitých faktorov, ktoré môžu mať vplyv na toto vnímanie:

- Informovanosť: Úroveň informovanosti študentov o hybridných hrozbách môže značne ovplyvniť ich vnímanie frekvencie výskytu. Ak študenti majú dostatok informácií o týchto hrozbách, môžu mať tendenciu vnímať ich ako častejšie, keďže majú lepšie povedomie o tom, čo sa deje v digitálnom svete.
- Skúsenosti: Skúsenosti so skutočnými prípadmi hybridných hrozieb môžu mať významný vplyv na vnímanie frekvencie výskytu. Ak študenti mali osobné skúsenosti s takýmito hrozbami, môžu ich vnímať ako častejšie a reálnejšie.
- Média a správy: Správy v médiách o hybridných hrozbách môžu tiež formovať vnímanie frekvencie výskytu. Ak sa tieto hrozby často objavujú v médiách, môže to vytvoriť dojem, že sa vyskytujú častejšie, než tomu skutočne je.
- Bezpečnostné opatrenia: Úroveň bezpečnostných opatrení prijímaných vysokými školami môže mať tiež vplyv na vnímanie frekvencie výskytu hybridných hrozieb. Ak sú študenti informovaní o opatreniach, ktoré sa prijímajú na ochranu pred týmito hrozbami, môžu mať pocit väčšej bezpečnosti a vnímať ich menej často.
- Osobné vnímanie rizika: Každý jednotlivý študent môže mať svoje vlastné vnímanie rizika a bezpečnosti. Niektorí môžu byť citlivejší na hybridné hrozby a vnímať ich ako častejšie, zatiaľ čo iní môžu mať tendenciu ich podceňovať a vnímať ich ako menej časté.

Je dôležité si uvedomiť, že vnímanie frekvencie výskytu hybridných hrozieb môže byť medzi študentmi vysokých škôl výrazne variabilné, a to aj vzhľadom na individuálne faktory a skúsenosti.

Výskumná časť

Výskumnú vzorku v zmysle tab.1 tvorilo celkovo 252 mužov a 400 žien. V rámci analýzy definovaných hypotéz sme si stanovili ako relevantné vstupné premenné StupenS (Stupeň štúdia) a FormaS (Forma štúdia). Výskumná vzorka teda bola tvorená študentami dvoch vybraných vysokých škôl na území Slovenskej republiky. Podrobnejšia analýza výskumnej vzorky z pohľadu troch relevantných vstupných premenných je uvedená v tab.1.

Tabuľka 1 Popis výskumnej vzorky

Summary Table for all Multiple Response Items Totals/percentages based on number of respondents Multiple identical responses were ignored					
	N=652 Rod	StupenS	FormaS denná forma štúdia	FormaS externá forma štúdia	Row Totals
Count	muž	bakalárske štúdium	58	40	98
Column %			43,94%	33,33%	
Row %			59,18%	40,82%	
Table %			23,02%	15,87%	38,89%
Count		magisterské štúdium	72	60	132
Column %			54,55%	50,00%	
Row %			54,55%	45,45%	
Table %			28,57%	23,81%	52,38%
Count		doktorandské štúdium	2	20	22
Column %			1,52%	16,67%	
Row %			9,09%	90,91%	
Table %			0,79%	7,94%	8,73%
Count		Total	132	120	252
Table %			52,38%	47,62%	100,00%
Count	žena	bakalárske štúdium	92	14	106
Column %			41,82%	7,78%	
Row %			86,79%	13,21%	
Table %			23,00%	3,50%	26,50%
Count		magisterské štúdium	126	144	270
Column %			57,27%	80,00%	
Row %			46,67%	53,33%	
Table %			31,50%	36,00%	67,50%
Count		doktorandské štúdium	2	22	24
Column %			0,91%	12,22%	
Row %			8,33%	91,67%	
Table %			0,50%	5,50%	6,00%

Count		Total	220	180	400
Table %			55,00%	45,00%	100,00%

Zdroj: vlastné spracovanie

V rámci výskumu v oblasti hybridných hrozieb, sme si teda položili základnú výskumnú otázku: Ako vnímajú respondenti, študenti vysokých škôl pojem hybridné hrozby. Od tejto primárnej výskumnej otázky sa odvodili aj ďalšie: Je rozdiel vo vnímaní pojmu hybridných hrozieb z pohľadu rodu, stupňa a formy štúdia? Na základe definovaných výskumných otázok sa stanovili tri základné výskumné hypotézy:

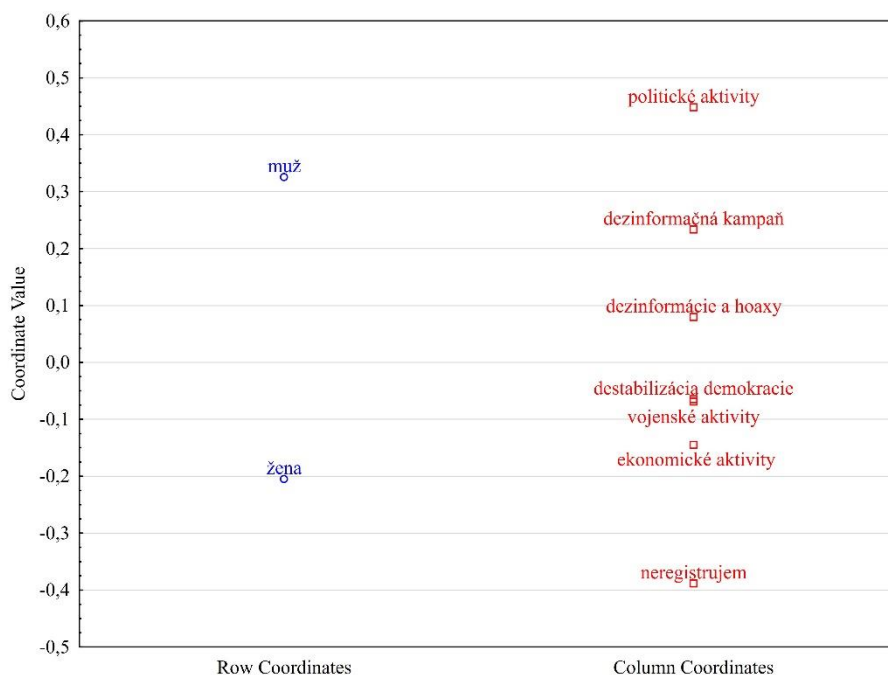
H_1 : Existuje signifikantný vzťah medzi rodom respondenta a vnímaním pojmu hybridných hrozieb na zvolenej hladine významnosti $\alpha = 5 \%$.

H_2 : Existuje signifikantný vzťah medzi stupňom štúdia respondenta a vnímaním pojmu hybridných hrozieb na zvolenej hladine významnosti $\alpha = 5 \%$.

H_3 : Existuje signifikantný vzťah medzi formou štúdia respondenta a vnímaním pojmu hybridných hrozieb na zvolenej hladine významnosti $\alpha = 5 \%$.

Ako základný spôsob analýzy stanovených hypotéz sme si zvolili viacrozmernú štatistickú metódu, korešpondenčnú analýzu. Prvým zaujímavým zistením v rámci analýzy prvej výskumnej hypotézy je skutočnosť, že až 21.779 % respondentov nezaregistrovala pojem hybridných hrozieb. Z toho je to 11.111 % oslovených mužov a 28.500 oslovených žien. Hybridné hrozby ako koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine vníma celkovo 13.191 % z čoho sa k tejto možnosti priklonilo 20.635 % mužov a 8.500 % žien. Ďalšou možnosťou v rámci výskumného nástroja bolo vnímanie pojmu hybridné hrozby ako koordinovanej aktivity, ktorej cieľom je destabilizovať demokraciu v inej krajine. K tejto odpovedi sa priklonilo celkovo 9.509 % (8.730 % mužov a 10.000 % žien). Využívanie rôznorodých aktivít, ktoré využívajú dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine si zvolilo celkovo 38.957 % respondentov, pričom túto možnosť si zvolilo 42.857 % mužov a 36.500 % žien. Hybridné hrozby ako koordinovanú vojenskú aktivitu, ktorej cieľom je narušenie politického systému inej krajiny, koordinovanú dezinformačnú kampaň, ktorej cieľom je podkopanie dôvery k politickým elitám inej krajiny a koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny si zvolilo približne rovnaké percento respondentov na úrovni cca 5 %. Ak budeme analyzovať prvú výskumnú hypotézu tak na základe dosiahnutej hladiny významnosti $p = 0.000$ ($\chi^2 = 43.507$, $df = 6$) je možné prijať záver, že rod respondenta má vzťah k

vnímaniu hybridných hrozieb na zvolenej hladine významnosti 5 %. Detailnejšie výsledky prinášame na obr.1. Ak prijeme výsledok analýzy prvej hypotézy ako platný, tak pomocou korešpondenčnej mapy je možné sledovať z pohľadu rodu preferenciu, ako je vnímaný pojem hybridné hrozby. Z obr.1 je teda zrejmé, že muži chápu pojem hybridné hrozby prioritne ako koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine a koordinovanú dezinformačnú kampaň, ktorej cieľom je podkopať dôveru k politickým elitám inej krajiny. Na druhej strane, ženy vnímajú pojem hybridné hrozby predovšetkým ako koordinovanú aktivitu, ktorej cieľom je destabilizovať demokraciu v inej krajine, koordinovanú vojenskú aktivitu, ktorej cieľom je narušenie politického systému inej krajiny, koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny resp. až 28.500 % žien tento pojem neregistruje ako problém. Zaujímavú pozíciu má vnímanie hybridných hrozieb respondentami ako rôznorodé aktivity využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine, kde muži (42.857 %) a ženy (36.500 %) túto možnosť preferujú.

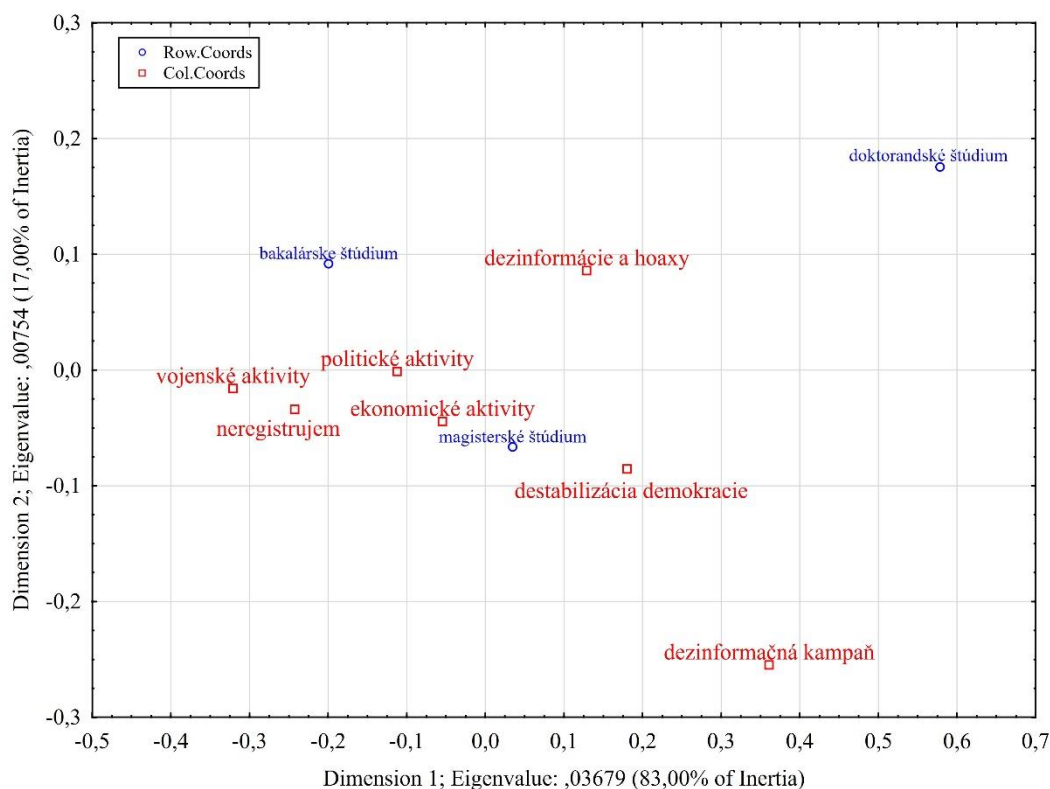


Obrázok 1 Korešpondenčná mapa analýzy prvej výskumnej hypotézy

Zdroj: vlastné spracovanie

Druhá stanovená výskumná hypotéza sa dotýka vzťahu stupňa štúdia respondenta a jeho vnímania pojmu hybridné hrozby. Najväčšie zastúpenie vnímania hybridných hrozieb medzi

respondentami má vnímanie hybridných hrozieb ako rôznorodých aktivít využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine. Túto možnosť, tak ako bolo uvedené vyššie si zvolilo až 38.957 %. Z celkového počtu 204 študentov bakalárskeho štúdia (ďalej ako Bc.) si práve túto možnosť zvolilo 37.255 %, z celkového počtu 402 študentov magisterského štúdia (ďalej ako Mgr.) si túto možnosť zvolilo 37.313 % a z celkového počtu 46 študentov doktorandského štúdia (ďalej ako PhD.) si túto možnosť zvolilo 60.859 % študentov. Pojem hybridné hrozby neregistruje až 21.779 % všetkých študentov, pričom túto možnosť si zvolilo 26.471 % študentov Bc., 21.393 % študentov Mgr. ale iba 4.348 % študentov PhD. Hybridné hrozby ako koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine vníma celkovo 13.190 %. Túto možnosť si zvolilo celkovo 14.706 % študentov Bc., 12.935 % študentov Mgr. a 8.696 % študentov PhD. Ďalšie z pohľadu početnosti výskytu bolo priradenie pojmu hybridných hrozieb možnosti, že sa jedná o koordinovanú aktivitu, ktorej cieľom je destabilizovať demokraciu v inej krajine, pričom túto možnosť si zvolilo 6.863 % študentov Bc., 10.448 % študentov Mgr. a 13.043 % študentov PhD. Tu teda vnímame, že so zvyšujúcim sa stupňom štúdia, respondenti prikladajú tejto možnosti vyššiu dôležitosť. Hybridné hrozby ako koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny vníma 5.882 % študentov Bc., 5.970 % študentov Mgr. a 4.348 % študentov PhD. V tejto možnosti pozorujeme pomerne vyrovnané hodnotenie bez ohľadu na stupeň štúdia respondentov. Pomerne zaujímavé je vnímanie hybridných hrozieb ako koordinovanej dezinformačnej kampane, ktorej cieľom je podkopanie dôvery k politickým elitám inej krajiny, kde iba 1.961 % študentov Bc. si zvolilo túto možnosť, 6.965 % študentov Mgr. a 8.696 % študentov PhD. štúdia. Ak budeme analyzovať druhú výskumnú hypotézu tak na základe dosiahnutej hladiny významnosti $p = 0.0041$ ($\chi^2 = 28.9002$, $df = 12$) je možné prijať záver, že stupeň štúdia respondenta má vzťah k vnímaniu hybridných hrozieb na zvolenej hladine významnosti 5 %. Detailnejšie výsledky prinášame na obr.2.

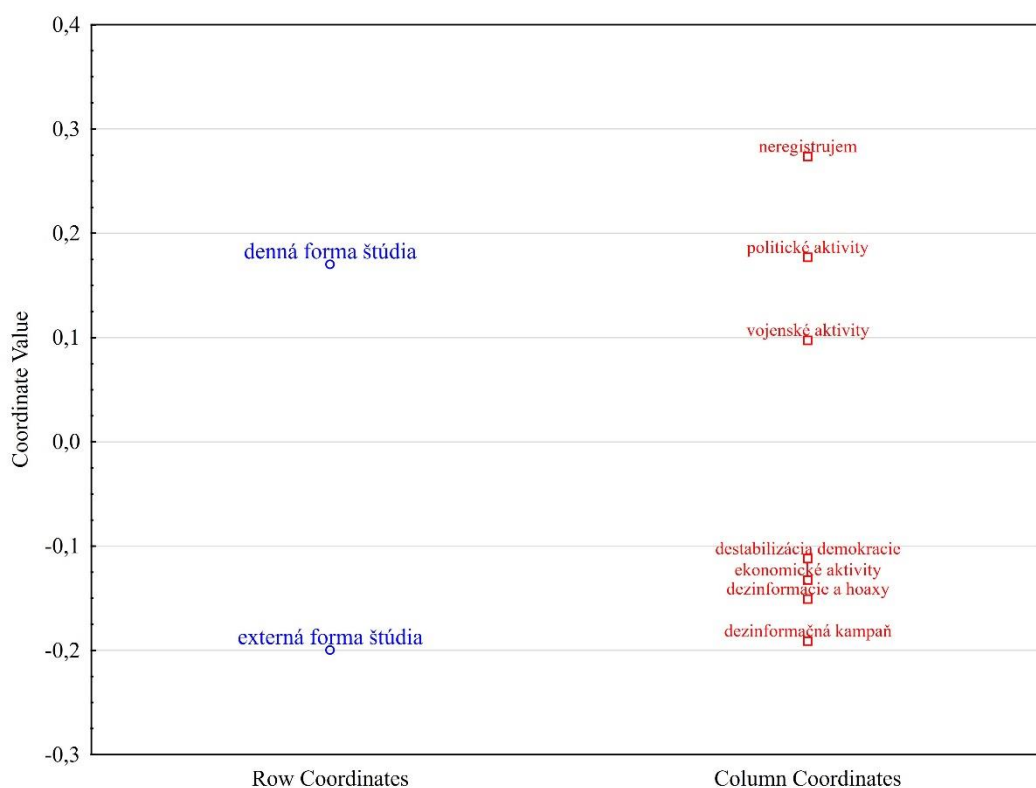


Obrázok 2 Korešpondenčná mapa analýzy druhej výskumnej hypotézy
Zdroj: vlastné spracovanie

Z obr.2 je teda zrejmé, že študenti bakalárskeho štúdia vnímajú hybridné hrozby predovšetkým ako rôznorodé aktivity využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine. Študenti magisterského štúdia si prioritne chápu hybridné hrozby ako: koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny (5.790 %), koordinovanú aktivitu, ktorej cieľom je destabilizovať demokraciu v inej krajine (10.448 %), koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine (12.936 %), koordinovanú vojenskú aktivitu, ktorej cieľom je narušenie politického systému inej krajiny (4.975 %) a súčasne hybridné hrozby neregistruje 21.393 % študentov magisterského štúdia.

Tretia stanovená výskumná hypotéza sa dotýka vzťahu formy štúdia respondenta a jeho vnímania pojmu hybridné hrozby. Táto vstupná premenná, forma štúdia, bola volená za účelom porovnania študentov s vekom od 19 do 24 rokov (22.30 rokov), ktorí nemajú pracovné skúsenosti, so študentami externého štúdia, ktorí majú priemerne vyšší vek (31.15 rokov) ako prvá skupina a súčasne predpokladáme, že v rámci tejto skupiny, respondenti už pracujú. Najčastejšiu voľbu pre

definovanie hybridnej hrozby a to rôznorodé aktivity využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine si zvolilo 33.523 % študentov denného štúdia a až 45.333 % študentov externého štúdia. Ďalšia zaujímavé diferencie pozorujeme pri možnosti „neregistrujem“, kde túto možnosť si zvolilo 27.272 % študentov denného štúdia a 15.333 % študentov externého štúdia a pri možnosti „koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine“ kde túto možnosť si zvolilo 15.341 % študentov denného a 10.667 % študentov externého štúdia. V prípade ostatných možností, sú rozdiely v početnosti odpovedí minimálne a obe skupiny je možné v týchto položkách považovať za homogénne. Ak budeme analyzovať tretiu výskumnú hypotézu tak na základe dosiahnutej hladiny významnosti $p = 0.0011$ ($\chi^2 = 22.176$, $df = 6$) je možné prijať záver, že forma štúdia respondenta má vzťah k vnímaniu hybridných hrozieb na zvolenej hladine významnosti 5 %. Detailnejšie výsledky prinášame na obr.3.



Obrázok 3 Korešpondenčná mapa analýzy tretej výskumnej hypotézy

Zdroj: vlastné spracovanie

Z obr.3 je teda zrejmé, že študenti denného štúdia chápu pojem hybridné hrozby ako: koordinovanú vojenskú aktivitu, ktorej cieľom je narušenie politického systému inej krajiny,

koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine resp. neregistrujú tento pojem. Na druhej strane študenti externého štúdia vnímajú hybridné hrozby ako: koordinovanú aktivitu, ktorej cieľom je destabilizovať demokraciu v inej krajine (10.667 %), koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny (6.667 %), rôznorodé aktivity využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine (45.333 %) a koordinovanú dezinformačnú kampaň, ktorej cieľom je podkopať dôveru k politickým elitám inej krajiny (6.667 %).

Záver

Záverom je potrebné konštatovať, že všetky tri stanovené výskumné hypotézy sa na základe aplikácie korešpondenčnej analýzy potvrdili. Je možné prijať záver: vnímanie hybridných hrozieb je signifikantne podmienené ako rodom respondenta, stupňom aj formou štúdia. V rámci predloženej štúdie sa analyzovali názory na chápanie pojmu hybridné hrozby medzi študentami vysokých škôl a výsledky nás oprávňujú konštatovať, že vo všetkých analyzovaných skupinách chýba komplexné vnímanie tohto závažného problému.

Vnímanie frekvencie výskytu hybridných hrozieb zo strany študentov vybraných vysokých škôl je dôležitým faktorom v súvislosti s bezpečnosťou a ochranou študentov v digitálnom prostredí. Na základe analýzy a výsledkov tejto štúdie sme získali užitočné informácie o tom, ako študenti vnímajú tieto hrozby a aký vplyv majú na ich povedomie o bezpečnosti.

Vnímanie frekvencie hybridných hrozieb je subjektívnym procesom a môže sa líšiť medzi jednotlivými študentmi. Skúsenosti so skutočnými prípadmi hybridných hrozieb a úroveň informovanosti môžu ovplyvniť, ako často študenti považujú tieto hrozby za výskyt. Zároveň sme zistili, že médiá a verejná diskusia majú tiež vplyv na vnímanie frekvencie týchto hrozieb.

Preto je dôležité zvýšiť informovanosť a poskytovať vzdelávacie programy zamerané na hybridné hrozby pre študentov vysokých škôl. Vytvorenie spolupráce medzi vysokoškolskými inštitúciami, bezpečnostnými organizáciami a študentmi môže pomôcť zlepšiť povedomie o týchto hrozbách a zvýšiť úroveň bezpečnosti v digitálnom prostredí.

Okrem toho by sa mal podporovať výskum a inovácie v oblasti kybernetickej bezpečnosti, aby bolo možné sa lepšie vyrovnávať s novými formami hybridných hrozieb. Kontinuálne

monitorovanie a analýza týchto hrozieb pomôžu identifikovať nové trendy a vyvinúť efektívne opatrenia na ochranu študentov.

Vnímanie frekvencie výskytu hybridných hrozieb je dynamickou oblasťou, ktorá sa mení s technologickým vývojom a novými hrozbami. Preto je nevyhnutné, aby sa neustále sledoval tento vývoj a prispôbovali sa bezpečnostné opatrenia a vzdelávacie aktivity tak, aby boli efektívne a aktuálne.

Pod'akovanie

Príspevok vznikol v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zoznam použitej literatúry

Avery, R. J., Bryant, W. K., Mathios, A., Kang, H., & Bell, D. (2006). Electronic course evaluations: Does an online delivery system influence student evaluation? *The Journal of Economic Education*, 37(1), 21–37. <https://doi.org/10.3200/JECE.37.1.21-37>

Arcos, R.; Smith, H. (2021) Digital Communication and Hybrid Threats, REVISTA ICONO 14-REVISTA CIENTIFICA DE COMUNICACION Y TECNOLOGIAS, Volume 19, Issue 1, Page 1-14. DOI 10.7195/ri14.v19i1.1662

Balcaen, P.; Du Bois, C.; Buts, C.: (2022) A Game-theoretic Analysis of Hybrid Threats. DEFENCE AND PEACE ECONOMICS. Volume 33. Issue 1. Page 26-41. DOI 10.1080/10242694.2021.1875289

Bazarkina, D.: (2021) Evolution of Approaches to Countering Hybrid Threats in the European Union's Strategic Planning. CONTEMPORARY EUROPE-SOVREMENNAYA EVROPA. Issue 6. Page 133-143. DOI 10.15211/soveurope62021133143

Berk, R. A. (2012). Top 20 strategies to increase the online response rates of student rating scales. *International Journal of Technology in Teaching and Learning*, 8(2), 98–107.

Berzins, J. (2018). Countering hybrid threats: the European Union's response. *Contemporary Security Policy*, 39(3), 417-440.

Bratko, A.; Zaharchuk, D.; Zolka, V. (2021) Hybrid warfare - a threat to the national security of the state. *REVISTA DE ESTUDIOS EN SEGURIDAD INTERNACIONAL-RESI*. Volume 7. Issue 1. Page 147-160. DOI 10.18847/1.13.10

Čavojský, M., & Szalay, L. (2019). Hybrid Threats and Slovakia's Security Environment. In 31st International Scientific Conference on Economic and Social Development - "Legal Challenges of Modern World" (pp. 491-500). Varazdin Development and Entrepreneurship Agency.

Galinec, D.; Steingartner, W.; Zebic, V.: (2019) Cyber Rapid Response Team: An Option within Hybrid Threats. Book Group Author: IEEE 15TH INTERNATIONAL SCIENTIFIC CONFERENCE ON INFORMATICS. Page 43-49. Poprad, SLOVAKIA. NOV 20-22, 2019

Giegerich, B., & Mutschler, M. (Eds.). (2017). *The Routledge handbook of hybrid warfare and hybrid threats*. Routledge.

Korauš, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. *RELIK 2022*. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

Mazaraki, A.; Kalyuzhna, N.; Sarkisian, L.: (2021) MULTIPLICATIVE EFFECTS OF HYBRID THREATS. *BALTIC JOURNAL ECONOMIC STUDIES*. Volume 7. Issue 4. Page 136-144. DOI 10.30525/2256-0742/2021-7-4-136-144

NATO StratCom COE. (2018). *NATO StratCom COE Handbook on Hybrid Warfare: A Guide to the Dark Art*. NATO Strategic Communications Centre of Excellence.

Rid, T., & Hecker, M. (Eds.). (2018). *Hybrid threats: Reconceptualizing the challenges to global security*. Georgetown University Press.

Steingartner, W.; Galinec, D.: (2021) Cyber Threats and Cyber Deception in Hybrid Warfare Volume 18. Issue 3. Page 25-45. *ACTA POLYTECHNICA HUNGARICA*. ISSN: 1785-8860

Tkachuk, I.V.; Shynkarenko, R.S.; Tokovenko, O.S.; Svorak, S.D.; Lavoryk, A.V.: (2021) HYBRID THREATS AND THE TRANSFORMATION OF THE STATE POLITICAL INSTITUTE: A NEO-INSTITUTIONAL APPROACH. *AD ALTA-JOURNAL OF*

Kontaktné údaje

prof. Ing. Antonín Korauš, PhD., LL.M., MBA
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 35,
Slovak Republic
E-mail: antonin.koraus@akademiapz.sk

doc. Ing. Miroslav Gombár, PhD.
Fakulta manažmentu, ekonomiky a obchodu,
Prešovská univerzita v Prešove,
Konštantínova 16, Prešov.
E-mail: miroslav.gombar@unipo.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA
doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Kybernetická bezpečnosť v krajinách EÚ so zameraním na Slovenskú republiku

Cybersecurity in EU countries with focus on the Slovak Republic

Antonín Korauš, Beáta Stehlíková, Kristián Újváry

Abstrakt

Hybridné hrozby, medzi ktoré patria aj kybernetické útoky vzbudzujú stále väčšie obavy. Preto sa hľadajú vhodné riešenia. Jedným z nástrojov, ktoré tu možno nasadiť, je globálny index kybernetickej bezpečnosti (GCI), mechanizmus kontroly a spätnej väzby založený na zloženom indikátore. V príspevku hodnotíme stav kybernetickej bezpečnosti v krajinách EÚ pomocou Globálneho indexu kybernetickej bezpečnosti GCI. Použitím zhlukovej analýzy odhaľujeme skupiny štátov s podobnými hodnotami pilierov GCI. Slovensko patrí do skupiny štátov, ktoré potrebujú zvýšiť Kooperatívne opatrenia. Poukazujeme, že práve tu je priestor pre verejnú správu, aby pomohla zvýšiť národnú kybernetickú bezpečnosť.

Kľúčové slová

GCI, zhluková analýza, kooperatívne opatrenia, hybridné hrozby kybernetická bezpečnosť

Abstact

Hybrid threats, including cyber-attacks, are a growing problem. Appropriate solutions are therefore being sought. One tool that can be used here is the Global Cyber Security Index (GCI), a control and feedback mechanism based on a composite indicator. In this paper, we assess the state of cybersecurity in EU countries using the Global Cybersecurity Index GCI. Using cluster analysis, we reveal groups of countries with similar GCI pillar values. Slovakia belongs to the group of countries that need to increase cooperative measures. We point out that this is where there is room for the public administration to help enhance national cybersecurity.

Key words

GCI, cluster analysis, cooperative measures, hybrid treats, cybersecurity

Úvod

Spoločnosť je čoraz viac závislá od technológií a internetu. Využívanie kybernetického priestoru narastá. Narastá tiež počet rôznych kybernetických útokov, ktoré sú formou hybridnej hrozby. Kybernetická bezpečnosť sa tak stáva čoraz dôležitejšou. EÚ pôsobí na rôznych frontoch, kde sa usiluje podporiť kybernetickú odolnosť, bojovať proti počítačovej kriminalite a posilniť kybernetickú diplomaciu a obranu, konštatuje Európska rada a Rada EÚ (2023). Vzhľadom na zvýšený počet sofistikovaných kybernetických útokov na verejnú správu EÚ navrhla Európska

komisia v marci 2022 opatrenia zamerané na zabezpečenie **vysokej spoločnej úrovne kybernetickej bezpečnosti**.

Stav kybernetickej bezpečnosti sa v rôznych krajinách značne odlišný. Pre objektívne hodnotenie kybernetickej bezpečnosti v krajinách môžeme použiť medzinárodné indexy kybernetickej bezpečnosti. Na meranie kybernetickej bezpečnosti bolo navrhnutých niekoľko viacerých indexov, ktoré merajú kybernetickú bezpečnosť štátov z rôznych pohľadov. Khudyntsev et al. (2022) popisujú 65 existujúcich indexov kybernetickej bezpečnosti a prístupy k ich tvorbe. Uvádzajú tiež vymedzenie pojmov potrebných na analýzu ratingu v oblasti informačnej bezpečnosti a kybernetickej bezpečnosti. Článok Kravets (2019) poskytuje komparatívnu analýzu štruktúry, metodík a aplikácií najznámejších medzinárodných indexov kybernetickej bezpečnosti: Global Cybersecurity Index (GCI), National Cybersecurity Index (NCSI) a Indexu kybernetickej bezpečnosti (ICSGCI a NCSI majú podobný okruh hodnotiacich respondentov, sú dôveryhodnejšie od ostatných vďaka overovaniu údajov. Overenie údajov pre ICS sa neuplatňuje. GCI obsahuje najrozsiahlejšiu sadu ukazovateľov. NCSI je najpresnejší, odráža aktuálnu situáciu v kybernetickej bezpečnosti a má online nástroje na spracovanie údajov. ICS je jedinečný v hodnotení nie krajín, ale je zameraný na riziká, t.j. pravdepodobnosť hrozieb, aktivitu aktérov kybernetických útokov a podobne. Porovnaním medzinárodných indexov kybernetickej bezpečnosti sa zaoberal aj Sharkov, G. (2020). Çifci (2022) v článku analyzuje a porovnáva indexy hodnotenie kybernetickej bezpečnosti a kybernetickej sily z hľadiska ich komplexnosti a sily na meranie kapacít na úrovni krajiny. Na porovnanie autor vytvoril koncepčný rámec pokrývajúci všetky ukazovatele známych indexov a možno ho použiť aj ako nový komplexný model na meranie kybernetických schopností na národnej úrovni. Tento článok je jedinečný z hľadiska počtu, časovej aktualizácie a rôznorodosti indexov.

GCI je založený na hierarchii čiastkových ukazovateľov. Bruggemann et al. (2022) poukazujú na mimoriadnu dôležitosť pilierov Technické opatrenia, Budovanie kapacít a Spolupráca.

ITU expresne reaguje na novú situáciu v oblasti kybernetickej bezpečnosti, predovšetkým zmien vyvolaných AI. Posledná aktualizácia ukazovateľov GCI bola v roku 2021. Oh a Youm (2022) využitím SWOT analýzy stanovili i základné princípy zlepšovania a využívania GCI a navrhli nové ukazovatele súvisiace s dotazníkom GCI verzie 5. Takto upravený index GCI by mal prispieť k

zvýšení účinnosti GCI a národnej schopnosti kybernetickej bezpečnosti. Cieľom práce Polotaja et al. (2020) je aplikovať predikčné metódy na vytvorenie predikcie globálneho indexu kybernetickej bezpečnosti GCI na Ukrajine.

V literatúre nájdeme aj ďalšie súvislosti GCI a ďalšími faktormi – či už ekonomickými alebo bezpečnostnými. V článku Leahovcenco (2021) je vykonaná analýza tesnosti vzťahu medzi podielom digitálnej ekonomiky na HDP a indexom GCI pomocou korelačnej analýzy. Podľa zistení Leahovcenco (2021) vyšší je podiel digitálnej ekonomiky na HDP indikuje vyšší index GCI. Korelácia medzi GCI, indexmi rozvoja informačnej spoločnosti (IDI, NRI, EGDI) a HDP na obyvateľa podľa Yerina, Honchar a Zaiets (2021) potvrdzuje, že digitálna transformácia ekonomiky a spoločnosti pôsobí ako kľúčová hnacia sila ekonomického rozvoja len vtedy, ak je zabezpečená informačná a kybernetická bezpečnosť. Yerina, Honchar a Zaiets (2021) v článku zdôrazňujú najlepšie postupy a identifikujú sa kriticky slabé segmenty národnej kybernetickej bezpečnosti. Výsledky zistil, že rozvoj informačných a telekomunikačných technológií koreluje s rozvojom inovácií a ekonomickej aktivity.

Podľa Yerina, Honchar a Zaiets (2021) v krajinách s vysokým stupňom ekonomického rozvoja, ktorý je do značnej miery založený na príspevku IT technológií k národnej produkcii, je potenciál kybernetickej bezpečnosti výrazne vyšší, bez ohľadu na lokáciu. Podľa Kravetsa (2019) existuje tendencia k nesúladu úrovne kybernetickej bezpečnosti s rozvojom informačnej a telekomunikačnej infraštruktúry. Farahbod, Shayo a Varzandeh (2020) zistili, že IDI je relatívne lepší prediktor ako GCI alebo NCSI na odhad pomeru ročných strát spôsobených počítačovou kriminalitou pre každú krajinu v porovnaní s hrubým národným produktom. Cieľom štúdie Samada (2022) je *poskytnúť alternatívne riešenia s cieľom optimalizovať verejné služby Štátnej spravodajskej služby Indonézie formou hodnotenia bezpečnosti v intenciách indexu GCI 2020.*

Materiál a metódy

V článku budeme pracovať s GCI. Globálny index kybernetickej bezpečnosti (GCI) publikuje Medzinárodná telekomunikačná únia (ITU). Index GCI pomáha identifikovať oblasti potrebných zlepšit', ktoré sa týkajú vnútroštátnych opatrení v oblasti kybernetickej bezpečnosti. Global Cyber Security Index mapuje kybernetickú bezpečnosť štátu pomocou 82 otázok zhrnutých do 20 indikátorov, ktoré tvoria päť pilierov:

- Legislatívny pilier obsahuje opatrenia založené na existencii právnych inštitúcií a rámcov zaoberajúcich sa kybernetickou bezpečnosťou a počítačovou kriminalitou;
- Technický pilier zahŕňa opatrenia založené na existencii technických inštitúcií a rámcov zaoberajúcich sa kybernetickou bezpečnosťou;
- Organizačný pilier obsahuje opatrenia založené na existencii inštitúcií na koordináciu politík a stratégií rozvoja kybernetickej bezpečnosti na národnej úrovni;
- Pilier budovania kapacít je zameraný na opatrenia založené na existencii výskumných a vývojových, vzdelávacích a školiacich programov; agentúr verejného sektora podporujúce budovanie kapacít.
- Pilier spolupráce je založený opatreniach založených na existencii partnerstiev, kooperatívnych rámcov a sietí zdieľania informácií.

Na spracovanie údajov sme použili analýzu hlavných komponentov (PCA). PCA nám umožňuje sumarizovať a vizualizovať informácie v súbore údajov obsahujúcom pozorovania popísané viacerými vzájomne korelovanými kvantitatívnymi premennými. Hlavné komponenty zodpovedajú lineárnej kombinácii pôvodných premenných. Jedným z kritérií pre voľbu počtu hlavných komponentov vychádza z kumulatívneho percentuálneho podielu na celkovej variancii, ktorá je zachytená hlavnými komponentami. Obvykle sa udáva hodnota minimálne 70 percent (Blighe, Lun; 2021).

Na znázornenie výsledkov sme použili biplot, ktorý umožňuje grafické zobrazenie informácií o pozorovaniach aj premenných dátovej matice v jedinom grafe. Relatívna súradnice objektu môžeme priblížiť premietnutím bodu na príslušný vektor v biplote. Euklidovská vzdialenosť medzi dvoma objektmi (bodmi) neaproximuje vzdialenosti medzi ich riadkami v pôvodnej matici, ale ich štandardizovanú vzdialenosť, ktorá je druhou odmocninou Mahalanobisovy vzdialenosti.

Skupiny podobných krajín z hľadiska hodnotených faktorov sme identifikovali pomocou zhlukovej analýzy. Zhlukovateľnosť údajov sme overili pomocou Hopkinsovej štatistiky. Počet zhlukov sme určili pomocou procedury NbClust, ktorý navrhuje užívateľovi najlepšiu schému zhlukovania z rôznych výsledkov získaných zmenou všetkých kombinácií počtu zhlukov, mier vzdialenosti a metód zhlukovania.

Výsledky a diskusia

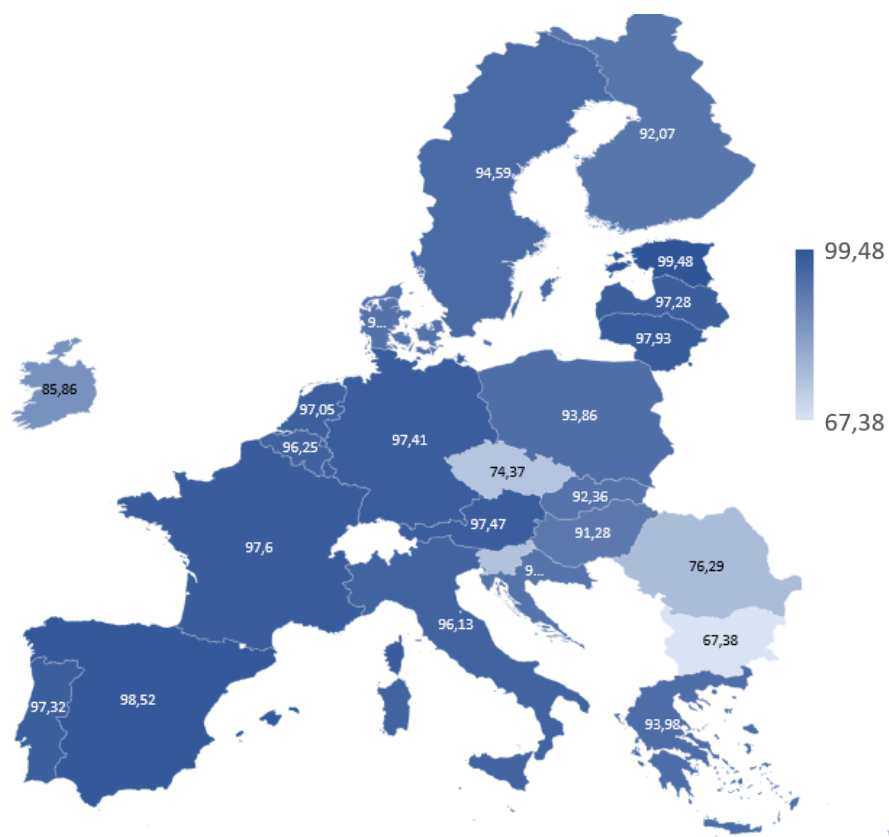
V roku 2020 sa Spojené štáty americké umiestnili na prvom mieste a dosiahli maximálne skóre 100 bodov. Medzi krajinami s najvyšším záväzkom v oblasti kybernetickej bezpečnosti sa Spojené kráľovstvo a Saudská Arábia delili o druhé a tretie miesto so skóre GCI 99,54 pre každú z nich. Z krajín EÚ najlepšie sa umiestnilo Estónsko na štvrtom mieste so skóre 99,48.

Podľa GCI 2020 reportu sa Slovensko umiestnilo na 38. mieste v rebríčku 194 krajín². V rámci piatich pilierov sa Slovensko umiestnilo nasledovne:

- Právne opatrenia (20,00): 44. miesto
- Technické opatrenia(20,00): 39. miesto
- Organizačné opatrenia(18,64): 38. miesto
- Rozvoj kapacít (17,50): 37. miesto
- Kooperatívne opatrenia (16,22): 33. miesto

V správe z roku 2020 sú uvedené silné stránky SR – Právne a Technické opatrenia. Oblasťou potencionálneho rastu sú Kooperatívne opatrenia.

Na kartograme Obrázok 1 sú znázornené krajiny EÚ.



Obrázok 1 Hodnoty GCI v krajinách EÚ v roku 2020

Zdroj: Vlastné znázornenie údajov GCI

Medzi piliermi GCI existuje priama lineárna závislosť. Väčšina z nich je štatisticky významná (Tabuľka 1). Najsilnejšia závislosť je medzi právnymi a technickými opatreniami.

Tabuľka 1 Korelačné koeficienty medzi piliermi GCI 2020

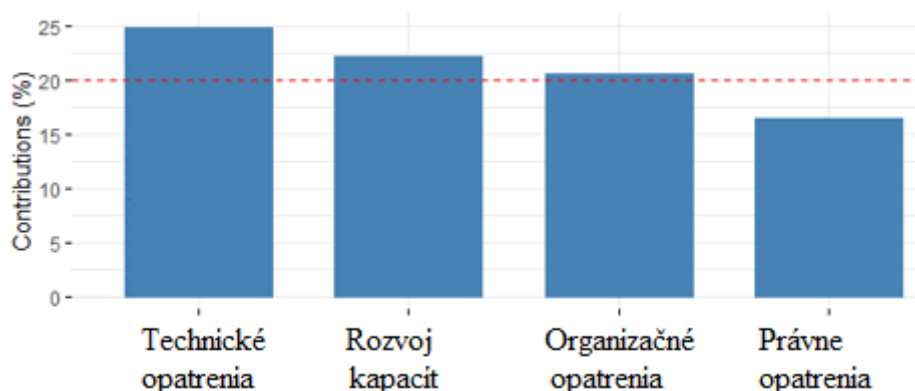
	Právne opatrenia	Technické opatrenia	Organizačné opatrenia	Rozvoj kapacít	Kooperatívne opatrenia
Právne opatrenia	1,0000	0,6007***	0,4358**	0,4739**	0,2430
Technické opatrenia	0,6007***	1,0000	0,3428*	0,2254	0,5332**
Organizačné opatrenia	0,4358**	0,3428*	1,0000	0,5486**	0,2587
Rozvoj kapacít	0,4739**	0,2254	0,5486**	1,0000	0,5157**

Kooperatívne opatrenia	0,2430	0,5332**	0,2587	0,5157**	1,0000
------------------------	--------	----------	--------	----------	--------

Poznámka: Signifikantnosť : */0,05 ; **/ 0,01; ***/0,001

Zdroj : vlastné výpočty

Zhlukovú analýzu chceme urobiť pomocou nezávislých premenných. Preto sme požili PCA, ktorá sa používa na identifikáciu menšieho počtu nekorelovaných premenných známych ako hlavné komponenty. V našom prípade prvé dve hlavné komponenty vysvetľujú 71,18 percent variability. Podľa tohoto kritéria zvolíme počet hlavných komponentov dva. Príspevky premenných k hlavným komponentom znázorníme graficky. Červená čiara predstavuje priemerný príspevok. Nadpriemerný príspevok majú Technické opatrenia a Rozvoj kapacít. O máličko nadpriemerný príspevok majú Organizačné opatrenia, Právne opatrenia a Kooperatívne opatrenia.



Obrázok 2 Príspevky pilierov GCI k prvým dvom hlavným komponentom

Zdroj: vlastné znázornenie

Nakoľko každý pilier GCI má aspoň s jednou hlavnou komponentou štatisticky signifikantný korelačný koeficient, preto žiadnu premennú z ďalších analýz nie je potrebné vylučovať.

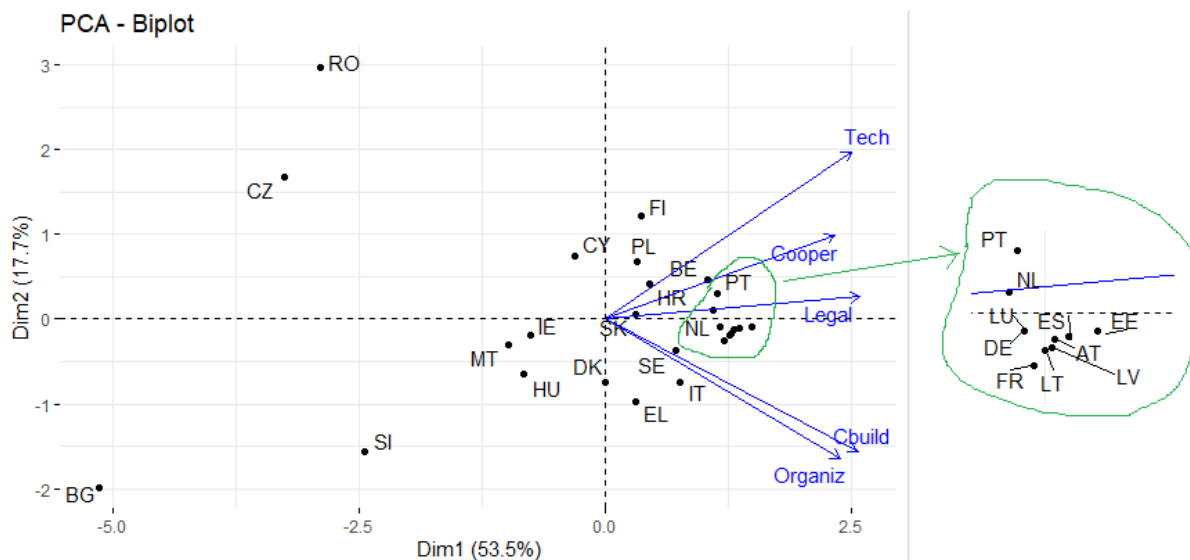
Tabuľka 2 Korelačné koeficienty medzi piliermi a prvými dvoma hlavnými komponentami

Pilier	1. hlavná komponenta		2. hlavná komponenta	
	Korelačný koeficient	P hodnota	Korelačný koeficient	P hodnota
Právne opatrenia	0,7661	3,6760E-06		

Rozvoj kapacít	0,7583	4,5883E-06	-0,4637	0,014845
Technické opatrenia	0,7393	1,0561E-05	0,5846	0,001316
Organizačné opatrenia	0,7047	4,0662E-05	-0,4856	0,010235
Kooperatívne opatrenia	0,6885	7,1829E-05		

Zdroj : vlastné výpočty

Na biplote (Obrázok 3) vidíme, že Slovensko (SK) je najbližšie k počiatku sústavy súradníc. Znamená to, že hodnoty za SK sú najbližšie k priemeru hodnôt pilierov za krajiny EÚ. Mierne nižšie hodnoty ako priemer EÚ má Slovensko v pilieroch Rozvoj kapacít a Kooperatívne opatrenia. Pozitívne je zistenie, že priemerné hodnoty na každý pilier sú na časti v smere šípky, t.j. žiadny pilier SR nie je úrovňou priemeru EÚ. Priesečníky priemetov ďaleko na predĺženej čiare - v opačnom smere ako je šípka - predstavujú nízke hodnoty skúmanej premennej pre daný objekt. Takým prípadom je Bulharsko (BG), Česká republika (CZ), Rumunsko (RO), Slovinsko (SI).

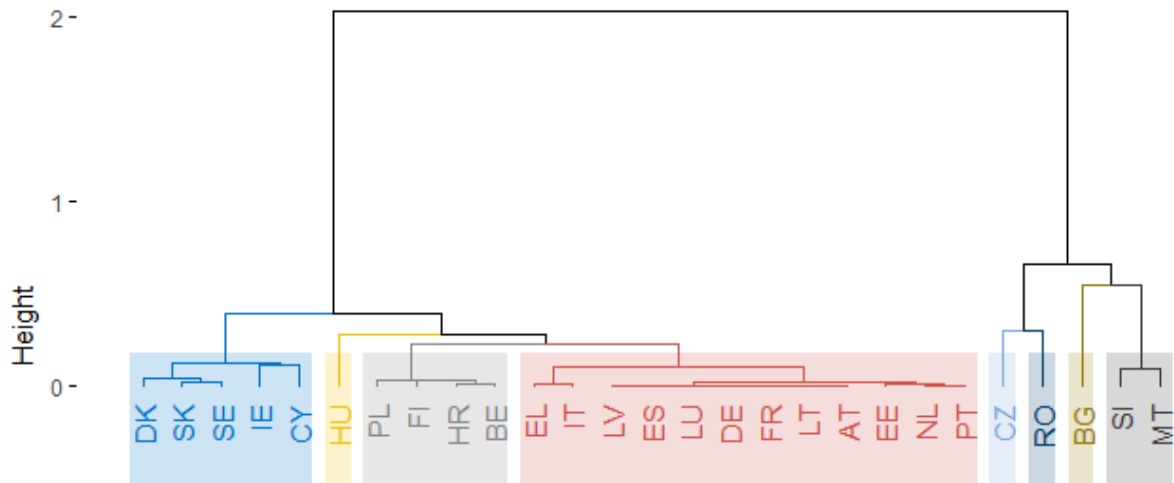


Obrázok 3 Biplot

Zdroj: vlastné znázornenie

Hodnota Hoplinsovej štatistiky je 0,66657. Jej P hodnota je 0,0121. To znamená údaje za jednotlivé krajiny majú štatisticky významnú tendenciu sa zhlukovať. Podľa NbClust je

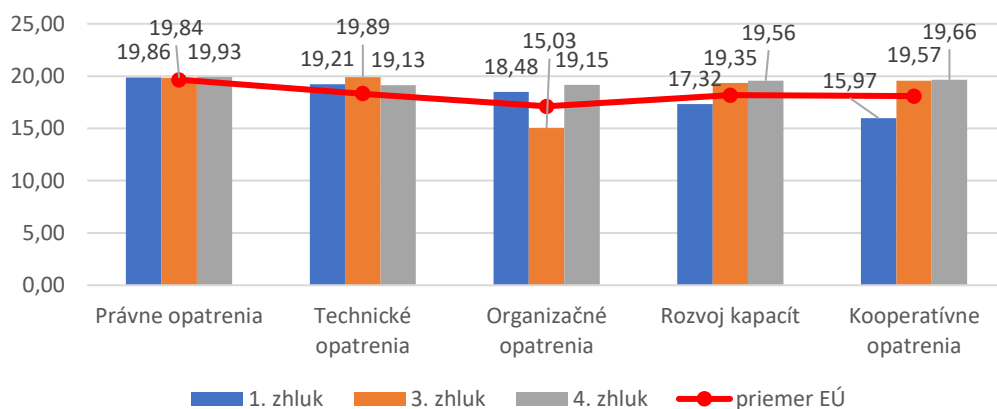
optimálny počet zhlukov 8. Niektoré zhluky (druhý a predposledné tri) obsahujú iba jeden štát. Sú to krajiny s takými hodnotami pilierov, ktoré sa nepodobajú so žiadnym iným štátom (viď. Biplot). Posledný zhluk obsahuje Slovensko (SI) a Maltu (MT). Prvý, tretí a štvrtý zhluk obsahujú niekoľko krajín.



Obrázok 4 Dendrogram

Zdroj: Vlastné výpočty a vlastné znázornenie

Krajiny štvrtého zhľuku majú priemerné hodnoty každého piliera vyššie ako je Z hľadiska právnych opatrení, majú krajiny prvého zhľuku, kde patrí aj Slovensko, mierne nadpriemerné hodnoty oproti priemeru EÚ (19,6574). V technických opatreniach je priemer hodnôt prvého zhľuku nad priemerom EÚ (18,3056), rovnako ako v prípade Organizačných opatrení (EÚ 17,1130). Priemer hodnôt krajín prvého zhľuku, ale tiež každého z nich) sú nižšie ako európsky priemer v pilieri rozvoj kapacít (18,2856), ako aj v pilieri Kooperatívne opatrenia (18,0793).



Obrázok 5 Priemerní hodnoty vybraných zhlukov

Zdroj: Vlastné výpočty a vlastné znázornenie

Výsledky znamenajú, že krajiny prvého zhľuku, a teda aj Slovensko by mali vyvinúť väčšie úsilie v oblasti kooperatívnych opatrení. V ďalšom sa zameriame na možnosti, ako k naplneniu tohto cieľa môže prispieť práve verejná správa.

Verejná správa má zodpovednosť za kybernetickú bezpečnosť vo svojej oblasti pôsobnosti. V Slovenskej republike je zodpovedným orgánom Ministerstvo obrany SR, ktoré má na starosti koordináciu a riadenie kybernetickej obrany. Okrem toho existuje aj Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe (NSRIB), ktorý má za úlohu koordinovať a riadiť kybernetickú bezpečnosť vo verejnej správe. NSRIB má tri hlavné úlohy: prevencia, detekcia a reakcia. Prevencia zahŕňa opatrenia na zvýšenie bezpečnosti informačných systémov a sietí verejnej správy. Detekcia zahŕňa monitorovanie informačných systémov a sietí verejnej správy na príznaky kybernetických útokov. Reakcia zahŕňa koordinovanú reakciu na kybernetické incidenty, vrátane obnovy poškodených informačných systémov a sietí.

Verejná správa by preto mala čím skôr prijať, realizovať a udržiavať ochranné systémy (prostriedky, procesy a riadenie zainteresovaných účastníkov) v stave bezpečnosti, uvádza Sivák (2019). Podľa Sivák (2019) a TUVsud Slovensko môže zlepšiť kybernetickú bezpečnosť vo verejnej správe predovšetkým tým, že:

- zabezpečí pravidelné audity kybernetickej bezpečnosti,
- zlepši silnú väzbu právneho systému v oblasti kybernetickej bezpečnosti na oblasť kritickej infraštruktúry a doplní ho o ďalšie prvky informatickej bezpečnosti,
- zvýši úroveň informačnej a kybernetickej bezpečnosti v podsektore ISVS/ITVS.

Problematika kybernetickej bezpečnosti sa nedotýka len vysoko špecializovaných pracovísk alebo inštitúcií, ktoré disponujú citlivými dátami. Každý okresný úrad, krajské riaditeľstvo či iný orgán verejnej správy s pripojením na internet predstavuje z hľadiska hybridných hrozieb potenciálny cieľ. Zraniteľnosť verejnej správy stále narastá v rámci presúvania prostriedkov komunikácie a procesov riadenia v takmer všetkých sférach života spoločnosti z reálneho do virtuálneho sveta, najmä v oblasti riadenia kritickej infraštruktúry, konceptov „Priemysel 4.0“, „Internet vecí“ a ďalších. Pracoviská verejnej správy sa stávajú atraktívnym

cieľom pre kyberzločincov, ktorí môžu získať prístup k niektorým súborom osobných údajov alebo získať kontrolu nad inteligentne prevádzkovanými mestskými zdrojmi prostredníctvom infraštruktúr LPA2.

Boj proti hybridným hrozbám znamená nielen zastavenie aktivít kriminálnych aktérov, ale aj vedenie informačných kampaní s cieľom pripraviť spoločnosť na ochranu pred rastúcou hrozbou alebo minimalizovať informačné a psychické škody spôsobené akciami narušiteľov. Školenia a cvičenia môžu pomôcť verejnej správe zlepšiť mechanizmy reakcie na rôzne incidenty alebo krízy, ktoré sa vzťahujú na hybridné hrozby. Cvičenia tiež posilňujú vzťahy medzi zúčastnenými organizáciami a jednotlivcami.

Súkromný sektor vlastní a prevádzkuje väčšinu kritickej infraštruktúry krajín EÚ. Preto sú partnerstvá medzi verejným a súkromným sektorom, ktoré podporujú dôveru a efektívnu koordináciu, sú nevyhnutné na udržanie bezpečnosti a odolnosti kritickej infraštruktúry. Okrem toho môžu pomôcť pravidelné spoločné školenia a cvičenia, na ktorých sa pracovníci verejného a súkromného sektora naučia lepšie spolupracovať.

Príklady kooperatívnych opatrení v oblasti kybernetickej bezpečnosti zahŕňajú zdieľanie informácií o kybernetickej bezpečnosti medzi súkromným sektorom a medzi štátom, územnými a miestnymi samosprávami. Medzi ďalšie príklady kooperatívnych opatrení v oblasti kybernetickej bezpečnosti patria cvičenia a simulácie kybernetickej bezpečnosti. Školenia a programy na zvyšovanie povedomia o kybernetickej bezpečnosti sú mimoriadne dôležité (Korauš, Kurilovská a Šišulák (2022). Úspešne tomu dochádza v rámci národného projektu Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy .

Problematicou úspešnosti školiacich programov v oblasti kybernetickej bezpečnosti sa zaoberali viacerí autori. Ciuperca et al. (2022) sa zaoberali príčinami rozdielov v schopnostiach kybernetickej bezpečnosti medzi krajinami podľa GCI pomocou PEST analýzy školiacich programov v oblasti kybernetickej bezpečnosti. Identifikované politické, ekonomické, sociálne - s osobitným zameraním na makrokultúrne a technické prvky.

Prístup k vytvoreniu modelu Jeonga et al. (2019) na určenie vplyvu národnej kultúry na politiku kybernetickej bezpečnosti je interdisciplinárny. Národná kultúra a zrelosť kybernetickej bezpečnosti zohrávajú určujúce úlohy v identite a bezpečnosti národa. Jeonga et al. (2019) dospeli

k názoru, že národná kultúra musí byť zohľadnená pri určovaní politiky kybernetickej bezpečnosti a rámcov, ktorými sa riadia jednotlivci.

Záver

Bezpečnostné prostredie v Európe prešlo za posledných niekoľko rokov zásadnými zmenami a ich výsledkom je zmena už známych konvenčných hrozieb, ktoré získali v dôsledku rozvoja technológií úplne novú dimenziu a zvýšila sa ich intenzita.

EÚ vo svojej globálnej stratégii definovala hybridnú hrozbu ako jednu z najväčších bezpečnostných výziev EÚ a smerom k jej obyvateľom a v tejto súvislosti boj proti hybridným hrozbám by mal vychádzať z odporúčaní definovaných už z prijatých dokumentov EÚ a dohôd o spolupráci EÚ a NATO s cieľom zabezpečiť čo najvyššiu efektivitu prijímaných opatrení.

Súčasťou zvyšovania odolnosti Slovenskej republiky pred hybridnými hrozbami bude zvýšenie úrovne bezpečnostného povedomia verejnosti o rizikách spojených s prejavmi hybridných hrozieb. Tam kde to bude účelné, zapoja štátne orgány do vzdelávacích podujatí aj akademickú obec, súkromný sektor a subjekty občianskej spoločnosti.

Verejná správa má zodpovednosť za kybernetickú bezpečnosť vo svojej oblasti pôsobnosti. Výsledky našej štúdie znamenajú, že krajiny prvého zhľuku, a teda aj Slovensko by mali vyvinúť väčšie úsilie v oblasti kooperatívnych opatrení.

Problematika kybernetickej bezpečnosti sa nedotýka len vysoko špecializovaných pracovísk alebo inštitúcií, ktoré disponujú citlivými dátami. Pracoviská verejnej správy sa stávajú atraktívnym cieľom pre kyberzločincov, ktorí môžu získať prístup k niektorým súborom osobných údajov alebo získať kontrolu nad inteligentne prevádzkovanými mestskými zdrojmi. V článku sa zameriame aj na možnosti, ako k lepšiemu plneniu v oblasti naplneniu kooperatívnych opatrení, a tým aj celkovému zvýšeniu kybernetickej bezpečnosti môže prispieť práve verejná správa.

PodĎakovanie

Príspevok vznikol v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zoznam použitej literatúry

- Blighe, K., Lun, A. (2021). PCAtools: everything Principal Component Analysis. Dostupné na internete. <https://bioconductor.org/packages/release/bioc/vignettes/PCAtools/inst/doc/PCAtools.html>
- Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1-19.
- Çifci, H. (2022). Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework. <https://www.researchsquare.com/article/rs-2159915/latest.pdf>
- Ciupercă, E. M., Donnelly, N., Gartland, A., & Stanciu, A. (2022). The Digital Divide in Education-Macro cultural Comparative Analysis between Ireland and Romania. *IFAC-PapersOnLine*, 55(39), 99-104.
- Dragulescu, A. and Cole Arendt (2020). xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.5. <https://CRAN.R-project.org/package=xlsx>
- Európska rada a Rada EÚ (2023) Kybernetická bezpečnosť: ako EÚ bojuje proti kybernetickým hrozbám dostupné online: <https://www.consilium.europa.eu/sk/policies/cybersecurity/>
- Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, 32(1), 63-71.
- Greenacre, M., Groenen, P. J., Hastie, T., d'Enza, A. I., Markos, A., & Tuzhilina, E. (2022). Principal component analysis. *Nature Reviews Methods Primers*, 2(1), 100.
- ITU: Global cybersecurity index. Dostupné na <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Jeong, J. J., Grobler, M., Chamikara, M. A. P., & Rudolph, C. (2019, December). Fuzzy logic application to link national culture and cybersecurity maturity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 330-337). IEEE.
- Khudyntsev, M., Davydiuk, A., Lebid, O., Trofymchuck, O., & Zhylin, A. (2022). Cybersecurity Indices: Review and Classification. Dostupné na <https://ceur-ws.org/Vol-3187/paper11.pdf>

- Korauš, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. RELIK 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>
- Kravets, V. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. *Theoretical and Applied Cybersecurity*, 1(1).
- Leahovcenco, A. (2021). Cybersecurity as a fundamental element of the digital economy. *MEST Journal*, 9(1), 97-105.
- Maechler, M., Rousseeuw, P., Struyf, A., Hubert, M., Hornik, K.(2021). cluster: Cluster Analysis Basics and Extensions. R package version 2.1.2.
- Oh, H. R., & Youm, H. Y. (2022). Proposals for GCI Indicators to Improve a National Cybersecurity Level. *Journal of the Korea Institute of Information Security & Cryptology*, 32(2), 289-307.
- Polotaj, O.I., Kucharika, N.P. Samotij, V.V., Lagun, A.E. (2020). Using of the trend extrapolation method for qualitative prognosis the global cybersecurity index in Ukraine. Dostupné na <https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/7541/1/5articlelagune2.pdf>
- R Core Team (2021). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>.
- Samad, M. Y. (2022). Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index. *AL-ULUM: JURNAL SAINS DAN TEKNOLOGI*, 7(1).
- Sharkov, G. (2020). Assessing the maturity of national cybersecurity and resilience. *Connections: The Quarterly Journal*, 19(4), 5-24.
- Sivák J. (2019) Hybridné hrozby na Slovensku. Kybernetická bezpečnosť Analýza legislatívy, štruktúr a procesov. Bratislava Globsec Dostupné na [Hybridne-hrozby-na-Slovensku-Kyberneticka-bezpecnost.pdf \(globsec.org\)](https://globsec.org/Kyberneticka-bezpecnost.pdf)
- Tuvsud: Audit kybernetickej bezpečnosti Dostupné na <https://www.tuvsud.com/sk-sk/cinnosti/kyberneticka-bezpecnost/audit-kybernetickej-bezpecnosti>
- Yerina, A., Honchar, I., & Zaiets, S. (2021). Statistical indicators of cybersecurity development in the context of digital transformation of economy and society. *Science and Innovation*, 17(3), 3-13.

Kontaktné údaje

prof. Ing. Antonín Korauš, PhD., LL.M., MBA

Akadémia Policajného zboru v Bratislave,

Sklabinská 1, 835 17 Bratislava 35,

Slovak Republic

E-mail: antonin.koraus@akademiapz.sk

prof. RNDr. Beáta Stehlíková, CSc.

Slovenská technická univerzita v Bratislave

E-mail: beata.stehlikova@stuba.sk

pplk. RNDr. Kristián Újváry, PhD

Ministerstvo vnútra SR,

vyslaný národný expert v agentúre Frontex

E-mail: kristian.ujvary@frontex.europa.eu

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Building Reputation in Community Open Data Ecosystems to improve the security of shared data

Ján Lang, Jakub Knežo, Dávid Korman and Stanislav Šišulák

Abstract

The concept of open data, the so-called "open data ecosystem", solves several problems related to the correctness of data, the trustworthiness of its users and, in general, its main vulnerability due to potential subversive activities, attacks or generally the intent to harm, also in a hybrid or collaborative way.. This paper deals with the analysis of the resilience of selected policies defined over an open community system based on Q&A due to hardware-defined boundaries and limits. Analysis of the impact of selected metrics due to computational complexity, availability, integrity, security of shared data and the method of determining the reputation and weight of events in a distributed environment, the role of users in the system and the method of safely calculating their reputation and the weight of events edited by them. Finally to propose, implement and evaluate an expertise model for selected domain. Considering the role of Q&A, this approach is sufficiently generic even for the security domain.

Index Terms

Q&A open data, reputation, security, hybrid threats, shared data, community

INTRODUCTION

The basic idea of reputation systems is to determine the degree of trustworthiness of a subject, most often by deriving it from its activity itself. Exposing the trustworthiness of the subject in the community is characteristic especially in gamer communities and specifically professional communities and their forums in the form of Q&A systems. The characteristics of these systems are openness, availability and, in general, content sharing, e.g. in the form of questions and answers. The user's reputation often serves as an orientation or selection criterion here. However, the challenge is to identify other even hybrid forms of threats to the consistency of open data derived from the reputation of their users. The seriousness of this situation is higher due to the nature of the data itself, e.g. in case of existing Q&A systems, as a serious educational tools, they may face educational content related threats. The importance of Q&A tools increases due to the fact that they provide the necessary procedures and suggestions for adequate and effective solutions also for the purpose of raising awareness of hybrid threats that are currently publicly communicated [13].

The correct calculation of the object's authenticity (the object can be defined as a user, a review in the e-shop, an answer in Q&A systems, etc.) may be prone to specific situations which must be treated or bypassed using different calculation methods. The calculation, respectively,

defining a correct reputation, must work so that the building of reliability is not strongly dependent on long-term user activity. Also, there must be a way to consider the target users' current reputation and further credibility assessment. Reputation and trustworthiness is often an identifier of variables such as security, whether, on the contrary, susceptibility to fraud in the systems. The low reputation of the object should indicate lower trustworthiness in the given object and, therefore, warn about a possible scam or misinterpretation of the object.

Open Data Ecosystems (ODE) is a concept of sharing data under public license goals in software ecosystems, in some parts similar to OSS (Open Source System) or OGD (Open Government Data). Community or open Q&A systems contain a database of questions and comments added by users. By formulating a question, the user expresses the need for community cooperation to solve the issue. The main advantage and condition simultaneously is accessibility to open data for everyone. Openness consists of the possibility of creating such content by each user.

Trust can be divided into two groups trust in reliability and trust in decision-making. Confidence in reliability, defined according to Gambett [1], is that trust is a subjective probability based on which an individual expects that another individual will perform a given activity on which his well-being depends. This definition includes the reliance on a trusted party and the reliability (probability) of the relying party as seen by the relying party. Jøsang and Lo Presti [2] distinguished between confidence in reliability and decision-making and developed a mathematical model of trust in decision-making based on more subtle principles, such as the reliability, effectiveness, usefulness, and risk attitude of the trusted party.

Reputation is closely related to trust or trustworthiness, but there is some difference. Jøsang et al. defines reputation according to the Concise Oxford words. Reputation is generally said or believed about a person's character or status. This definition corresponds well with the opinion of social network researchers [3], [4] that reputation is a quantity derived from the underlying social network, which is globally visible to all network members. The difference between trust and reputation may be illustrated by the following statements: "I trust you because of your good reputation" or "I trust you despite your bad reputation."

In addition, there are Q&A forums that have educational potential. These questions and answers are result of certain user activity. The content of these questions and answers may represent

a form of educational content in electronic form. It represents easy access to educational content at all. And it is therefore important that the content should be safe and reliable. We assume that reliability and security can be derived from the author's reputation. Our goal is to identify a model that can calculate the author's reputation based on a small number of inputs even in the form of questions.

The rest of the paper is organized as follows. Section 2 introduces related work. Section 3 explains Section 4 describes Section 5 describes

Section 6 compares the approach proposed in this paper to related work. Section 7 concludes the paper and indicates some possibilities for further work.

RELATED WORK

In Q&A systems with a predefined database, we usually go through the questions and answers mechanically. However, the first answer to the question may need to be corrected, or it may not be in the requested wording of the questioner, and thus the waiting time for the answer often multiplies [6]. The study analyzing the reputation system of StackOverflow pointed out that the average time for the first answer to a question in the Q&A system was 16 minutes [7].

Another study found that StackOverflow had 1.3 million users between 2008-2012, including 3.4 million responses, with approximately twice as many answers [8]. Despite the established reputation of this online community, Stack Overflow was experiencing a high number of inactive users, which raised doubts about the enthusiasm of this software user. About 82% of users in regular software support groups became the so-called "lurkers," or users who do not actively contribute to the content creation of the given community but are its passive observers. A recent study by Slag, De Waard, and Bacchelli from 2015 [9] used "one-day flies," indicating users who contributed to the community/forum only once. Unfortunately, this applied to approximately 47% of all users. Empirical research by the authors Nonnecke & Preece [10] from 1999 listed the possibilities for which users are prone to become "lurkers" and passive participators of the forum. As the most common reasons for users' inconsistency (degradation factors of Q&A communities), the authors gave the following reasons: unanswered or removed questions, negative responses, a lack of effort to provide an assessment, high subjectivity, constant changes of identities, duplicate ratings by the same user, or discrimination.

On the other hand, some authors dedicated their work to pinpointing the factors supporting the consistency of online communities. There are users who can, e.g., control a specific part of the content [11]. There is an assumption that reputation increases with the reputation of connected users. For example, the earliest version of Google’s PageRank algorithm measures the rank of a website as a function of the ranks of the linked sites [12]. According to the phenomenon described by the authors, Movshovitz-Attias et al. [7], users with a “higher social status” within the online community are more likely to get the question answered by an “expert” within the issue. They assume that the quality of the question asked is directly correlated with the status of its questioner.

The works, that deal with the creation of reputation apply different models and algorithms, which are based on different approaches. These approaches include e.g. a procedure based on the analysis of lines, as in the article [14]. In this case it focuses more on the creation of structure and continuity than on the content itself that it connects. One of the bibliometric techniques for determining reputation is the g-score [15]. New expertise evaluation techniques were also created by extending and modifying already known algorithms, such as by adapting the PageRank algorithm [16]. There are authors who have analyzed the relationships between different user activities and their mapping to StackOverflow and GitHub pages [17]. Tagging of individual posts could help to better calculate reputation [18], [19]. One of the more recent approaches for assessing expertise is a probability model [20], successful in finding highly experienced developers on StackOverflow and GitHub. The authors in [21] divide users into two classes: owls and sparrows. Sparrows are the most active users and owls are the most knowledgeable users. In recent years, in this regard, artificial intelligence and approaches based on deep learning [22], [23] have been applied in the classification of experts within Q&A communities. The uniqueness of our approach compared to the existing ones is that we calculate the expertise of the author with regard to the questions asked. We assume that an expert will not ask trivial questions and also that a beginner will not be able to formulate a non-trivial question construction. Finally, metrics are created that examine different patterns of expert behavior.

REPUTATION TO EXPERTISE MODEL COMPARISON PROPOSAL

There are several approaches we can use. Considering related work and applied approaches, we have used Jaccard’s metric and Average positional deviation. For the purposes of our testing, we decided that an expert is someone who is on the top of the list of users in a given dataset. We

have used the Jaccard metric 1 similarly as [24] to calculate correlations between identified experts and the users of the open data ecosystem.

$$H = \frac{M_{exp} \cap M_{uode}}{M_{exp} \cup M_{uode}} \quad (1)$$

In case of Average positional deviation we measure the agreement between two ranking boards and to the list of users ranked by their reputation Q and users ranked by reputation based on the reference model (StackExchange, TeX - LaTeX) Ref . For each user in the input Q , we find the same user from the sorted output according to the reference model Ref . In both cases, it is necessary to remember their position. Subsequently, we subtract these positions $abs(Q-Ref)$ to obtain the

resultId	Reputation		resultId	Reputation
2891.0	4.864318e+06		510.0	91.0
3144.0	3.836290e+06		4301.0	68.0
510.0	3.813732e+06	4	169.0	61.0
4301.0	2.852716e+06		2674.0	56.0
2674.0	2.822042e+06		3144.0	52.0

user's deviation. We perform this operation on each user and average the result by the number of users 2.

Fig. 1. Example of a user deviation where the positional deviation is four places
Zdroj: vlastné spracovanie

In essence, we track the position of the user and how his position has changed relative to himself if he is assigned to a different position by the reference model.

$$Deviation = \frac{\sum_{i=0}^{n-1} abs(i_Q - i_{Ref})}{n} \quad (2)$$

In our approach we use the questions asked by the user on the Q&A. The very issue of the question was also addressed here [25], [26]. In these works, the importance of the question itself in Q&A was clarified, where it was also shown that the way in which the question is written reflects the knowledge of the questioner. In the work [27] it was pointed out that experts in the given Q&A circles have the same personality characteristics when writing their questions. It was also pointed

out in [28] that if a person asks a question, it indicates not only that this person demands an answer but also hidden expertise. That's why we wanted to propose a model that, even on the basis of a small number of questions, can create a reputation for the user that would correspond more closely with his knowledge. We called our approach "QuestionBased". We have extended our question based idea by two more attributes to determine the author's expertise:

- Keywords in the question
- Reputation of the responder
- Time to answer

Together, these three attributes represent our proposed approach. Key words in the question - the first attribute will have the task of selecting a certain number of keywords from the question, creating a set of keywords for this question. Reputation of the responder - the model will also track, in the case of a question, the reputation of the user who answered the question. Time to answer - it tracks how long it take to answer the question that was asked by the user. Our assumption is that a question is difficult if the questioner had to wait too long for an answer. We can say that the question was difficult if it took longer to answer.

REFERENCE MODEL PROPOSAL EVALUATION

We have performed several test scenarios to evaluate our QuestionBased approach to several different approaches (RepFS, ExpertiseRank and ExpRankFB). Even in our approach we have distinguished between weighted and unweighted QuestionBased.

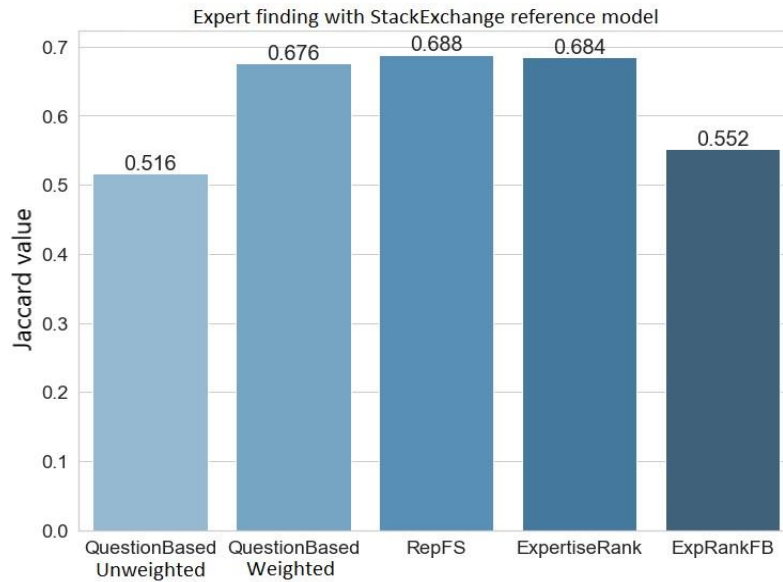


Fig. 2. Modified approach against other existing approaches - Jaccard value
Zdroj: vlastné znázornenie

A. Weighting the attributes of our approaches - Jaccard's metric

In the case of the Jaccard value as a metric see Fig. 2, we have achieved a significant improvement compared to our unweighted approach. It can also be seen that we have shown a higher success rate than the ExpRankFB approach. The resulting success of finding an expert in our case was almost as high as with the ExpertiseRank and RepFS approaches. As a result, we can see that the changes we made to our approach improved its success in building reputation.

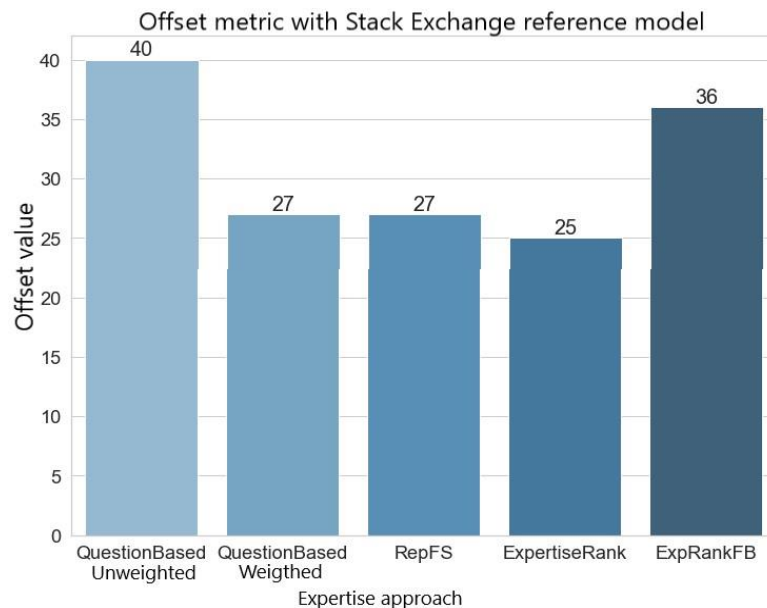


Fig. 3. Modified approach compared to other existing approaches - Average positional deviation

In the case of Average Positional Deviation see Fig. 3, it can be seen that our approach has significantly improved after adjustments compared to the unweighted approach. We surpassed ExpRankFB in terms of success and also equaled RepFS. RepFS is a purely question-based approach just like our proposed approach. We can thus say that our proposed approach has the same reputation creation success as another existing approach, which also deals exclusively with questions based on the Average Positional Deviation metric.

CONCLUSIONS AND FURTHER WORK

We have performed a robustness analysis of selected policies defined over an open community system from the StackExchange group focused on the TEX community in order to find the way how to recognize the proper way to building reputation of users. In such a Community Open Data Ecosystem we have recognized the assumption that better rated authors are a guarantee of quality and a guarantee of safety in relation to content that can also have an educational nature. We have shown that our approach is different from other existing reputation building approaches, and we have experimentally proven that this approach shows success comparable to other existing reputation building approaches. We have built the QuestionBased hybrid approach based on questions itself and two more attributes to determine the author's expertise: keywords in the question, reputation of the responder and time to answer. The main research contribution of this work is in the creation of user reputation from the point of view of the educational potential of the contribution to the Community Open Data Ecosystem in order to improve its security especially in the context of the operation of hybrid threats. It is possible to continue in this work by building a superstructure on top of shared content to identify duplicates through machine learning and artificial intelligence.

ACKNOWLEDGMENT

The contribution was created as part of the national project "Increasing Slovakia's resistance to hybrid threats by strengthening public administration capacities", project code ITMS2014+: 314011CDW7. This project is supported by the European Social Fund.

REFERENCES

- Abbas, S., Merabti, M., Kifayat, K., & Baker, T. (2019). Thwarting Sybil attackers in reputation-based scheme in mobile ad hoc networks. *KSII Transactions on Internet and Information Systems*, 13(12), 6214-6242.
- Ashutosh Adhikari et al. "Rethinking complex neural network architectures for document classification". In: Proceedings of the 2019 Conference of the North American Chapter of the Association for
- Battiston, S., Puliga, M., Kaushik, R., Tasca, P., & Caldarelli, G. (2012). Debtrank: Too central to fail? financial networks, the fed and systemic risk. *Scientific reports*, 2(1), 1-6.
- Blerina Bazelli, Abram Hindle a Eleni Stroulia. "On the personality traits of stackoverflow users". In: 2013 IEEE international conference on software maintenance. IEEE. 2013, p. 460–463
- Bogdan Vasilescu, Vladimir Filkov a Alexander Serebrenik. "Stackoverflow and github: Associations between software development and crowdsourced knowledge". In: 2013 International Conference on Social Computing. IEEE. 2013, p. 188–195.
- Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers). 2019, p. 4046–4051
- Divya Srivastava a RN Mall. "Structural Analysis of L-Bracket using ANSYS". In: i-Manager's Journal on Mechanical Engineering 7.2 (2017), p. 17
- Fabio Calefato, Filippo Lanubile a Nicole Novielli. "How to ask for technical help? Evidence-based guidelines for writing questions on Stack Overflow". In: *Information and Software Technology* 94 (2018), p. 186–207
- Freeman, L. C. (2002). Centrality in social networks: Conceptual clarification. *Social network: critical concepts in sociology*. Londres: Routledge, 1, 238-263.
- G. Alan Wang et al. "ExpertRank: A topic-aware expert finding algorithm for online knowledge communities". In: *Decision Support Systems* 54.3 (2013), p. 1442–1451. issn: 0167-9236. doi: <https://doi.org/10.1016/j.dss.2012.12.020>. url: <https://www.sciencedirect.com/science/article/pii/S0167923612003867>

Gambetta, D. (2000). Can we trust trust. *Trust: Making and breaking cooperative relations*, 13(2000), 213-237.

Hong Yu et al. “Tag recommendation method in folksonomy based on user tagging status”. In: *Journal of Intelligent Information Systems* 50.3 (2018), p. 479–500

Ivan Cantador et al. “Personalized recommendations in e-participation: Off-line experiments for the ‘Decide Madrid’ platform”. In: *Proceedings of the International Workshop on Recommender Systems for Citizens*. 2017, p. 1–6

James Lanagan, Nikolai Anokhin a Julien Velcin. “Early stage conversation catalysts on entertainment-based web forums”. In: *State of the art applications of social network analysis*. Springer, 2014, p. 97–118.

Jie Yang et al. “Sparrows and owls: Characterisation of expert behaviour in stackoverflow”. In: *International conference on user modeling, adaptation, and personalization*. Springer. 2014, p. 266–277.

Jøsang, A., & Presti, S. L. (2004). Analysing the relationship between risk and trust. In *Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29-April 1, 2004. Proceedings 2* (pp. 135-145). Springer Berlin Heidelberg

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2), 618-644.

Korauš, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. *RELIK 2022*. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

Marsden, P. V., & Lin, N. (Eds.). (1982). *Social structure and network analysis* (Vol. 57). SAGE Publications, Incorporated.

Mohammad Masudur Rahman a Chanchal K Roy. “An insight into the unresolved questions at stack overflow”. In: *2015 IEEE/ACM 12th Working Conference on Mining Software Repositories*. IEEE. 2015, p. 426–429

Movshovitz-Attias, D., Movshovitz-Attias, Y., Steenkiste, P., & Faloutsos, C. (2013, August). Analysis of the reputation system and user contributions on a question answering website:

Stackoverflow. In Proceedings of the 2013 IEEE/ACM international conference on advances in social networks analysis and mining (pp. 886-893). In 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014) (pp. 328-335). IEEE.

Nan Zhao et al. “A Novel Expert Finding System for Community Question Answering”. In: Complexity 2020 (2020).

Naomi Miyake a Donald A Norman. “To ask a question, one must know enough to know what is not known”. In: Journal of verbal learning and verbal behavior 18.3 (1979), p. 357–364

Nonnecke, B., & Preece, J. (1999). Shedding light on lurkers in online communities. *Ethnographic studies in real and virtual environments: Inhabited information spaces and connected communities*, Edinburgh, 123128.

Salman Mohammed, Peng Shi a Jimmy Lin. “Strong baselines for simple question answering over knowledge graphs with and without neural networks”. In: arXiv preprint arXiv:1712.01969 (2017)

Slag, R., de Waard, M., & Bacchelli, A. (2015, May). One-day flies on stackoverflow-why the vast majority of stackoverflow users only posts once. In 2015 IEEE/ACM 12th Working Conference on Mining Software Repositories (pp. 458-461). IEEE.

Yang, J., Hauff, C., Bozzon, A., & Houben, G. J. (2014, September). Asking the right question in collaborative q&a systems. In Proceedings of the 25th ACM conference on Hypertext and social media (pp. 179-189).

Yao Wan et al. “SCSMiner: mining social coding sites for software developer recommendation with relevance propagation”. In: World Wide Web 21.6 (2018), p. 1523–1543

CONTACT INFORMATION

Ján Lang,

Faculty of Informatics and Information Technologies

Slovak University of Technology in Bratislava

Slovakia

E-mail: jan.lang@stuba.sk

Jakub Knežo,

Faculty of Informatics and Information Technologies Slovak University of Technology in
Bratislava
Bratislava, Slovakia
E-mail: knezozakub@gmail.com

Dávid Korman
Faculty of Informatics and Information Technologies Slovak University of Technology in
Bratislava
Slovakia
E-mail: xkorman@stuba.sk

Stanislav Šišulák
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 3,
Slovakia
E-mail: stanislav.sisulak@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA
doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Limity anonymizácie transakcií virtuálnych mien

Andrej Lipták

Abstrakt

V príspevku sa autor venuje problematike anonymizácie transakcií vybraných virtuálnych mien. Autor rozoberá metódy a formy, ktoré umožňujú užívateľovi virtuálnej meny zastrieť pôvod virtuálnej meny v otvorených verejne prehliadateľných distribuovaných záznamoch – blockchainoch virtuálnych mien. Na základe výsledkov tejto analýzy vyvodzuje limity anonymizačných metód a foriem, a navrhuje možnosti vysporiadania sa s anonymitou vzťahujúcou sa na potenciálnu trestnú činnosť, ako je napríklad legalizácia výnosov z trestnej činnosti, ktorá je realizovaná prostredníctvom virtuálnych mien.

Kľúčové slová

Anonymita virtuálnych mien, mixing, znečistená virtuálna mena, AML, swapping, obfuscating

Abstract

The author of the article focuses on the issue of anonymizing transactions of selected virtual currencies. The author examines methods and forms that enable virtual currency users to conceal the origin of virtual currency in publicly visible distributed records - virtual currency blockchains. Based on the results of this analysis, the author draws conclusions on the limits of anonymization methods and forms, and proposes options for dealing with anonymity related to potential criminal activities, such as the legalization of proceeds from criminal activities carried out through virtual currencies.

Keywords

Anonymity of virtual currencies, mixing, tainted virtual currency, AML, swapping, obfuscating

Úvod

Virtuálne meny predstavujú neoficiálny ekvivalent k aktuálnemu finančnému systému najmä na úrovni *stability* elektronického vykonávania transakcií. Zasielane takýchto transakcií je podmienené decentralizovanej sieti, ktorej jednotlivé uzly, podľa pravidiel určených v zdrojovom kóde virtuálnej meny, udržiavajú stabilný chod odosielania a prijímania transakcií. Tieto uzly okrem iného zabezpečujú ukladanie, overovanie a zapisovanie transakcií a iných dát do verejného distribuovaného záznamu alebo blockchainu. Zakázaním, vypnutím alebo napadnutím jedného alebo viacerých uzlov teda nedôjde k významnému narušeniu siete. Platí teda, že s nárastom zodpovedných účastníkov siete virtuálnej meny rastie aj celková bezpečnosť a stabilita vykonávania transakcií virtuálnej meny. Zodpovednosť v sieti je daná najmä filozofiou hier a filozofiou profitu. V jednoduchosti môžeme povedať, že filozofiou hier sa zaistuje rovnosť

medzi jednotlivými účastníkmi a filozofiou profitu sa zaist'uje odmeňovanie účastníkov za správny a zodpovedný prístup k ekosystému danej virtuálnej meny. Uvedenej stabilite napomáha aj skutočnosť, že distribuovaný verejný záznam alebo blockchain obsahujúci transakcie a iné dáta, je otvorený. To znamená, že je voľne prehliadateľný, každý, aj ten, kto nie je priamo účastníkom siete má prístup k uloženým dátam, vie ich porovnať s dátami iného uzla a tým určovať napríklad pravdivosť dát. Táto funkcia virtuálnej meny je dôležitým aspektom pri sledovaní toku transakcií virtuálnych mien medzi účastníkmi a analýze všetkých dostupných dát v distribuovanom verejnom zázname alebo blockchaine. Nie všetci účastníci virtuálnej meny však vzhľadom na ich hodnotové nastavenie, históriu virtuálnych mien alebo vzhľadom na pôvod virtuálnych mien chcú, aby ich transakcie boli verejne prístupné. Títo účastníci preto používajú anonymizačné metódy a techniky, ktorými sa snažia zakryť tok realizovaných transakcií. Prvým problémom je identifikácia toku transakcií tých virtuálnych mien, ktoré majú čo do činenia s nezákonnými aktivitami, najmä na úrovni legalizovania výnosov z trestnej činnosti. Druhým problémom je aj stav ochrany tých účastníkov siete, ktorí disponujú legálne nadobudnutými virtuálnymi menami a zároveň chcú anonymizovať svoje transakcie alebo chcú čerpať profit z poskytnutia svojich virtuálnych mien na zaistenie funkčnosti anonymizačných služieb bez toho, aby sami porušovali zákon. Tieto legálne nadobudnuté virtuálne meny sa po použití anonymizačných metód a techník môžu premiešať napr. s výnosmi z trestnej činnosti vo forme virtuálnych mien, a účastník namiesto legálne držaných virtuálnych mien odošle alebo príjme výnos z trestnej činnosti.

Objektom skúmania tohto príspevku je teda problematika anonymizácie transakcií virtuálnych mien, možné metódy a techniky anonymizácie, ktoré sú v tomto prostredí využívané. Abstrahujeme však od virtuálnych mien, ktoré nemajú tzv. otvorený blockchain, resp. distribuovaný verejný záznam transakcií. Tieto virtuálne meny, inak nazývané aj anonymné vyžadujú samostatné skúmanie a nie je možné ich zahrnúť pod predmet skúmania tohto príspevku. Abstrahujeme aj od skúmania anonymity, ktorú poskytujú virtuálne meny vo vzťahu k verejným adresám jednotlivých užívateľov. Predmetom skúmania sú anonymizačné metódy a techniky využívané v otvorenom distribuovanom zázname alebo blockchaine. Cieľom príspevku je prostredníctvom analýzy anonymizačných metód a techník, poukázať na ich fundament, na ich znaky a faktory, ich funkčnosť, popísať ich miesto v ekosystéme virtuálnych mien, určiť mieru rizika, ktoré predstavujú pre ostatných účastníkov siete virtuálnej meny, poukázať na ich limity

a vyvodit' možnosti ich prelomenia, resp. možnosti ochrany poctivých účastníkov siete pred nezodpovedným užívaním týchto anonymizačných metód a techník.

„Every new technology provides new ways to abuse power” – Lawrence Lessig.

1. PODSTATA MIXOVACÍCH METÓD A TECHNÍK

Z fundamentu otvorených distribuovaných záznamov a otvorených blockchainov vyplýva skutočnosť, že všetky skonštruované, overované a uložené transakcie musia podliehať kontrole ostatných účastníkov siete. Táto otvorenosť je z kryptografického hľadiska nutná, pretože bez nej by nebolo možné spravovať systém otvorených virtuálnych mien, najmä z hľadiska zaistenia jednotnosti distribuovaného záznamu alebo blockchainu. V úvode je preto nutné spomenúť, že úplná anonymita v otvorených a domnievame sa, že aj v anonymných virtuálnych menách neexistuje. Stav úplnej anonymity by odporoval funkčnosti virtuálnej meny. Transakcia virtuálnej meny pozostáva pre jednoduchosť z vstupu, z výstupu a z hodnoty posielanej virtuálnej meny. Tieto údaje sa uzavru do súboru, ktorý potom účastníci siete skontrolujú, či osoba, ktorá virtuálnu menu posiela naozaj disponovala touto virtuálnou menou, teda, či existuje v distribuovanom záznamne alebo blockchaine informácia o predošlej transakcii daného odosielateľa, a pri úspešnom overení ju po splnení kryptografických podmienok zaradia do bloku transakcií. Ak by pri vytvorení transakcie nebolo možné vidieť, kto virtuálne meny odosiela, komu ich odosiela a v akej hodnote, nebolo by možné transakciu overiť a tým pádom zapísať do blockchainu.¹

Mixovacie metódy a techniky predstavujú systém zastierania transakcií bez toho, aby narušovali fundamentálne princípy virtuálnej meny. Mixovacie metódy a techniky vytvárajú autori, ktorí ich poskytujú formou služieb za účelom profitu. Samotné vytvorenie mixovacej služby nie je nemorálne, takisto ako snaha účastníkov siete anonymizovať svoje transakcie v elektronickom prostredí, tak ako to je možné pri fiat menách vo forme hotovosti. To, čo porušuje morálne a etické zásady, resp. objekty chránené právom je zneužívanie mixovacích služieb virtuálnych mien napríklad na legalizovanie výnosov z trestnej činnosti, podporu terorizmu, nákupy nelegálnych zbraní, detskej pornografie, zakázaných drog, podporu rozvratu štruktúry politického režimu, nemorálnu propagandu a pod. Pri mixovaní, ako z názvu vyplýva dochádza k spájaniu transakcií rôznych odosielateľov, prijímateľov, hodnôt virtuálnych mien, dochádza k vytváraniu množstva transakcií, ktoré spolu zdanlivo nesúvisia, a to všetko za účelom zastierania

¹ HOSP, J., Kryptomeny. Bratislava: TATRAN, 2021, str. – 40-52

pôvodu a za účelom čo najväčšieho sťaženia sledovania toku transakcií. Mixovacie metódy a techniky sa od seba líšia v závislosti od používanej virtuálnej meny.² Pre účely tohto článku sa zameriame na dve najpodstatnejšie virtuálne meny. Bitcoin, ktorý má aktuálne trhovú kapitalizáciu 507,79 miliónov Eur³ a je považovaný za najrozšírenejšiu a najstabilnejšiu virtuálnu menu vôbec, využíva mechanizmus konsenzu proof-of-work⁴; a Ethereum, ktoré má aktuálne trhovú kapitalizáciu 214,64 miliónov Eur⁵, využíva mechanizmus konsenzu proof-of-stake, umožňuje Smart kontrakty a decentralizované financovanie.⁶

Mixovacia služba musí spĺňať jednotlivé znaky, aby bolo vôbec možné hovoriť o takejto službe. Tieto znaky je potrebné skúmať pre odlišenie fundamentálnych mixovacích služieb od podvodných, ktorých účelom nie je poskytnutie anonymity, ale podvodné odčerpanie virtuálnej meny v prospech páchatel'a. Riadna mixovacia služba musí svojim užívateľom poskytnúť:

- Anonymitu - tak, aby bolo zložité spojiť výstupy a napárovať ich na vstupy.
- Možnosť odmietnutia – jednotlivé uzly v sieti zaistujúce mixovanie musia mať možnosť odmietnuť účasť na mixovacej operácii.
- Výkonnosť – protokol mixovacej služby musí byť schopný vykonať viacero mixovacích operácií s čo najväčším možným počtom užívateľov.
- Kompatibilitu – protokol musí byť plne kompatibilný so sieťou vybranej virtuálnej meny, musí vedieť komunikovať v rámci siete s uzlami a musí vedieť vytvárať a spracovávať transakcie.
- Cenovú efektivitu – v rámci mixovacej služby musí byť jasne dané, za akú protihodnotu je služba poskytnutá, a výsledná suma by mala zahŕňať aj cenu za vytvorenie transakcií vyplývajúcich z fundamentu virtuálnej meny.
- Správnosť mixovacej operácie – virtuálna mena v rámci mixovania nesmie byť ukradnutá, stratená, opakovane utratená v rámci dvojitej útraty. Zodpovední užívatelia

² ŠANTA, J., ŠANTA, I., ŠIROKÝ, T.: K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. In: Justičná revue. – Roč. 2022, Vydanie 4/2022, s. 3.

³ Graf Bitcoin k EUR, trhovú kapitalizácia. (online, cit. 20.04.2023). Dostupné na internete: < <https://coinmarketcap.com/sk/currencies/bitcoin/> >

⁴ Bitcoin: A Peer-to-Peer Electronic Cash System. (online, cit. 20.04.2023). Dostupné na internete: < <https://bitcoin.org/bitcoin.pdf> >

⁵ Graf Ethereum k EUR, trhovú kapitalizácia. (online, cit. 20.04.2023). Dostupné na internete: < <https://coinmarketcap.com/sk/currencies/ethereum/> >

⁶ Proof-of-stake (PoS). (online, cit. 20.04.2023)- Dostupné na internete: < <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> >

využívajúci mixovaciu službu by mali dostať ich virtuálnu menu v dostatočnom časovom horizonte.⁷

2. MIXOVACIE SLUŽBY NA VIRTUÁLNEJ MENE BITCOIN

Vo všeobecnosti môžeme rozdeliť mixovacie služby na centralizované, decentralizované a tie, ktoré realizujú mixovanie v rámci viacerých distribuovaných verejných záznamov, resp. blockchainov.

Centralizované mixovacie služby predstavujú úplne centralizovanú architektúru, to znamená, že mixovanie pre jednoduchosť zabezpečuje jeden centrálny uzol v sieti, ktorému je nutné veriť, že poskytnuté prostriedky vo forme virtuálnej mene nezneužije na svoje osobné účely. Takéto služby neposkytujú žiadne garancie vrátenia poskytnutých virtuálnych mien, prípadne riadne vykonanie mixovacej služby, sú náchylné na kybernetické útoky, napr. DDOS alebo Sybil. Ak užívatelia siete hľadajú anonymitu v rámci virtuálnej meny, centralizované služby ju paradoxne neposkytujú, najmä z toho hľadiska, že jeden centralizovaný bod má vedomosť o celkovom toku transakcií, ktoré boli v rámci tejto služby mixované. Tieto služby majú dispozíciu mapovať vstupné adresy a priradiť ich k výstupným adresám. Za predstaviteľa takejto centralizovanej služby možno považovať Mixcoin. Tu však musíme spomenúť skutočnosť, že niektoré mixovacie služby sú projekty podložené vývojom a výskumom vedeckých výskumníkov, aj keď možno na prvý pohľad znejú ako produkty šedej ekonomiky. V prípade Mixcoinu sa jednalo o protokol, na ktorom spolupracovala univerzita Princeton, Maryland a Concordia.⁸ Väčšiu anonymitu poskytoval v mixovaní Blindcoin, ktorý nadväzoval na Mixcoin, pričom do svojho protokolu zapracoval technológiu upravujúcu podpisovanie transakcií a pridal nezmeniteľnosť jednotlivých logov. Perzistentnosť centralizovaných mixovacích služieb nie je ich doménou, preto väčšina z nich nie je funkčná a aktuálne nie sú tieto služby využívané vo veľkej miere. Za ďalších predstaviteľov mixovacích služieb možno považovať projekt BestMixer spustený v roku 2018 a skončený rok po tom z dôvodu zatknutia jeho tvorca, projekt Helix spustený v roku 2017 a ukončený rok po tom z obdobných dôvodov spomenutých vyššie, alebo projekt BitMixer z roku 2014, ktorý bol oficiálne

⁷ ZIEGELDORF, J., GROSSMAN, F., HENZE, M., INDEN, N., WEHRLE, K. 2015. In ACM Conference on Data and Application Security and Privacy. DOI: doi.org/10.1145/2699026.2699100. (online, cit. 21.04.2023). Dostupné na internete: < <https://dl.acm.org/doi/10.1145/2699026.2699100> >

⁸ Mixcoin. Anonymity for Bitcoin with accountable mixes. (online, cit. 20.04.2023). Dostupné na internete: < <https://eprint.iacr.org/2014/077.pdf> >

ukončený v roku 2017.⁹ Z dôvodu zachovania výskumnej etiky nespomíname aktuálne funkčné centralizované mixovacie služby.

Na druhú stranu *decentralizované mixovacie služby* nepredstavujú centralizovanú architektúru, to znamená, že mixovanie nepodlieha jednému centrálnemu uzlu v sieti. Eliminuje sa potreba dôvery pre realizovanie mixovania od vstupu až po samotný výstup, a to tak, že sa namiesto viacerých malých transakcií zhotoví jedna veľká transakcia, čím sa okrem iného aj zníži hodnota poplatku za vykonanie transakcie v rámci virtuálnej meny. Základným projektom predstavujúcim decentralizované mixovanie je CoinJoin, na základe ktorého boli vytvorené a produkované ďalšie projekty ako CoinShuffle, alebo SecureCoin. CoinShuffle rozširuje a zlepšuje CoinJoin napríklad v tom, že jednotlivé kryptograficky zabezpečené transakcie zo vstupu preposiela uzlom zaistujúcim permutácie dát, ktoré ďalej pokračujú na výstup. Vo výstupe si ich užívatelia mixovacej služby kryptograficky prevedú na zrozumiteľné údaje. Tento proces je následne opakovaný, až pokiaľ sa nedosiahne pre užívateľov dostatočný stupeň anonymity.¹⁰

Mixovacie služby, ktoré zaistujú mixovanie v rámci viacerých distribuovaných verejných záznamov, resp. blockchainov sú špeciálnym typom mixovacích služieb, ktoré dokážu poskytovať zmenu jednej virtuálnej meny za druhú. Tieto služby po väčšine predstavujú legitímne prostredie na zámenu virtuálnych mien. Aktuálny slovenský právny poriadok v zmysle definície poskytovateľa zmenárne virtuálnej meny podľa zákona č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov, zákonne uvádza a charakterizuje len nákup a predaj virtuálnej meny za eurá alebo inú fiat menu. Za eurá alebo inú fiat menu nie je možné považovať inú virtuálnu menu. Návrh Nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937 (ďalej aj MiCA), hovorí o prevádzkovaní obchodnej platformy pre kryptoaktíva, ktorá zahŕňa aj nákup a predaj kryptoaktíva za iné kryptoaktívum. V zmysle fundamentálnej stránky takýchto mixovacích služieb môžeme povedať, že účinnosťou MiCA budú musieť tieto služby spĺňať podmienky dané týmto nariadením. Ostatné mixovacie služby, ktoré nezabezpečujú zámenu jednej virtuálnej meny za druhú ostanú v šedej zóne. Do úvahy by mohlo prísť ich zákonné subsumovanie pod prijímanie a postupovanie pokynov týkajúcich sa kryptoaktív

⁹ ZIEGELDORF, J., GROSSMAN, F., HENZE, M., INDEN, N., WEHRLE, K. 2018. In Future Generation Computer Systems. DOI: <https://doi.org/10.1016/j.future.2016.05.018>. (online, cit. 20.04.2023). Dostupné na internete: <<https://www.sciencedirect.com/science/article/abs/pii/S0167739X16301297?via%3Dihub>>

¹⁰ tamtiež.

ako jedného z typu služby kryptoaktív. Takisto problematickým sa javí poskytovanie decentralizovaných mixovacích služieb, ktoré sú typom smart kontraktu. Uvedené však bude relevantné po účinnosti tohto nariadenia MiCA.¹¹

Mixovanie v rámci viacerých distribuovaných záznamov, resp. blockchainov zabezpečoval ZeroCoin, ktorý rozširoval Bitcoinový systém o nový typ transakcií ZeroCoin. Fungovalo to tak, že pred samotným mixovaním si účastník Bitcoinovej siete podľa predom určených pravidiel previedol svoju virtuálnu menu na ZeroCoin. Mixovanie následne prebiehalo v ZeroCoine prostredníctvom technológie Zero-Knowledge Proof¹², ktorá zaistovala vyšší stupeň anonymity. Na uvedenom staval neskôr ZeroCash¹³ alebo PinochioCoin¹⁴. Keďže sa jednalo o rozšírenia pre Bitcoin sieť, potrebovali tieto mixovacie služby neustále modifikácie a akceptáciu minimálne 51% uzlov v sieti.

Koncept mixovania v jednoduchosti pozostáva z kombinovania vstupov a výstupov viacerých strán v transakcii. Čím väčší počet jednotlivých užívateľov zapojených do mixovacej transakcie, tým zložitejšie je identifikovanie a trasovanie toku virtuálnych mien a poznávanie vzťahov medzi odosielateľmi a príjemcami reprezentovanými adresami virtuálnej meny. Takýto proces je často opakovaný, čo opäť negatívne vplýva na prelomenie dosiahnutej anonymity. Avšak ani tieto metódy a techniky nemenia fundamentálnu stránku virtuálnej meny, distribuovaný verejný záznam, blockchain alebo podmienky vytvárania jednotlivých transakcií, ktoré stále obsahujú relevantné dáta možné analyzovania.¹⁵

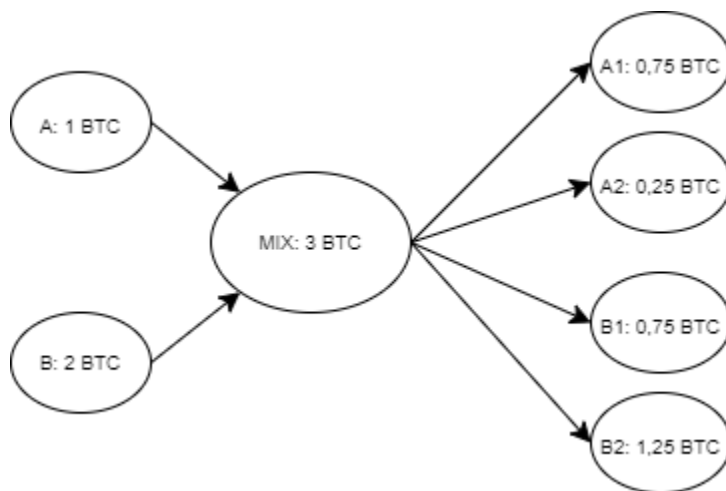
¹¹ Návrh Nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937, čl. 68,69,72

¹² What are zero-knowledge proofs ? (online, cit. 21.04.2023). Dostupné na internete: < <https://ethereum.org/en/zero-knowledge-proofs/> >

¹³ Zerocash. (online, cit. 21.04.2023). Dostupné na internete: < <http://zerocash-project.org/> >

¹⁴ DANEZIS, G., FOURNET, C., KOHWEISS, M., PARNO, B. 2013. Pinocchio coin: building zerocoin from a succinct pairing-based proof system. In Proceedings of the First ACM workshop on Language support for privacy-enhancing. (online, cit. 21.04.2023). DOI: 10.1145/2517872.2517878. Dostupné na internete: < <https://dl.acm.org/doi/10.1145/2517872.2517878> >

¹⁵ LIU, X., YU, X., ZHU, H., YANG, G., WANG, Y., YU, X. 2020. A game-theoretic approach of mixing different qualities of coins. DOI: 10.1002/int.22277. (online, cit. 20.04.2023). Dostupné na internete: < <https://onlinelibrary.wiley.com/doi/abs/10.1002/int.22277> >.



Obrázok 1 Jednoduchá schéma mixovania virtuálnej meny

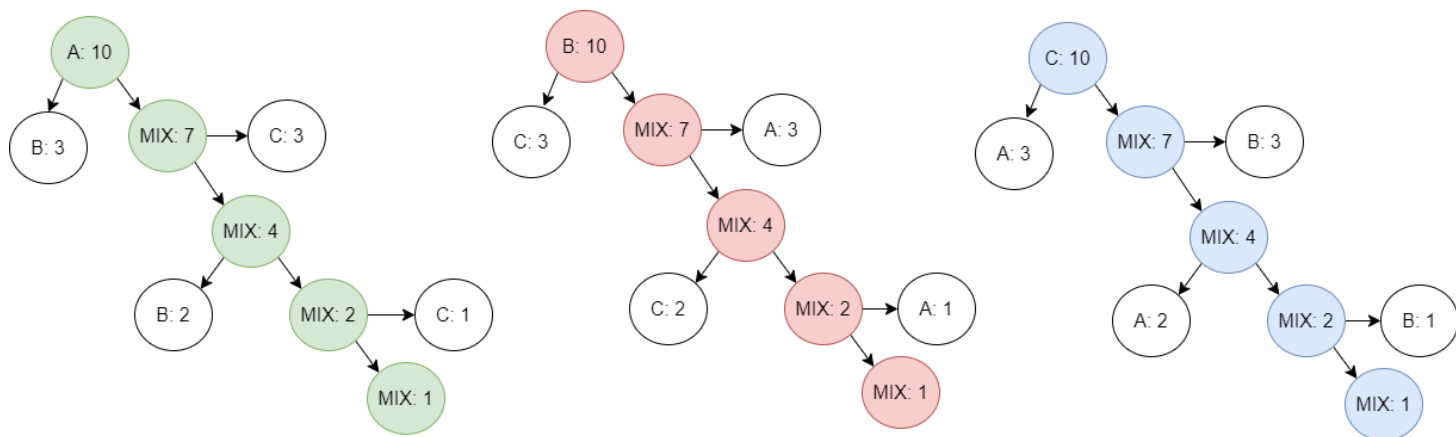
Zdroj: vlastné spracovanie

3. METÓDY ANONYMIZÁCIE TRANSAKCIÍ VIRTUÁLNYCH MIEN V RÁMCI MIXOVACÍCH SLUŽIEB

▪ Swapping

Alebo doslovne zmeny, zámenny alebo výmeny sú metódou, ktorá sa dá považovať za jednu z najčastejšie využívaných v rámci mixovacích služieb. Základnou ideou swappingu je zaistiť zámenu vstupov a výstupov medzi jednotlivými užívateľmi mixovacej služby. Namiesto toho, aby bola priamo zo vstupu odoslaná celá hodnota virtuálnej meny na viacero výstupov, ako to bolo reprezentované na obrázku č.1, mixovacia služba ich zamení s výstupom s ďalším účastníkom. Spojenie tejto štruktúry s tzv. peeling reťazcom, ktorý pozostáva zo súborov na seba nadväzujúcich transakcií virtuálnej meny, z ktorej sa „odlupujú“ čiastky virtuálnej meny, sa zabezpečuje navonok prirodzený systém transakcií virtuálnej meny s jednoduchým vstupom a jednoduchým výstupom. Pri využití peeling reťazca je jeden z výstupov používaný na generovanie výstupu pre špecifickú výstupnú adresu a iný je používaný ako výdavok, ktorý je v podstate ďalším vstupom pre nový peeling reťazec. Ako možno pozorovať z obrázka č.2, jednotlivé peeling reťazce vstupov A, B, C, ktorých hodnota je pre jednoduchosť rovnaká, sú farebne odlišené. Časová postupnosť transakcií je v tomto prípade reprezentovaná vertikálne. V každom peeling reťazci vystupujú mixovacie

adresy, ktoré zabezpečujú samotné mixovanie. Vo všetkých peeling reťazcoch dochádza k postupnému odlupovaniu virtuálnej meny pre ostatných účastníkov. Odlupovanie je realizované v jednoduchých transakciách s jedným vstupom a dvomi výstupmi, čím sa zaistuje status quo predstieranej bežnej transakčnej aktivity v rámci danej virtuálnej meny. Mixovacia služba si v tomto príklade zobrala profit za poskytnutie služby 1 BTC. Súčet vstupov a výstupov po mixovaní je u účastníkov rovnaký.¹⁶



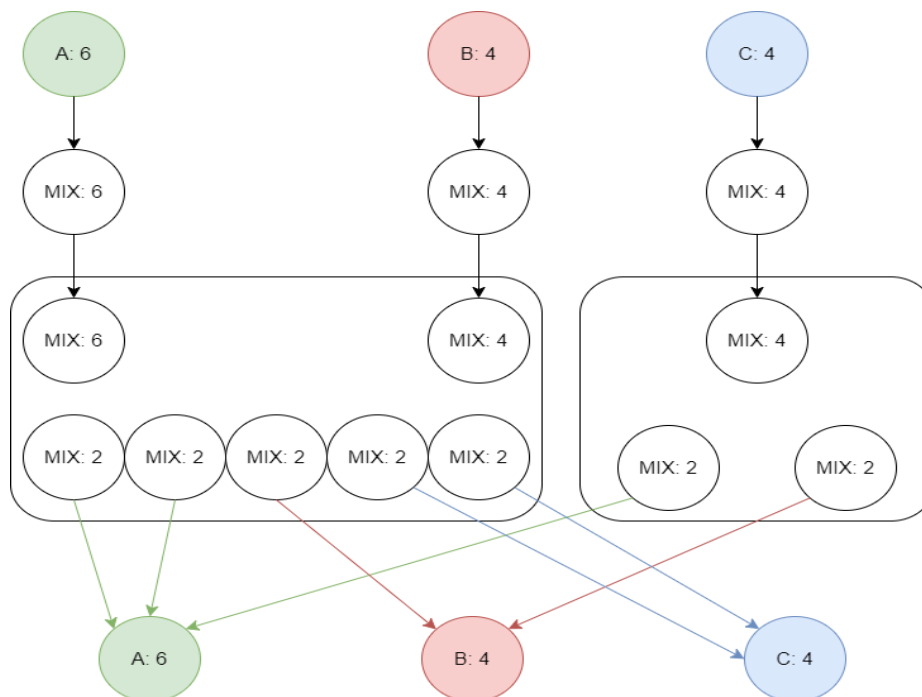
Obrázok 2: Jednoduchá schéma swapping metódy anonymizácie transakcií virtuálnej meny

Zdroj: vlastné spracovanie

▪ Obsfuscating

¹⁶ WU, L., HU, Y., YHOU, Y., WANG, H., LUO, X., WANG, Z. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In Proceedings of the Web Conference 2021. DOI: 10.1145/3442381.3449880. (online, cit. 21.04.2023). Dostupné na internete: < <https://dl.acm.org/doi/10.1145/3442381.3449880>>

alebo zastieranie je metóda, ktorá zaist'uje anonymitu prelomením spájacej procedúry medzi užívateľovými vstupmi a výstupmi, tak, že mixovacia služba použije anonymizačné sety na zakrytie užívateľových výstupov. Ako možno vidieť na obrázku č.3, anonymizačné sety sú reprezentované štvorcami, jedná sa v podstate o skonštruovanú transakciu, ktorej výstupy sú hodnoty, ktoré od seba nie je možné vzhľadom na poznanie ich sumy rozlíšiť. Následne sú tieto výstupy odosielané jednotlivým účastníkom siete. Obfuscating metóda môže pracovať s jedným



Obrázok 3: Jednoduchá schéma obfuscating metódy anonymizácie transakcií virtuálnej meny

alebo viacerými anonymizačnými setmi. Viaceré anonymizačné sety môžu generovať viacero menších výstupov s hodnotami, ktoré si špecifikujú užívatelia. Na základe týchto požiadaviek, ktoré mixovacia služba prijme sa nastaví jednotlivé anonymizačné sety.¹⁷

4. MIXOVACIE SLUŽBY NA VIRTUÁLNEJ MENE ETHEREUM

Ethereum je virtuálna mena, ktorá má veľa spoločných fundamentálnych prvkov s virtuálnou menou Bitcoin. Poznanie virtuálnych mien a ich fundamentu nie sú predmetom skúmania tohto príspevku, avšak je potrebné spomenúť skutočnosť, že Ethereum akoto virtuálna mena

¹⁷ WU, L., HU, Y., YHOU, Y., WANG, H., LUO, X., WANG, Z. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In Proceedings of the Web Conference 2021. DOI: 10.1145/3442381.3449880. (online, cit. 21.04.2023). Dostupné na internete: < <https://dl.acm.org/doi/10.1145/3442381.3449880>>

sprostredkováva dva typy účtov, ktoré sú nevyhnutné pre tvorbu transakcií. Jedným typom je účet s vonkajším vlastníctvom, pri ktorom účastník siete vlastní kľúčový pár, pričom privátny kľúč slúži najmä na podpisovanie transakcií. Druhým typom sú kontraktné účty alebo smart kontrakty, ktoré majú charakter programu s vlastným zdrojovým kódom napísaným v programovacom jazyku Solidity a umiestneným na blockchain Etherea. Takýto smart kontrakt dokáže fungovať v rámci decentralizovanej siete za podmienok určených fundamentom virtuálnej meny Ethereum.¹⁸

Jednou z významných mixovacích služieb v rámci Etherea je MixEth, ktorý je smart kontraktom umožňujúcim efektívne mixovanie virtuálnej meny bez nutnosti dôverovania centrálnemu uzlu. Účastník, ktorý chce mixovať virtuálnu menu Ethereum (ďalej aj „ether“) prostredníctvom MixEth musí byť inicializovaný parametrom, ktorý určí nominálnu hodnotu etheru určeného na mixovanie. Následne musí každý účastník vložiť do siete toľko depozitu, koľko určil spomínaný parameter, a určiť verejnú adresu, na ktorú chce neskôr zaslať výstup. V prípade, ak by nebol vložený presne určený depozit, smart kontrakt danú transakciu vyhodnotí ako nevalidnú a verejná adresa sa zamietne. Ak vkladanie depozitov prebehne, na rad prichádza samotné miešanie a overovanie. Po každom mixovaní dochádza k overovaniu, ktorým sa sleduje správnosť mixovania. Ak by niekto overovaním zistil nekalú činnosť vo vnútri mixovania, depozit účastníka by prepadol v prospech uzla, ktorý vykonal overovanie. Ak skončí overovanie, nasleduje ďalšie kolo samotného mixovania. Overovanie sa realizuje prostredníctvom Chaum-Pederson dôkazu.¹⁹ MixEth je možné aplikovať on-chain, to znamená, že celé mixovanie prebehne prostredníctvom transakcií, ktoré sa zapisujú na blockchain Etherea. Druhým spôsobom je rozdelenie mixovania na on-chain operácie a off-chain operácie, pričom off-chain je realizovaná najmä operácia samotného mixovania a operácia overovania, on-chain je realizovaná operácia súvisiaca so vstupmi a s výstupmi.

Ďalšou mixovacou službou je Möbius, ktorá bola spustená v roku 2017 a pozostáva z dvoch základných častí, a to klientskej aplikácie a smart kontraktu, ktorý funguje na blockchaine Etherea. Aplikácia umožňuje vkladať virtuálne meny na verejnú adresu mixovacej služby, pričom smart kontrakt zabezpečuje samotné mixovanie a zasielanie výstupov na adresy užívateľov tejto

¹⁸ Introduction to smart contracts. (online, cit. 21.04.2023). Dostupné na internete: < <https://ethereum.org/sk/smart-contracts/> >

¹⁹ Chaum-Pedersen Zero Knowledge Proof. (online, cit. 21.04.2023). Dostupné na internete: < <https://asecuritysite.com/encryption/chaum> >

mixovacej služby. ²⁰ Opomenúť nemožno ani Miximus, ktorý používa technológiu zkSNARKs pre ukrytie možného zmapovania užívateľov na vstupe a užívateľov na výstupe. Tá ma však nevýhodu v tom, že ak jej setup prezradený, tvorca smart kontraktu môže vygenerovať kľúč, ktorým je možné ukradnúť virtuálne meny uložené v smart kontrakte za účelom mixovania. ²¹ Za ďalšie centralizované mixovacie služby v rámci Etherea možno považovať Mixcoin, Blindcoin, TumbleBit. Za ďalšie decentralizované mixovacie služby možno považovať XIM a MixEthChannel. ²²

5. MOŽNÉ RIEŠENIA

▪ Teória hier

Pri mixovaní virtuálnej meny môže dôjsť k situácii, kedy užívateľ siete, ktorý realizuje anonymizačné činnosti z dôvodu legalizácie výnosov z trestnej činnosti premieša svoj výnos z trestnej činnosti vo forme virtuálnej meny s virtuálnou menou osoby, ktorá realizuje anonymizačné činnosti z iného dôvodu, ktoré nie je nelegálny. Ak je počas blockchain analýzy zistené, že má určitá adresa súvis s trestnou činnosťou, uvedie sa na čiernu listinu. Čiernu listinu spravuje ten subjekt, ktorý vykonáva blockchain analýzu a už samotné poskytnutie adries a transakcií na čiernej listine iným subjektom, ako sú napríklad orgány činné v trestnom konaní môže zefektívniť trasovanie virtuálnej meny. Takéto transakcie a adresy virtuálnej meny môžeme pre jednoduchosť nazvať znečistené virtuálne meny. Aby nedochádzalo k zmiešaniu týchto znečistených virtuálnych mien s čistými virtuálnymi menami je potrebné predstaviť systém, ktorý by demotivoval účastníkov siete so znečistenými virtuálnymi menami používať mixovacie služby. Jednou z možností je vytvorenie smart kontraktu, ktorý by ukladal depozity, akoto kolaterál, zálohu za vykonanie mixovania. Takýto depozit by slúžil ako záruka na dodržiavanie pravidiel určených smart kontraktom a pôsobil by preventívne na účastníkov siete. Uvoľňovanie depozitu by prebehlo

²⁰ MERCER, R., MEIKLEJOHN, S. 2018. Möbius: Trustless Tumbling for Transaction Privacy. (online, cit. 21.04.2023). Dostupné na internete: <<https://smeiklej.com/files/pets18.pdf>>

²¹ Miximus. (online, cit. 21.04.2023). Dostupné na internete: <<https://github.com/barryWhiteHat/miximus>>

²² SERES, I., NAGY, D., BUCKLAND, CH., BURCSI, P. 2020. MixEth: Efficient, Trustless Coin Mixing Service for Ethereum. In International Conference on Blockchain Economics, Security and Protocols. DOI: 10.4230/OASICS.Tokenomics.2019.13. (online, cit. 20.04.2023). Dostupné na internete: <<https://drops.dagstuhl.de/opus/volltexte/2020/11977/>>

až v čase po mixovaní, kedy by už bolo z blockchain analýzy jasné, či sa jedná o znečistené virtuálne meny.

Predstavujeme 3 stratégie, ktoré by mohol uvedený smart kontrakt zabezpečovať:

○ *Stratégia 1*

V prípade, ak by jeden z účastníkov mixoval znečistené virtuálne meny, všetky výstupy bez rozdielu by sa zaradili na čiernu listinu. Všetky výstupy, ktorých predchodcom by bola znečistená virtuálna mena by boli označené za invalidné. V rámci tejto stratégie platí, že virtuálne meny v mixovacej službe sú buď čisté alebo znečistené. Užívatelia majú teda dve možné taktiky, ktoré reprezentujú túto stratégiu. Ak sa v mixovaní objaví znečistená virtuálna mena, tak všetky virtuálne meny na výstupe budú označené za znečistené. Ak teda užívatelia pri vstupe nevedia určiť kvalitu virtuálnych mien, nebudú ochotní použiť mixovaciu službu. Predstavme si situáciu, kedy by pri tejto stratégii bolo nutné do smart kontraktu uzavrieť depozit medzi dvomi účastníkmi siete, ktorý by hovoril, že ak budú na výstupe virtuálne meny zistené ako znečistené, prepadne depozit v prospech toho, kto mixoval čisté virtuálne meny. Takáto situácia by motivovala účastníkov používať mixovaciu službu iba v prípade, ak by chceli mixovať čisté virtuálne meny, pretože by sa im mixovanie jednoducho vo vzťahu k teórii profitu neoplatilo.

○ *Stratégia 2*

Táto stratégia by rozdeľovala všetky výstupy proporčne k celkovému počtu znečistených virtuálnych mien na vstupe. To znamená, že by každý výstup obsahoval určitú časť znečistených virtuálnych mien, čo by bolo následne prepočítané na hodnotu celkových znečistených virtuálnych mien na vstupe. Táto stratégia pracuje s vstupnými predpokladmi, že ak sú dvaja účastníci mixovacej služby, ktorí si z princípu nedôverujú a zároveň nevedia určiť kvalitu vstupných virtuálnych mien, určia si predom podmienky. Účastníci siete prezumujú, že pomer vstupných znečistených a čistých virtuálnych mien toho druhého je 1:1. V takomto prípade obidvaja do smart kontraktu uzamknú depozit 25% zo svojich vstupných virtuálnych mien. Ak pomer znečistených virtuálnych mien na výstupe u jedného účastníka presiahne prezumovanú hodnotu 50%, druhý dostane depozit a uvedie prvého na čiernu listinu. Ak do uvedenej mixovacej služby vstupuje osoba za účelom legalizovania výnosov z trestnej činnosti, potrebuje mixovať výnosy s čistými

virtuálnymi menami. Táto stratégia poukazuje na skutočnosť, že čím väčšia hodnota znečistených virtuálnych mien v mixovacej službe, tým je menšia pravdepodobnosť úspešnej legalizácie takýchto výnosov. Táto stratégia by demotivovala páchatel'ov trestnej činnosti využívať mixovacie služby najmä z toho dôvodu, že by nedosiahli účel legalizácie výnosov z trestnej činnosti.

- *Stratégia 3*

Podobne ako pri druhej stratégii, usporiadanie a sumy výstupov by podmieňovali to, ako budú znečistené virtuálne meny distribuované. V tejto stratégii by panoval predpoklad, že sa znečistené virtuálne meny rozosielať tak ako sú usporiadané výstupy. V tejto stratégii sa prezumuje, že ak je v mixovaní riziko získania znečistených virtuálnych mien, je pravdepodobnejšie, že účastníci pre mixovanie takisto použijú znečistené virtuálne meny. Ak jeden účastník požiadá o mixovanie virtuálnych mien, druhý prezumuje, že napríklad 10% z tých, ktoré prvý zadá do vstupu bude znečistených a takúto hodnotu pre výstup akceptuje. Podľa tejto stratégie musí prvý účastník odovzdať depozit v hodnote dvojnásobku svojho vkladu. Ak je vo výstupe viac ako deklarovaných 10% vkladu znečistených, druhý účastník dostane depozit zo smart kontraktu a zaznamená prvého účastníka na čiernu listinu. Predom určená podmienka a vysoký depozit demotivuje páchatel'ov trestnej činnosti používať mixovacie služby.²³

- **Jednoduchá blockchain analýza transakcií**

Táto možnosť pozostáva z viacerých krokov, ktoré je možné použiť pre analýzu jednotlivých transakcií v rámci mixovacích služieb, ak je podozrenie, že jednotliví účastníci siete realizujú legalizovanie výnosov z trestnej činnosti. Prvým krokom je determinovanie, či jednotlivé mixovacie služby využívajú metódu swappingu alebo obfuscatingu, potom je potrebné pochopiť špecifické aplikačné znaky virtuálnej meny a použiť metódy aplikovanej na danú mixovaciu službu. Následne je potrebné využiť samotnú blockchain analýzu, sledovanie a párovanie transakcií, využívanie grafov a schém, ktoré pri nie zložitých situáciách postačia na efektívne odhalenie toku transakcií, vstupných a výstupných adries a identifikovaní páchatel'a.

- **Podrobná blockchain analýza transakcií**

²³ LIU, X., YU, X., ZHU, H., YANG, G., WANG, Y., YU, X. 2020. A game-theoretic approach of mixing different qualities of coins. DOI: 10.1002/int.22277. (online, cit. 20.04.2023). Dostupné na internete: < <https://onlinelibrary.wiley.com/doi/abs/10.1002/int.22277>>.

Pri využití podrobnej blockchain analýzy je potrebné okrem krokov uvedených vyššie aj zhodnotiť efektivitu algoritmu, na základe ktorého beží daná mixovacia služba. Odporúča sa aj zhodnotiť a vypočítať profit, ktorý je reálne uhrádzaný mixovacej službe. Na základe uvedeného je okrem toku transakcií možné odhaliť aj technické chyby a nedokonalosti, na základe ktorých je možné ďalej postupovať pri de anonymizovaní celej mixovacej služby. Je však potrebné si uvedené techniky vyskúšať experimentovaním tak, aby sa v čo najväčšej miere obmedzila skutočnosť odhalenia zásahu do mixovacej služby. Zlyhanie by spôsobilo vlnu protiopatrení zo strany tvorcov, čo by predstavovalo riziko pre dosiahnutie účelu podrobnej blockchain analýzy transakcií.²⁴

▪ Špeciálne analytické nástroje

AITs systém pre sledovanie identity v rámci virtuálnej meny je jeden zo špeciálnych analytických nástrojov, ktoré používajú orgány činné v trestnom konaní. Jeho podstatou je trasovanie toku virtuálnych mien a zisťovanie identity účastníka siete reprezentovaného verejnou adresou virtuálnej meny. Tento nástroj je určený pre blockchain Etherea, presnejšie pre účty s vonkajším vlastníctvom spomínané vyššie, a poskytuje cenné údaje aj pre off chain vyšetrenia. AITs pozostáva z backendu, ktorý vykonáva podstatné analytické činnosti na pozadí; frontendu, ktorý sprostredkováva vizualizáciu a grafické ilustrácie pre používateľov; API, algoritmu, ktorý zbiera blockchain dáta do databáz a grafových modelov; Etherscan, ktorý slúži na skenovanie Ethereum blockchainu; a databáz a grafov. Takýto nástroj dokáže efektívne spracovať celý dej nelegálnych aktivít, poskytuje obraz o moduse operandi a správaní jednotlivých páchatel'ov v sieti. V ďalšom vývoji tohto softvéru sa plánuje aj implementovanie umelej inteligencie na dodatočné zefektívnenie tohto nástroja.²⁵ Považujeme za potrebné zdôrazniť, že tento nástroj je novinkou v sfére analýzy transakcií virtuálnych mien.

²⁴ WU, L., HU, Y., YHOU, Y., WANG, H., LUO, X., WANG, Z. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In Proceedings of the Web Conference 2021. DOI: 10.1145/3442381.3449880. (online, cit. 20.04.2023). Dostupné na internete: < <https://dl.acm.org/doi/10.1145/3442381.3449880>>

²⁵ WERAPUN, W., SUABOOT, J. 2023. An EOA Identity Tracing System (AITs) on Ethereum Blockchain. In Conference on Information and Network Technologies (ICINT 2023). (online, cit. 20.04.2023). Dostupné na internete: <https://www.researchgate.net/publication/368960770_An_EOA_Identity_Tracing_System_AITs_on_Ethereum_Blockchain>

Záver

Samotná anonymita transakcií virtuálnych mien a samotné využívanie metód a techník zabezpečujúcich anonymitu v prostredí virtuálnych nie je možné považovať za negatívny jav. Negatívnym javom však je, ak sa prostredníctvom metód anonymizovania transakcií virtuálnych mien legalizujú výnosy z trestnej činnosti. Boj proti legalizovaniu môže byť silno reštriktívny, môže mať formu prelomenia alebo zákazu mixovacej služby, avšak takéto niečo je aktuálne veľmi ťažko dosiahnuteľné. Schodnejšie je využívať také možnosti riešenia, ktoré sú podmienené motiváciou jednotlivých účastníkov siete od seba odčleniť páchatel'ov trestnej činnosti, resp. vytvorenie systému, v ktorom by nebolo v rámci teórie hier a teórie profitu efektívne realizovať legalizáciu výnosov z trestnej činnosti. V príspevku poukazujeme na smart kontrakt s tromi stratégiami, ktoré by potenciálne mohli dosiahnuť uvedený účel. Pri príprave na zločin, pokuse o trestný čin alebo pri dokonanom trestnom čine však už nie je možné pôsobiť preventívne a orgány činné v trestnom konaní musia disponovať aj možnosťami represívneho zasiahnutia. V tomto ohľade príspevok ponúka možnosti ako je jednoduchá alebo podrobná analýza virtuálnych mien, ktorá slúži ako nástroj na identifikovanie toku transakcií aj pri využití anonymizačných metód a techník. Zefektívnenie takejto blockchain analýzy poskytujú aj špeciálne analytické a grafické nástroje, ktorých príkladom je AITS systém.

Zoznam použitej literatúry

LIU, X., YU, X., ZHU, H., YANG, G., WANG, Y., YU, X. 2020. A game-theoretic approach of mixing different qualities of coins. DOI: 10.1002/int.22277. (online, cit. 20.04.2023). Dostupné na internete: < <https://onlinelibrary.wiley.com/doi/abs/10.1002/int.22277> >.

WU, L., HU, Y., YHOU, Y., WANG, H., LUO, X., WANG, Z. 2021. Towards Understanding and Demystifying Bitcoin Mixing Services. In Proceedings of the Web Conference 2021. DOI: 10.1145/3442381.3449880. (online, cit. 20.04.2023). Dostupné na internete: < <https://dl.acm.org/doi/10.1145/3442381.3449880> >

YANOVICH, Y., MISCHENKO, P., OSTROVSKIY, A. 2016. Shared Send Untangling in Bitcoin. (online, cit. 20.04.2023). Dostupné na internete: <<http://cryptochainuni.com/wp-content/uploads/bitfury-whitepaper-shared-send-untangling-in-bitcoin-8-24-2016.pdf>>

WERAPUN, W., SUABOOT, J. 2023. An EOA Identity Tracing System (AITS) on Ethereum Blockchain. In Conference on Information and Network Technologies (ICINT 2023). (online, cit. 20.04.2023). Dostupné na internete: <https://www.researchgate.net/publication/368960770_An_EOA_Identity_Tracing_System_AIT_S_on_Ethereum_Blockchain>

VAN WEGBERG, R. OERLEMANS, J.-J., VAN DEVENTER, O. 2018. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. In Journal of Financial Crime. DOI: 10.1108/JFC-11-2016-0067. (online, cit. 20.04.2023). Dostupné na internete: <<https://www.emerald.com/insight/content/doi/10.1108/JFC-11-2016-0067/full/html>>

ZIEGELDORF, J., GROSSMAN, F., HENZE, M., INDEN, N., WEHRLE, K. 2018. In Future Generation Computer Systems. DOI: <https://doi.org/10.1016/j.future.2016.05.018>. (online, cit. 20.04.2023). Dostupné na internete: <<https://www.sciencedirect.com/science/article/abs/pii/S0167739X16301297?via%3Dihub>>

ZIEGELDORF, J., GROSSMAN, F., HENZE, M., INDEN, N., WEHRLE, K. 2015. In ACM Conference on Data and Application Security and Privacy. DOI: doi.org/10.1145/2699026.2699100. (online, cit. 21.04.2023). Dostupné na internete: <<https://dl.acm.org/doi/10.1145/2699026.2699100>>

SERES, I., NAGY, D., BUCKLAND, CH., BURCSI, P. 2020. MixEth: Efficient, Trustless Coin Mixing Service for Ethereum. In International Conference on Blockchain Economics, Security and Protocols. DOI: 10.4230/OASICS.Tokenomics.2019.13. (online, cit. 20.04.2023). Dostupné na internete: <<https://drops.dagstuhl.de/opus/volltexte/2020/11977/>>

ŠANTA, J., ŠANTA, I. Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami. In: Justičná revue. – Roč. 2022, Vydanie 10/2022, s. 1146 - 1164.

ŠANTA, J., ŠANTA, I., SZABOVÁ, E.: Manipulácia s trhom – niektoré medzinárodné a trestnoprávne aspekty. In: Justičná revue. – Roč. 2022, Vydanie 11/2022, s. 1296 - 1311.

ŠANTA, J., ŠANTA, I.: K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a Slovenskej republiky. In: Justičná revue. – Roč. 2022, Vydanie 2/2022, s.164 – 179

ŠANTA, J., ŠANTA, I., ŠIROKÝ, T.: K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. In: Justičná revue. – Roč. 2022, Vydanie 4/2022, s. 484-499.

ŠANTA, J., ŠANTA, I.: Riziká investovania do virtuálnych mien z ekonomického a trestnoprávneho hľadiska. In: Justičná revue. – Roč. 2022, Vydanie 3/2022, s. 365 – 378.

HOSP, J. Kryptomeny, Bratislava: TATRAN, 2021., str. 170. ISBN: 978-80-222-0945-8.

Ethereum. (online, cit. 20.04.2023). Dostupné na internete: < <https://ethereum.org/sk/>>

Kontaktné údaje

Mgr. Andrej Lipták

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava e-mail:

andrej.liptak@akademiapz.sk

Recenzenti:

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

doc. RNDr. Tatiana Hajdúková, PhD

Právne podmienky ochrany osobných údajov v internetovom priestore **Legal Terms for the Protection of Personal Data in the Online Space**

Miriam Odlerová

Abstrakt

Internet v súčasnosti stále viac využívame na rôzne účely, čím sa tento priestor stáva cieľom pre rôzne formy kybernetických útokov, ale aj zneužitia osobných údajov. Slovenská legislatíva napriek tomu umožňuje za určitých podmienok zverejňovanie pomerne širokého okruhu osobných údajov. Cieľom článku je analyzovať možnosti zverejňovania osobných údajov na internete a načrtnúť otázku opodstatnenosti niektorých právnych základov.

Kľúčové slová

osobné údaje, zverejňovanie osobných údajov, oprávnený záujem, súhlas dotknutej osoby, právny základ spracúvania osobných údajov, právo na súkromie, právo na ochranu osobnosti

Abstract

The internet is increasingly being used for various purposes, making this space a target for various forms of cyber attacks and misuse of personal data. Despite this, Slovak legislation allows for the publication of a fairly wide range of personal data under certain conditions. The aim of the article is to analyze the possibilities of publishing personal data on the internet and to outline the question of the justification of certain legal bases.

Key words

personal data, disclosure of personal data, legitimate interest, consent of the data subject, legal basis for processing personal data, right to privacy, right to protection of personality

Úvod

Najväčším zdrojom informácií je dnes jednoznačne internet. Potreba chrániť svoje osobné údaje na internete je v súčasnosti odôvodnená viac ako inokedy. S narastajúcim využívaním internetu pre rôzne účely, ako napríklad nakupovanie, bankové transakcie či komunikáciu na sociálnych sieťach, sa stáva internetový priestor cieľom pre rôzne formy kybernetických útokov a zneužitia osobných údajov. Preto je dôležité správať sa v internetovom priestore čo najviac opatrne a bezpečne. Jedným z najdôležitejších krokov je používanie silných hesiel a ich pravidelná zmena. Ďalším krokom je zabezpečenie bezpečného pripojenia k internetu a používanie overených zdrojov pre rôzne transakcie. V neposlednom rade je potrebné dobre si premyslieť, komu povolíme prístup k našim osobným údajom a kde ich zdieľame.

Avšak aj keď používateľ internetu dodržiava všetky bezpečnostné pravidlá a chráni si svoje osobné údaje, zverejniť ich môže niekto iný – či už legálne alebo nelegálne. Závažným problémom

ochrany osobných údajov v internetovom priestore je dnes práve zverejňovanie a zdieľanie fotografií, videí a iných osobných údajov bez súhlasu dotknutej osoby, či iného relevantného právneho základu. Ďalším problémom, ktorý bol nedávno predmetom rozhodovania Súdneho dvora EÚ, je rozsah zverejňovaných údajov, kedy sú právnym základom takéhoto spracúvania práve niektoré osobitné právne predpisy. Tie sprístupňujú na internete osobné údaje vo verejných častiach rôznych registrov pre širokú verejnosť.

Právo na ochranu osobných údajov

Ochrana osobných údajov nie je novodobým fenoménom, v určitej forme tu s nami existuje minimálne od prijatia *Všeobecnej deklarácie ľudských práv* v roku 1948, ktorá deklaruje, že „*Nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromia, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takýmto zásahom alebo útokom.*“¹. Podobne je toto právo zakotvené v *Dohovore o ochrane ľudských práv a základných slobôd* z roku 1950: „*Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie*“.²

Právo na ochranu osobných údajov sa v týchto dokumentoch premieta v **práve na ochranu súkromia**. Účelom práva na súkromie je chrániť jednotlivcov pred zasahovaním do ich osobného života zo strany štátu, iných osôb alebo organizácií. Toto právo uznáva, že každý má právo na súkromie a na ochranu svojho osobného a rodinného života, obydlia a komunikácie. Cieľom práva na súkromie je zabezpečiť, aby jednotlivci mali kontrolu nad tým, aké informácie sa o nich zberajú, uchovávali a zdieľajú, a aby tieto informácie neboli zneužívané. Právo na súkromie je preto kľúčové pre ochranu základných práv a slobôd jednotlivcov a zahŕňa aj **informačné súkromie**. Balážiková A. uvádza, že „*Informačné súkromie môže označovať iba súkromie osobných údajov, ale vzhľadom na súčasnú spätosť komunikácie s výpočtovou technikou sa často využíva na spoločné pomenovanie komunikačného a dátového súkromia.*“³ Informačné súkromie zahŕňa takisto niekoľko oblastí a jednou z nich je práve **internetové súkromie**. Internetové súkromie sa týka ochrany osobných údajov používateľov v online prostredí. Zahrňuje právo na kontrolu nad tým, aké informácie sa o používateľovi zbierajú, uchovávali, zdieľajú, či inak spracúvajú na internete.

¹ Čl. 12 Všeobecnej deklarácie ľudských práv.

² Čl. 8 ods. 1 Dohovoru o ochrane ľudských práv a základných slobôd.

³ BALÁŽIKOVÁ, A. Právo na súkromie v informačnej spoločnosti. In: *Informačné technológie a knižnice*. [online]. [citované 3. mája 2023]. Dostupné na internete: <https://itlib.cvtisr.sk/%c4%8c%3%a1nky/clanek815/>

Internetové súkromie sa vzťahuje na rôzne aspekty online aktivít, ako sú prehliadačové aktivity, komunikácia cez email, sociálne siete, cloudové úložisko a podobne.

S rozvíjajúcimi sa technológiami bolo potrebné účinnejšie zabezpečiť práve internetové súkromie, a preto bol v januári 1981 otvorený na podpis ***Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor 108)***. Jeho cieľom je zabezpečiť ochranu základných práv a slobôd jednotlivcov v súvislosti so spracúvaním ich osobných údajov. Dohovor stanovuje pravidlá pre zber, uchovávanie, spracúvanie a ochranu osobných údajov, a to najmä v súvislosti so zásadou správnosti, účelnosti, zákonnosti, množstvom a kvalitou údajov, ich zabezpečením a ochranou proti neoprávnenému prístupu. Dohovor tiež ustanovuje, že každá osoba má právo na prístup k svojim osobným údajom a na ich opravu v prípade nepravdivosti. Osoby majú tiež právo na odvolanie súhlasu so spracúvaním svojich osobných údajov a na náhradu škody, ktorú im môže spôsobiť neoprávnené spracúvanie. Dohovor prešiel niekoľkokrát modernizáciou, čím reagoval na výzvy vyplývajúce z využívania nových informačných a komunikačných technológií, z posilnenia účinnej implementácie, či z potreby v čo najväčšej možnej miere stierať rozdiely medzi jednotlivými štátmi a týmto spôsobom zabezpečiť relevantnú úroveň ochrany súkromia vo svete.

Európska únia uznáva právo na ochranu osobných údajov ako samostatné právo, čo zakotvila aj v ***Charte základných práv Európskej únie*** z roku 2000, ktorá explicitne stanovuje, že „Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú“⁴. Zakotvuje aj právne základy spracúvania osobných údajov vrátane súhlasu dotknutej osoby, právo na prístup k osobným údajom, právo na ich opravu a tiež povinnosť kontroly nezávislým orgánom.

Najdôležitejší prameň sekundárneho práva Európskej únie v oblasti ochrany osobných údajov je v súčasnosti ***nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)*** (ďalej len „nariadenie GDPR“). Nariadenie GDPR nahradilo predchádzajúcu smernicu o ochrane osobných údajov z roku 1995 a vstúpilo do platnosti v máji 2018. Jeho cieľom je chrániť základné práva a slobody fyzických osôb v súvislosti so spracúvaním ich osobných údajov a zabezpečiť, aby

⁴ Čl. 8 Charty základných práv Európskej únie.

sa takéto údaje spracúvali v súlade so zásadami transparentnosti, správnosti, obmedzenia účelu, minimálneho spracúvania, presnosti, obmedzenia uchovávanía, integrity a dôvernosti.

V Slovenskej republike bol v roku 2018 prijatý **zákon č. 18/2018 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov** (ďalej len „zákon o ochrane osobných údajov“), ktorý upravuje ochranu práv fyzických osôb pred neoprávneným spracúvaním ich osobných údajov, práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb a postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky.

Spracúvanie osobných údajov – vysvetlenie pojmov

Zákon o ochrane osobných údajov definuje **osobné údaje** ako „údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.“⁵ V rovnakom rozsahu definuje osobné údaje aj nariadenie GDPR vo svojom čl. 4 bod 1. Čo je a čo nie je osobný údaj, nie je možné vymedziť absolútne. Každý jeden prípad je potrebné skúmať osobitne. „Miera, do akej sú identifikátory v danom prípade postačujúce na identifikovanie konkrétnej fyzickej osoby, závisí od posúdenia dostupných údajov v ich vzájomnej súvislosti a zároveň aj situácie ako celku. Napríklad často používané priezvisko spravidla nebude postačovať na identifikáciu fyzickej osoby v rámci väčšej skupiny obyvateľstva v danom územnom obvode, avšak je pravdepodobnejšie, že bude postačovať na identifikáciu zamestnanca na konkrétnom pracovisku.“⁶

Internet je však dnes hlavný nástroj pre zdieľanie fotografií a videí, a to najmä prostredníctvom sociálnych sietí. V tejto súvislosti podotýkam, že aj fotky a videá môžu byť považované za osobné údaje a to vtedy, ak identifikujú konkrétnu fyzickú osobu alebo existuje možnosť identifikovať ju. Fotografia môže byť považovaná za osobný údaj, aj keď nie je doplnená

⁵ § 2 zákona o ochrane osobných údajov.

⁶ VALENTOVÁ, T., BIRNSTEIN, M., GOLAI, J. *GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov*. Bratislava: Wolters Kluwer, 2018, s. 88.

inými údajmi, ako napríklad menom osoby, ak existuje možnosť, že by sa na základe fotografie dala táto osoba identifikovať. Preto sa fotografia alebo video považuje za osobný údaj podľa nariadenia GDPR a jej spracúvanie musí byť v súlade s pravidlami ochrany osobných údajov.

Európsky výbor pre ochranu údajov (EDPB) vydal dňa 29. januára 2020 Usmernenia č. 3/2019, v ktorých sa poskytujú rady, ako uplatňovať nariadenie GDPR v súvislosti so spracúvaním osobných údajov prostredníctvom kamerových zariadení⁷ (ďalej len „usmernenie“). Ako je však v úvode usmernení upozornené, uvádzané príklady nie sú vyčerpávajúce, avšak všeobecné zdôvodnenie je možné uplatniť vo všetkých potenciálnych oblastiach použitia.

Usmernenie vychádza z definície osobných údajov uvedenej v nariadení GDPR. Konkrétne hovorí o tom, že ak je možné z obrazového alebo obrazovo-zvukového záznamu identifikovať osobu/osoby, čo následne aj umožňuje spracúvať takéto údaje, vzťahuje sa na uvedenú činnosť nariadenie GDPR. Toto vyjadrenie sa však vzťahuje na systematické automatické monitorovanie konkrétneho priestoru optickými alebo audiovizuálnymi prostriedkami, predovšetkým na účely ochrany majetku alebo na ochranu života a zdravia jednotlivca. Podľa § 35 ods. 3 písm. c) nariadenia GDPR sa v tomto prípade vyžaduje posúdenie vplyvu na ochranu údajov, nakoľko takáto činnosť pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov.

Odlišná situácia nastáva pri fotografiách a videách pre súkromné/domáce účely. Predmetné predpisy sa totiž nevzťahujú na spracúvanie osobných údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti.⁸ Podľa nariadenia GDPR osobné alebo domáce činnosti by mohli zahŕňať korešpondenciu a uchovávanie adries či využívanie sociálnych sietí a online činnosti vykonávané v kontexte takýchto činností. Toto nariadenie sa však vzťahuje na prevádzkovateľov alebo sprostredkovateľov, ktorí poskytujú prostriedky na spracúvanie osobných údajov na takéto osobné alebo domáce činnosti. Výnimku pre „domáce činnosti“ je podľa Európskeho súdneho dvora potrebné vykladať tak, že *„sa vzťahuje výlučne na činnosti, ktoré patria do rámca*

⁷ European Data Protection Board. *Usmernenia 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení z 29. januára 2020*. [online]. [citované 3. mája 2023]. Dostupné na internete: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_sk.pdf

⁸ Pozri čl. 2 ods. 2 písm. c) nariadenia GDPR a § 3 ods. 5 písm. a) zákona o ochrane osobných údajov.

súkromného alebo rodinného života jednotlivcov, čo zjavne neplatí v prípade spracúvania osobných údajov, ktoré spočíva v ich zverejnení na internete takým spôsobom, že sa sprístupnia neobmedzenému počtu osôb.“⁹ Ak by však monitorovanie kamerou zahŕňalo nepretržité zaznamenávanie a uchovávanie osobných údajov a pokrývalo by „hoci len čiastočne, verejné priestranstvo, a smeruje mimo súkromnú sféru osoby, ktorá jeho prostredníctvom spracúva údaje, nemožno ho považovať za výlučne ‘osobnú či domácu’ činnosť v zmysle článku 3 ods. 2 druhej zarážky smernice 95/46.“¹⁰

Okrem toho sú zvlášť definované **osobitné kategórie osobných údajov**. Ide o údaje vyžadujúce si zvýšenú ochranu a starostlivosť pri ich spracúvaní. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby. Ich spracúvanie je v zásade zakázané, avšak existujú určité výnimky, ktoré pripúšťa zákon o ochrane osobných údajov, napríklad dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel, spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila atď.¹¹

Ďalší dôležitý pojem, ktorý je potrebné vysvetliť v súvislosti s osobnými údajmi, je **spracúvanie**. To je definované v čl. 4 bod 2 nariadenia GDPR (a podobne v § 5 písm. e) zákona o ochrane osobných údajov) ako „operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami“. Činnosti považované za spracúvanie osobných údajov sú vymenované deklaratórnym spôsobom, a teda môžu zahŕňať aj iné operácie či postupy s osobnými údajmi. Spracúvanie osobných údajov sa môže vykonávať ručne alebo pomocou automatizovaných prostriedkov, ako sú počítače a softvérové programy. Pri zverejňovaní osobných

⁹ Rozsudok Súdneho dvora Európskej únie zo 6. novembra 2003 vo veci C-101/01, Bodil Lindqvist, bod 47.

¹⁰ Rozsudok Súdneho dvora Európskej únie z 11. decembra 2014 vo veci C-212/13, František Ryneš/Úrad pro ochranu osobních údajů, bod 33.

¹¹ Bližšie pozri § 16 ods. 2 zákona o ochrane osobných údajov.

údajov na internete pôjde najmä o spracovateľskú operáciu „*poskytovanie prenosom, či šírením*“. Preto je dôležité pri zverejňovaní akýchkoľvek osobných údajov na internete (a to vrátane fotografií a videí) skúmať, či na takéto konanie existuje právny základ uvedený v nariadení GDPR a v zákone o ochrane osobných údajov.

Zákonné možnosti zverejňovania osobných údajov na internete

Nariadenie GDPR ustanovuje vo svojom čl. 6 podmienky, z ktorých musí byť splnená minimálne jedna, aby sa mohlo spracúvanie osobných údajov považovať za zákonné. V rovnakom rozsahu zákon o ochrane osobných údajov stanovuje vo svojom § 13 ods. 1 šesť dôvodov zakladajúcich zákonnosť spracúvania osobných údajov:

- a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,
- b) spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
- c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
- d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby,
- e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
- f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

1. Súhlas dotknutej osoby

Ak je zverejňovanie osobných údajov založené na *súhlase dotknutej osoby*, musia byť dodržané podmienky uvedené v čl. 7 nariadenia GDPR a v § 14 zákona o ochrane osobných údajov. Dôležité je, aby bol súhlas vyjadrený slobodne, jasne a zrozumiteľne, aby ho prevádzkovateľ vedel

preukázať, aby ho mohla dotknutá osoba kedykoľvek odvolať a bola o tom informovaná. V prípade, že dotknutá osoba nežije, súhlas môže poskytnúť jej blízka osoba¹². Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.

Súhlas dotknutej osoby zohráva dôležitú úlohu, ale nevylučuje možnosť, ktorá závisí od situácie, že iné právne dôvody by mohli byť vhodnejšie, či už z hľadiska prevádzkovateľa údajov, alebo dotknutej osoby. Ak sa správne používa, súhlas predstavuje nástroj, ktorý dotknutej osobe poskytuje kontrolu nad spracovaním jej údajov. Ak sa používa nesprávne, kontrola dotknutej osoby je zdanlivá a súhlas predstavuje nevhodný základ na spracovanie.¹³

Pracovná skupina na ochranu údajov vo svojich stanoviskách 15/2011 k definícii súhlasu a 06/2014 k pojmu legitímne záujmy prevádzkovateľa zastala názor, že jednoznačný súhlas vyžaduje použitie mechanizmov, ktoré nezanechávajú žiadne pochybnosti o úmysle dotknutej osoby prejavíť súhlas. Zároveň by sa malo ujasniť, že použitie vopred nastavených možností, ktoré musí dotknutá osoba zmeniť, ak chce spracovanie odmietnuť (súhlas založený na mlčaní), samo osebe nepredstavuje jednoznačný súhlas. Platí to osobitne v prostredí online. Tiež sa požaduje, aby prevádzkovatelia údajov zaviedli mechanizmy na preukázanie súhlasu (v rámci všeobecnej povinnosti zodpovednosti) a zákonodarca by mal doplniť výslovnú požiadavku, pokiaľ ide o kvalitu a dostupnosť informácií, ktoré tvoria základ súhlasu.

Forma takéhoto súhlasu však nie je stanovená. Za určitých okolností sa za súhlas so spracúvaním osobných údajov môže považovať aj **konkludentný súhlas**. Ide o súhlas, ktorý sa poskytuje nevýslovným spôsobom - teda bez potreby jeho písomného alebo ústneho vyjadrenia. Namiesto toho sa konkludentný súhlas poskytuje určitou činnosťou, ktorá naznačuje, že osoba súhlasí so spracúvaním jej osobných údajov – napr. vstupom do priestoru označeného informáciami o spracúvaní osobných údajov. Vždy bude záležať od konkrétnej situácie, aká forma súhlasu bude v danom prípade vhodnejšia.

V osobitných prípadoch sa však vyžaduje „**výslovný súhlas**“. Podľa metodického usmernenia Úradu na ochranu osobných údajov SR č. 2/2018 sa tento používa napr. „pri

¹² Blízkou osobou sa rozumie osoba podľa § 116 Občianskeho zákonníka.

¹³ Pracovná skupina na ochranu údajov zriadená podľa článku 29. *Stanovisko 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES*. [online]. [citované 3. mája 2023]. Dostupné na internete: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sk.pdf

spracúvaní osobitnej kategórie osobných údajov, alebo v prípade súhlasu so spracúvaním rodného čísla (za predpokladu, že súhlas je vhodným právnym základom spracúvania rodného čísla), ktorý musí byť výslovný. Z právneho hľadiska sa výslovným súhlasom rozumie vyjadrený súhlas. Každý súhlas so spracúvaním musí byť slobodný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia; alebo jednoznačného potvrdzujúceho úkonu (napr. nahratie fotografie na webové rozhranie dotknutou osobu), vyjadruje súhlas so spracúvaním osobných údajov, čo už ale za výslovný súhlas nemožno považovať.“¹⁴

2. Spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby

V tomto prípade musí byť zverejňovanie osobných údajov, rozsah a podmienky stanovený priamo v zmluve uzatvorenej medzi prevádzkovateľom a dotknutou osobou. Typické príklady zmlúv, pri ktorých môže dôjsť k spracúvaniu osobných údajov, sú zmluvy o poskytovaní služieb, zmluvy o nájme, zmluvy o predaji a pod. Ak sa majú niektoré osobné údaje zo zmluvy zverejniť na internete, musí byť táto skutočnosť v zmluve výslovne uvedená. Môže ísť napríklad o zmluvy o reklamnej spolupráci, ktorá je v súčasnosti veľmi rozšírená práve na sociálnych sieťach. Vo všeobecnosti však nie je bežné, aby zmluvy umožňovali priame zverejnenie osobných údajov na internete. Väčšina zmlúv skôr stanovuje podmienky a spôsoby, akými môžu byť osobné údaje použité na určité účely, avšak ak by išlo o ich zverejnenie na internete, skôr by sa volila forma súhlasu dotknutej osoby, ktorý ale v tomto prípade môže byť súčasťou zmluvy.

3. Spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná

V tomto prípade pôjde o zverejňovanie osobných údajov najmä podľa právnych predpisov alebo medzinárodných zmlúv upravujúcich činnosť verejnej správy. Osobitný zákon musí ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov. Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo

¹⁴ Úrad na ochranu osobných údajov SR. *Metodické usmernenie č. 2/2018*, str. 3. [online]. [citované 3. mája 2023]. Dostupné na internete: https://dataprotection.gov.sk/uouu/sites/default/files/mu_c._2_2018_k_zakonnosti_spracuvania.pdf

zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú.¹⁵ Právnym predpisom, ktorý umožňuje zverejňovať na internete široký okruh osobných údajov, je napríklad zákon č. 162/1995 Z. z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon) v znení neskorších predpisov. Ten vo svojej šiestej časti upravuje verejnosť katastrálneho operátu. V zmysle zásady verejnosti katastra má každý právo do katastrálneho operátu nahliadať a robiť si z neho pre svoju potrebu výpisy, odpisy, náčrty alebo kópie, ak ďalej v zákone nie je ustanovené inak. Na stránke Úradu geodézie, kartografie a katastra Slovenskej republiky je tak možné vyhľadať vlastníkov nehnuteľností a osoby, ktoré majú iné ako vlastnícke práva k nehnuteľnostiam a množstvo ich osobných údajov okrem rodného čísla.

Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov umožňuje spracúvať osobné údaje napríklad aj pri pátraní po osobách. V tomto prípade je dokonca Policajný zbor oprávnený spracúvať aj osobitné kategórie osobných údajov. Policajný zbor pri pátraní po osobách často využíva práve sociálne siete, kde zverejňuje nevyhnutný rozsah osobných údajov osôb v pátraní vrátane ich fotografií.

Na základe osobitných predpisov sa tiež zverejňujú napríklad osobné údaje štatutárnych orgánov vo verejných častiach rôznych registrov verejnej správy (register partnerov verejného sektora, register politických strán a politických hnutí, register mimovládnych neziskových organizácií, register občianskych združení, obchodný register, živnostenský register atď.). V tejto súvislosti je dôležité spomenúť rozsudok Súdneho dvora EÚ z konca minulého roka, ktorý zrušil časť AML smernice¹⁶ hovoriacej o plošnom prístupe verejnosti k údajom v rámci registra konečných užívateľov výhod. V uvedenom rozsudku Súdny dvor EÚ skonštatoval, že „*prístup širokej verejnosti k informáciám o konečných užívateľoch výhod stanovený zmenenou smernicou proti praniu špinavých peňazí predstavuje vážny zásah do základných práv na rešpektovanie súkromného života a na ochranu osobných údajov, ktoré sú zakotvené v článkoch 7 a 8 Charty základných práv Európskej únie (ďalej len „Charta“), nakoľko údaje obsahujú informácie*

¹⁵ § 13 ods. 2 zákona o ochrane osobných údajov.

¹⁶ Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES.

o identifikovaných fyzických osobách, konkrétne o končených užívateľoch výhod podnikateľských subjektov a iných právnych subjektov zaregistrovaných na území členských štátov, prístup kohokoľvek zo širokej verejnosti k týmto údajom má vplyv na základné právo na rešpektovanie súkromného života“ a tiež, že „je pravdepodobné, že umožnia profilovanie určitých osobných identifikačných údajov, stavu majetku dotknutej osoby, ako aj konkrétnych hospodárskych odvetví, krajín a podnikov, do ktorých táto osoba investovala.“¹⁷

4. *spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby*

Ide o právny základ spracúvania osobných údajov, ktorý by mal byť použitý iba vo výnimočných prípadoch, kedy nie je možné použiť žiadny iný právny základ. Do úvahy prichádza použitie tohto právneho základu aj v prípade, ak je spracúvanie nevyhnutné pre humanitárne účely, vrátane monitorovania epidémií a ich šírenia, alebo v humanitárnych núdzových situáciách.¹⁸

5. *Spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi*

Verejný záujem môže byť definovaný rôznymi spôsobmi a môže sa týkať rôznych oblastí, ako napríklad ochrana verejného zdravia, bezpečnosť, životné prostredie, verejné služby, kultúra, umenie a podobne. V každom prípade ide o záujmy, ktoré sú dôležité pre spoločnosť ako celok a záujmy, ktoré by mali byť chránené a zabezpečené štátnymi alebo verejnými orgánmi. Môže ísť o monitorovanie verejných priestranstiev s priamym streamovaním na internete, napríklad pre účely informovania o dopravnej situácii.

6. *Spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa*

¹⁷ **Rozsudok Súdneho dvora Európskej únie (veľká komora) v spojenej veci C-37/20 a C-601/20 WM (C-37/20) a Sovim SA (C-601/20) proti Luxembourg Business Registers** z 22. novembra 2022.

¹⁸ Úrad na ochranu osobných údajov SR. *Metodické usmernenie č. 2/2018*, str. 3. [online]. [citované 3. mája 2023]. Dostupné na internete: https://dataprotection.gov.sk/uoou/sites/default/files/mu_c._2_2018_k_zakonnosti_spracuvania.pdf

Oprávnené záujmy sledované prevádzkovateľom alebo treťou stranou môžu byť právne¹⁹, hospodárske alebo nemajetkové záujmy.²⁰ „*Tento právny základ je využívaný najmä v prípadoch, kedy nie je z objektívnych príčin možné zabezpečiť súhlasy dotknutých osôb pre vyhotovovanie a následné prípadné zverejňovanie fotografií, a to s ohľadom napríklad na nemožnosť vopred identifikovať účastníkov akcie, ale najmä veľký, nelimitovaný počet účastníkov akcie, či podmienky konania podujatia.*“²¹ Pre uplatnenie inštitútu oprávneného záujmu sa vyžaduje vykonanie **testu proporcionality** ešte pred začatím spracúvania osobných údajov. Test proporcionality pozostáva z troch krokov:

1. **Identifikovať oprávnený záujem** – t. j. musí existovať primerané očakávanie dotknutých osôb, že prevádzkovateľ bude spracúvať ich osobné údaje za konkrétnym účelom. V rámci tohto kroku je potrebné stanoviť, či objektívne dotknutá osoba mohla primerane očakávať a dospieť k záveru, že bude v tejto konkrétnej situácii predmetom monitorovania.
2. **Vykonať test nevyhnutnosti** – t. j. bude potrebné zodpovedať otázky, či by sa dal cieľ spracúvania osobných údajov dosiahnuť aj inak, inými spôsobmi, či sa pri ňom bude vykonávať automatické rozhodovanie a profilácia a pod.
3. **Vykonať porovnávací test** – t. j. či nad oprávneným záujmom prevádzkovateľa neprevažujú základné práva a slobody dotknutej osoby – napr. či nejde o spracúvanie osobitných kategórií osobných údajov, aký je vzťah prevádzkovateľa a dotknutej osoby, aké práva dotknutej osoby môžu byť zasiahnuté a v akom rozsahu, či môžu byť spracúvaním dotknuté aj iné osoby a pod.

Všetky tri podmienky musia byť splnené súčasne. Vyhodnotením testu proporcionality je tak možné dospieť k dvom výsledkom – buď oprávnený záujem existuje, pričom riziká pre práva a slobody dotknutých osôb sú minimálne, alebo by sa osobné údaje nemali spracúvať, pretože riziká pre dotknuté osoby sú zrejme.

¹⁹ **Rozsudok Súdneho dvora Európskej únie** zo 4. mája 2017 vo veci C-13/16, Rīgas satiksme.

²⁰ Pozri WP 217, pracovná skupina zriadená podľa článku 29.

²¹ Právne noviny. *GDPR a fotografie. Aké je odporúčanie Úradu?* [online]. [citované 3. mája 2023]. Dostupné na internete: https://www.pravnenoviny.sk/gdpr-a-fotografie-ake-je-odporucanie-uradu#_ftn4

Osobitné situácie zákonného spracúvania osobných údajov

Nariadenie GDPR aj zákon o ochrane osobných údajov pripúšťajú určité situácie, kedy je možné spracúvať osobné údaje aj napriek tomu, že ani jedna z uvedených podmienok nie je splnená. Napríklad podľa § 78 ods. 2 zákona o ochrane osobných údajov môže prevádzkovateľ spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak „*spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti; to neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.*“ Ide o zákonné ustanovenie, ktoré dáva možnosť novinárom zverejňovať na internete vo svojich článkoch aj osobné údaje. Novinári môžu zverejňovať osobné údaje v určitých prípadoch, ak to súvisí s plnením ich novinárskej práce a je to nevyhnutné pre zabezpečenie slobody tlače a slobody prejavu. Toto právo však nie je neobmedzené a novinári musia dodržiavať zásadu proporcionality a zabezpečiť, aby zverejňovanie bolo nevyhnutné a primerané pre daný účel. Zároveň musia byť dodržané práva a slobody osoby, ktorej sa údaje týkajú, a zabezpečená ochrana jej súkromia a osobnosti.

Ďalšou kategóriou sú údaje, ktoré spracúva zamestnávateľ o svojich zamestnancoch. Tu však treba odlišovať druh osobných údajov a právny základ. Zamestnávateľ spracúva osobné údaje zamestnancov najmä na základe pracovnej zmluvy. Údaje, ktoré môže výslovne zverejniť priamo zo zákona o ochrane osobných údajov (a to aj na internete), sú meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby.²² Avšak, ak by chcel zamestnávateľ zverejňovať fotografie svojich zamestnancov na svojej webovej stránke, musí mať na to ich súhlas.

²² § 78 ods. 3 zákona o ochrane osobných údajov.

Osobitne je upravené aj spracúvanie osobného údaju – rodného čísla. Rodné číslo je jednoznačný identifikátor konkrétnej osoby a jeho zverejňovanie je v zásade zakázané. Zverejniť ju môže iba sama dotknutá osoba.

Záver

Zverejňovanie osobných údajov na internete je spracovateľskou operáciou podľa nariadenia GDPR, aj podľa zákona o ochrane osobných údajov. Pre zverejňovanie takýchto údajov musí existovať **relevantný právny základ**, ktorý musí viesť prevádzkovateľ preukázať.

Aj v prípade zverejňovania videí a fotografií zaobstaraných pôvodne pre čisto súkromné účely, teda pôvodne vyhotovené výlučne k osobnej alebo domácej činnosti, musí existovať právny základ pre takéto zverejňovanie, napr. súhlas dotknutej osoby, nakoľko ich zverejnením neurčitému počtu užívateľov internetu *sa súkromný charakter takejto činnosti stráca*.

Napriek opatrnému prístupu k zverejňovaniu osobných údajov existuje vysoká pravdepodobnosť, že naše údaje nájdeme na niektorých internetových stránkach. Umožňujú to spomenuté právne základy, najmä *zverejňovanie osobných údajov, ktoré je nevyhnutné podľa osobitných predpisov*. Aj v súvislosti so spomenutým rozhodnutím Súdneho dvora EÚ je možné očakávať určitú úpravu právnych predpisov, ktoré upravujú registre, vo verejných častiach ktorých sa objavujú osobné údaje.

Osobitných predpisov, ktoré umožňujú zverejňovať osobné údaje, je veľké množstvo a na základe nich je možné dostať sa k širokému okruhu osobných údajov prakticky kohokoľvek. Otázkou je, *či je takáto právna úprava naozaj nevyhnutná* pre efektívne a transparentné fungovanie verejnej správy alebo je namieste zamyslieť sa nad zmenou slovenskej legislatívy bližšie ku skutočnej ochrane našich osobných údajov.

Zoznam použitej literatúry

BALÁŽIKOVÁ, A. Právo na súkromie v informačnej spoločnosti. In: *Informačné technológie a knižnice*. [online]. [citované 3. mája 2023]. Dostupné na internete: <https://itlib.cvtisr.sk/%c4%8c%3%a1nky/clanek815/>

Dohovor o ochrane ľudských práv a základných slobôd

Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (Dohovor 108)

European Data Protection Board. Usmernenia 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení z 29. januára 2020. [online]. [citované 3. mája 2023]. Dostupné na internete: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_sk.pdf

Rozsudok Súdneho dvora Európskej únie zo 6. novembra 2003 vo veci C-101/01, Bodil Lindqvist, bod 47.

Rozsudok Súdneho dvora Európskej únie z 11. decembra 2014 vo veci C-212/13, František Ryneš/Úrad pro ochranu osobných údajů, bod 33.

Charte základných práv Európskej únie

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

Pracovná skupina na ochranu údajov zriadená podľa článku 29. Stanovisko 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES. [online]. [citované 3. mája 2023]. Dostupné na internete: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sk.pdf

Právne noviny. GDPR a fotografie. *Aké je odporúčanie Úradu?* [online]. [citované 3. mája 2023]. Dostupné na internete: https://www.pravnenoviny.sk/gdpr-a-fotografie-ake-je-odporucanie-uradu#_ftn4

Rozsudok Súdneho dvora Európskej únie (veľká komora) v spojenej veci C-37/20 a C-601/20 WM (C-37/20) a Sovim SA (C-601/20) proti Luxembourg Business Registers z 22. novembra 2022.

Rozsudok Súdneho dvora Európskej únie zo 4. mája 2017 vo veci C-13/16, Rīgas satiksme.

Úrad na ochranu osobných údajov SR. Metodické usmernenie č. 2/2018, str. 3. [online]. [citované 3. mája 2023]. Dostupné na internete: https://dataprotection.gov.sk/uouu/sites/default/files/mu_c._2_2018_k_zakonnosti_spracuvania.pdf

VALENTOVÁ, T., BIRNSTEIN, M., GOLAIS, J. *GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov*. Bratislava: Wolters Kluwer, 2018. ISBN 978-80-8168-852-2.

Všeobecná deklarácia ľudských práv

Zákon č. 162/1995 Z. z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon)

Zákon č. 171/1993 Z. z. o Policajnom zbore

Zákon č. 18/2018 Z. z. o ochrane osobných údajov

Kontaktné údaje

doc. JUDr. Miriam Odlerová, PhD.

Akadémia Policajného zboru v Bratislave

Katedra správneho práva

E-mail: miriam.odlerova@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. RNDr. Tatiana Hajdúková, PhD.

Otvorený internet a Darkweb ako zdroje detskej pornografie

Tomáš Peták

Abstrakt

V súčasnosti, keď nám internet poskytuje neobmedzené možnosti je veľmi jednoduché páchať protiprávnu činnosť. Sociálne siete sú plne sexuálnych predátorov, ktorí len striehnu na svoju obeť, ktorú sa im pod rúškom anonymity často podarí chytiť. Šírenie, prechovávanie a výroba detskej pornografie je celospoločenský problém pred ktorým nie je možné prižmúriť oči, pretože ochrana detí je povinnosť spoločnosti. Deep web, odvrátená strana internetu, je miesto, ktoré poskytuje týmto skupinám ľudí tzv. „útočisko“, kde sa im darí anonymne páchať túto trestnú činnosť. Aj preto sa v príspevok zaoberá problematikou darkwebu a protiprávnej trestnej činnosti, ako hrozby pre súčasnú spoločnosť.

Kľúčové slová

internet, Darknet, Deep web, Dark web, protiprávna činnosť, detská pornografia, sexuálne zneužívanie detí

Abstract

Currently, when the Internet provides us with unlimited possibilities, it is very easy to commit illegal activities. Social networks are full of sexual predators, who are just looking for their victim, who they often manage to catch under the cover of anonymity. The spread, storage and production of child pornography is a societal problem that cannot be ignored, because the protection of children is essential for society. The deep web, the other side of the Internet, is a place that provides these groups of people with so-called a "sanctuary" where they manage to commit this criminal activity anonymously. That is also why the article addresses the issue of the dark web and illegal criminal activity as a threat to contemporary society.

Keywords

Internet, Darknet, Deep web, Dark web, illegal activity, child pornography, sexual abuse of children

Úvod

Internet je fenomén, ktorý v posledných desaťročiach zmenil spôsob, akým ľudia komunikujú, získavajú informácie a vykonávajú obchody. V posledných rokoch vznikli rôzne fóra a sociálne siete, na ktorých, pod rúškom anonymity, vystupuje veľké množstvo ľudí. Tí medzi sebou komunikujú, spájajú sa a navzájom si vymieňajú informácie. Internet sa tiež stal mocným nástrojom na zisk finančných prostriedkov. Jednoducho, zmenil svet. A to nielen k lepšiemu. Pod rúškom anonymity poskytol možnosť určitým jedincom alebo skupinám osôb páchať globálne trestnú činnosť.

Odhaduje sa, že bežne dohľadateľná časť internetu tvorí približne iba 4% celkovej veľkosti internetu. Naopak zvyšných 96% predstavuje Deep web.

Vymedzenie pojmov

Pojmy ako Darknet, Deep web alebo Dark web, ktoré sú vnímané ako miesto nelegálnych činností, často krát však nebývajú správne používané. Často sa zamieňajú a to mnohokrát aj na webových stránkach zaoberajúcich sa internetovými technológiami. Na začiatku definujeme niektoré pojmy, aby sme jednoznačne určili ich význam. Ako už bolo spomenuté, niektoré pojmy sú všeobecne vnímané aj následne vykladané mylne a nepríhodne, a mnohokrát sú rôzne pojmy z tejto oblasti zamieňané. K jedným z najčastejšie zamieňaných pojmov patrí Dark web a Deep web, ktoré sú tiež niekedy pomenované ako Darknet a Deepnet.

Termín Darknet vo všeobecnom zmysle označuje súbor webových stránok, ktoré sú viditeľné pre verejnosť, ale zároveň majú skrytú IP adresu servera, na ktorom sú hostované. Takéto stránky sú verejne dostupné všetkým používateľom webu, ale je veľmi ťažké zistiť, kto je ich administrátorom. Za zmienku tiež stojí, že nie je možné sa na také stránky dostať pomocou obľúbených vyhľadávačov. Darknet je v podstate súkromná sieť, v ktorej sú spojenia nadväzované iba medzi dôveryhodnými peermi, niekedy označovanými ako „priatelia“, a najčastejšie pomocou neštandardných protokolov a portov. Darknet sa líši od ostatných distribuovaných peer to-peer sietí, pretože zdieľanie súborov je anonymné (kvôli tomu, že IP adresy zdrojov nie sú verejne dostupné), a preto môžu používatelia komunikovať bez veľkého strachu a vládnych zásahov. Vzhľadom na uvedené je temný web často vnímaný ako nástroj na komunikáciu v zakázaných komunitách, undergroundu, a aj pre vykonávanie nelegálnych aktivít. Všeobecnejšie možno termín „Darknet“ použiť na popis nekomerčných „uzlov“ internetu, alebo sa vzťahuje na všetky „podzemné“ internetové komunikácie, ktoré sú väčšinou spojené s nelegálnou činnosťou alebo nesúhlasom.

Na zobrazenie a vyhľadanie je potrebný špeciálny softvér, akým je napríklad prehliadač Tor. Internetové stránky na Dark webe sú väčšinou zaheslované a obsahujú väčšinou ilegálny obsah, ktorý by bol na bežnom internete klasickými vyhľadávačmi ako Google automaticky cenzurovaný alebo zmazaný. Aj preto sa Dark web stáva miestom, kde dochádza k širokému spektru nelegálnych aktivít - od nelegálneho šírenia softvéru, cez predaj zbraní, drog, falošných dokladov, až po ponúkanie nájomných vražd, terorizmu, detskej pornografie a iných zločinov.

Deep web (Deepnet)

Slová Deep web a Dark web patria k najčastejšie zamieňaným výrazom, najmä v oblastiach mimo spomínaného odboru, a často sú tieto výrazy považované za zhodné, hoci ich významy zhodné nie sú. Čiastočnou charakteristikou slova Deep web je to, že ide o tú časť siete internet, ktorá je inverzná voči bežnému internetu (Surface webu). Ako Deep web je nazvaná časť World Wide Webu, ktorá nie je priamo dostupná a nie je teda v internetových vyhľadávačoch indexovaná. Veľakrát to sú portály dostupné prostredníctvom prihlasovacích údajov či určitou IP adresou. Pod pojem Deep web spadajú napríklad textové stránky, databázy, súbory a mnohé ďalšie informácie, ktoré nie je možné vyhľadať pomocou klasických, verejne známych vyhľadávačov. Niektoré zdroje uvádzajú, že Deep web zaberá deväťdesiatšesť percent veľkosti celého World Wide Webu, je teda oveľa obsiahlejší ako Surface web (bežný internet), ktorý zaujíma zvyšok celkového obsahu, teda iba štyri percentá¹.

Dark web (Darknet)

Dark web je segmentom Deep webu. Pre tento segment sú využívané špeciálne šifrované protokoly a pre pripojenie k Darknetu je potrebné použiť špeciálne programy, teda Dark webových prehliadačov, zrejme najvýznamnejším je Tor. Ten sa na základe svojej veľkosti, ktorá má v súčasnej dobe dva a pol milióna užívateľov, stal takmer synonymom pojmu Darknet. Ďalším významným Darknetom je napríklad Freenet a I2P. Obsahom siete Tor, ktorá je prístupná prostredníctvom špecializovaného prehliadača, sú neindexované služby onion. Služby Onion sú teda často označované ako Darknet².

Sexuálne a násilne orientovaný obsah

Osem terabajtov predstavuje enormné množstvo dát. Pre predstavu, o aké obrovské množstvo sa jedná, možno uviesť príklad s publikáciou s veľkosťou 207 strán, ktorá by sa do tohto množstva vošla presne desať miliónkrát. Pokiaľ by sme toto dátové množstvo previedli na videozáznam, vyšli by nám dva mesiace nepretržitého záznamu. Presne také množstvo dát detského

¹ ZAVRŠŇNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017, 135 s. Právní monografie. ISBN 978-80-7552-758-5.

² Eddy, 2011, in O'NEILL, Patrick. Back in booming Lolita City: the online child pornography community is thriving. Wayback Machine [online]. [cit. 2023-03-08].

porna zachytili britskí policajti na Dark webe v marci roku 2018. V spálni dvadsaťtriročného Kórejčana Jong Woo Sona, prevádzkovateľa serveru Welcome to Video, bolo nájdených 250 tisíc videozáznamov, ktorých obsahom bola detská pornografia.³ Bohužiaľ aj toto je Dark web. Najčastejšie sa o detskej pornografii na Dark webe ľudia dozvedajú cez správy, avšak až potom, čo dôjde k zatýkaniu. Nakladanie s detskou pornografiou predstavuje nemalú časť Dark webu, na ktorý by aj väčšina jeho priaznivcov najradšej zabudla. Pritom sa jedná o jednu z jeho najväčších častí. O aké veľké množstvo detskej pornografie sa jedná? Jednou vetou by sa dalo povedať, že na Dark webe je možné naraziť na bizarné množstvo detského porno materiálu.

Welcome to Video

Ide o server, ktorého prevádzkovateľ bol Jong Woo Son. Obsah servera bol striktne zameraný na detskú pornografiu. Stránka na seba cez Dark web zarábala prostredníctvom platieb v bitcoinoch. Používatelia týchto stránok museli pred vzhliadnutím zaplatiť, a to v kreditoch. Tieto kredity bolo možné získať dvoma spôsobmi. Prvou možnosťou, ako si tieto kredity obstarat', bola ich kúpa za bitcoiny. Druhú možnosťou bolo nahranie videa s detskou pornografiou. Na tomto princípe funguje aj mnoho stránok na surface webe. Jedná sa o účinný spôsob, ako motivovať používateľov videa nielen na pasívne sťahovanie, ale aj na podieľanie sa na ich distribúcii a tvorbe. Sone skončil za mrežami spolu s ďalšími 337 užívateľ, ktoré sa podarilo dopadnúť. Medzi nimi sa podľa vyjadrenie úradov nachádzal aj občan Českej republiky⁴.

Lolita City

Samotný názov tejto webovej stránky predikuje jej obsah, orientujúci sa na detskú pornografiu. Toto miesto bolo elektronickým rajom pre všetkých pedofilov. V roku 2011 tu bolo na získanie 100 GB pornografického materiálu. V ponuke webu možno nájsť pornografické videá, softcore aj hardcore fotografie. Vekové kategórie detí sa pohybujú od novorodencov po 17-ročné dievčatá a chlapcov. Prístup k tomuto webu je možný iba cez sieť TOR. Na webe je možné nájsť

³ U.S. Department of Justice - South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin [online].

⁴ BURDOVÁ, Eva a Jan TRAXLER. Bezpečně na internetu. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

aj takzvané Lolita City's forums. Rovnako ako na mnohých ďalších pedofilných fórach aj tu sú horlivé debaty ohľadom utlačania pedofilov, ktorí sa považujú za diskriminovanú menšinu⁵.

Childs Play

Bola doposiaľ najrozsiahlejšia webová stránka s detskou pornografiou na Dark webe. Tvrdenie má pôvod v počte registrovaných profilov. Stránka bola v prevádzke celkom jedenásť mesiacov a jej prevádzkovateľom bola austrálska policajná jednotka Taskos Argos. Polícia zverejšovala fotografie, na ktorých boli deti zneužívané. Vytvorila program, ktorý sťahoval obsah hneď z niekoľkých fór týkajúcich sa zneužívania detí. Cieľom akcie bolo zaistiť užívateľské mená a dáta užívateľov navštevujúcich nimi vytvorenú stránku. Polícia pri zisťovaní dát využívala takzvané hot maps, pomocou ktorých boli schopní určiť, kedy presne používateľ sleduje či zverejšuje nelegálny materiál. Ďalším krokom bola lokalizácia časového pásma a samotného užívateľa. Akcia bola úspešná, avšak popudila značné množstvo ľudí. Ivar Stokkerei, právny poradca Detského fondu OSN (UNICEF) v Nórsku konštatoval, že ide o „jasné porušenie Dohovoru OSN o právach dieťaťa, aj keď zámerom polícia je dlhodobo zabrániť novým trestným činom". Polícia bola osočená, že použila materiál s detskou pornografiou ako návnadu na chytenie pedofilov. Jednotka Argos, ktorá web prevádzkovala, mala za sebou 20 rokov skúseností s vyšetrovaním zneužívania detí. Počas niekoľko rokov sa im podarilo zničiť celý rad organizovaných skupín. V jednom takom prípade postupovali podobne. Na pol roka sa policajti stali správcami fóra s názvom The Love Zone na Dark Webe, a keď sa rozhodli prejsť do útoku, zachránili počas jedinej akcie 85 zneužívaných detí. Tiež sa im podarilo zatknúť Brita menom Richard Huckle, ktorý je dodnes považovaný za jedného z 37 najobávanejších pedofilov všetkých čias. Pri zatknutí bol nájdený podrobný zoznam 191 znásilnení, nechýbal ani najdetailnejší rozbor toho, akým spôsobom hrozné akty vykonával. Násilník dlhé roky útočil na deti v Malajzii, podľa všetkého ich mohli byť až stovky. Polícia ho dokázala usvedčiť iba z 22 činov, ku ktorým mala dôkazový video materiál. O ďalších súboroch sa vie, polícia sa k nim však bohužiaľ nedokázala dostať.

Treba podotknúť, že zneužívanie dvadsiatich dvoch detí na odsúdenie stačilo. Huckle za tieto činy dostal dvadsaťdva doživotí, jeho trest však netrval dlho. Spoluväzni vzali čoskoro

⁵ Eddy, 2011, in O'NEILL, Patrick. Back in booming Lolita City: the online child pornography community is thriving. Wayback Machine [online]

takpovediac spravodlivosť do vlastných rúk a Huckle bol nájdený v októbri 2019 vo svojej cele uškrtený a ubodaný na smrť. Richard Huckle sa správal tak arogantne, že nebol populárny ani medzi sebe podobnými. Došiel dokonca tak ďaleko, že vydal šesťdesiatstranovú knihu s názvom „Pedofili a chudoba: Sprievodca milovníka detí“. Knihu však našťastie nikdy nestihol na internet nahrat⁶.

Pink Meth

Bola jedna z najnavštevovanejších webových stránok na Dark webe. Obsah webu tvoria pornografické fotografie či videá maloletých dievčat, tie boli na stránku vložené bez ich vedomia, obvykle po rozchode s priateľom. Webová stránka bola vytvorená jedincem známym pod pseudonymom Olaudah Equiano. Na Pink Meth sa bolo možné dostať cez prehliadač TOR. V súčasnosti už nie je možnosť stránku navštevovať ani nájsť, pretože bola zrušená políciou na základe obžaloby študentky, ktorej fotografia na tento web unikla⁷.

Peddo Support Comunity

Ide zrejme o jednu z najväčších komúní pre pedofilov, na ktorú možno na Dark webe naraziť. Toto fórum obsahuje viac ako tisíce príspevkov s pedofilnou tematikou. Užívatelia si tu vymieňajú zážitky, rady a skúsenosti, ako dosiahnuť svoje ciele. Fórum rozdeľuje používateľa do dvoch kategórií. „Konzervatívni“ pedofili sú užívatelia, ktorých záujem o deti pretrváva čisto vo sfére fantazírovania. Zvyšok fóra sa nachádza mimo akejkolvek mysliteľné medze a stoja teda na „nekonzervatívnej“ strane. Autori príspevkov pri svojom profile vyplňajú vekovú a rodovú preferenciu. Užívateľ s prezývkou Midamoto uvádza, že preferuje 3+ dievčatá. Ďalší užívateľ OneLove má preferenciu dievčat vo veku 7 až 12 rokov. Zaujímavosťou je, že na tomto fóre sa nenachádza žiadny fotografický či videomateriál s detskou pornografiou, ba naopak je tu vyložené zakázaný. Fórum sa tak snaží tváriť, že vlastne nerobí nič zlé. Pedofili si tu vytvorili komunitu, v ktorej si medzi sebou radia, ako sa vnútorne vysporiadať s pocitmi, ktoré cítia. Najväčšej pozornosti sa však tešia diskusné príspevky zamerané na rady, ako sa tajne uspokojovať. Užívateľ s prezývkou Pedrobear44 tu napríklad otvoril horlivú debatu na tému, ako úžasné miesto pre pedofilov je

⁶ STROUKAL, Dominik. Dark Web: sex, drogy a bitcoiny. Praha: Grada, 2020, 207 s. ISBN 978-80-271-2934-8

⁷ GILBERT, David. Pink Meth Revenge Porn Darknet Website Shut Down by FBI in Operation Onymous. International Business Times [online]. [cit. 2023-03-08].

aquapark. Fórum bolo už niekoľkokrát uzavreté, ale stále sa obnovuje zo zálohy na iných miestach⁸.

V súčasnosti sú hore uvedené fóra a stránky vyradené z prevádzky.

Ochrana detí

Rodičovské filtre

V aplikáciách rodičovských filtrov rodič môže zablokovať alebo naopak povoliť konkrétne webové stránky. Môže taktiež zakázať prístup na určité typy a skupiny stránok, pričom tieto aplikácie automaticky odfiltruje. Služba tiež vytvára záznam stránok, ktoré deti navštevujú, aké informácie na internete vyhľadávajú a aká je ich činnosť na sociálnych sieťach. Okrem toho rodičovské filtre disponujú funkciou vymedzujúcou čas, ktorý dieťa môže denne stráviť na internete, je možné tiež nastaviť iný počet hodín (minút) pre všedné dni a víkendy. Niektoré rodičovské filtre sú schopné rodičom na e-mailovú adresu zaslať upozornenie v prípade, že sa jeho dieťa pokúsi navštíviť stránku, ktorú rodič uviedol na zoznam tzv. „čiernej listiny“. Avšak ani tieto bezpečnostné nástroje nemôžu na 100% zaručiť, že sa dieťa nestretne s nevhodným obsahom. Denne na internete pribúda nespočetne nových webových stránok, ktoré pod svojim nevinným názvom môžu často skrývať úplne iný obsah, a technológia rodičovských filtrov ich tak nevyhodnotí ako škodlivé. Väčšina detí je IT technológiách zdatnejšia ako ich rodičia. V takomto prípade sa rodič môže obrátiť na odborníkov, ktorí im v rámci softwarovej podpory poradia ako ochrániť svoje deti na internete. Prísne reštriktívne opatrenia bezpečnosť dieťaťa v kybernetickom priestore nezaistí.⁹

Prevencia

Z hľadiska prevencie kriminality možno v súhrne konštatovať, že v prvom rade je potrebné realizovať kroky smerujúce k predchádzaniu trestnej činnosti. Pri zameraní sa na trestný čin sexuálneho zneužívania je potrebné viac verejne hovoriť o nástrahách takéhoto konania, v čom by

⁸ BURDOVÁ, Eva a Jan TRAXLER. Bezpečne na internetu. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

⁹ KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. E-bezpečí [online].

mohli pomôcť hlavne médiá, a to formou filmov, dokumentov, poučných videí atď.¹⁰ Aj Ministerstvo vnútra SR v spolupráci s Europolom vytvorili náučné video pod názvom „Say No!“, ktoré je voľne dostupné na internete (youtube.com), ktoré je inšpirované skutočnými prípadmi a zobrazuje, ako sa môže stať dieťa obetou sexuálneho zneužívania alebo sexuálneho vydierania cez internet. Taktiež existuje viacero príručiek, brožúr, literatúry, ktoré prispievajú k prevencii kriminality. Treba ich však dávať do centra pozornosti napr. formou besied a kurzov pre širokú verejnosť.¹¹

Komunikácia s dieťaťom

Dieťa bude skôr či neskôr túžiť opatrenia prekonať či obísť, a to napríklad využívaním zariadenia mimo dosahu rodiča, napríklad počítače v knižnici, v škole či u kamaráta. Je teda oveľa dôležitejšie, aby sa rodič zameral predovšetkým na vybudovanie zdravého vzťahu s dieťaťom, ktorý je postavený na vzájomnej dôvere a podpore. Pokiaľ bude mať dieťa k rodičovi dôveru, nebude sa báť zverovať aj v krízových situáciách¹². Sexuálne obťažovanie si vyžaduje časový priestor, málokedy sa realizuje krátkom čase. Páchatelia komunikujú s potenciálnou obeťou väčšinou dlhšie a k stretnutiu príde až po dlhodobej príprave.¹³

Akonáhle rodič zistí čokoľvek nevhodné alebo sa mu dieťa zverí so zhladnutím závadného obsahu, nadviazaním kontaktu s vulgárnym človekom či inou rizikovou situáciou, nemal by za žiadnych okolností konať unáhle. Naopak by sa mal snažiť situáciu pochopiť a v pokoji sa o nej s dieťaťom porozprávať.

Dieťa nesmie stratiť v rodičovi dôveru, je dôležité, aby sa nabudúce nebálo opäť s problémom zveriť¹⁴.

¹⁰ PROKEINOVÁ, M., LACIAK, O. Sexuálne zneužívanie detí a zverených osôb a trestnoprávna ochrana obetí trestných činov. Bratislava : Wolters Kluwer SR, 2021, s. 35 (2 cit.). ISBN 978-80-571-0350-9.

¹¹ BACIGÁL Ivan a HAJDÚKOVÁ Tatiana, Preverovanie a vyšetrovanie sexuálneho zneužívania detí on-line v praxi, zborník príspevkov zo 4. medzinárodnej konferencie "Řešení elektronického násilí a kyberkriminality" konanej v dňoch 9. 10. - 10. 10. 2014 v Jihlave. - ISSN 2336-3657. - Roč. 1, zvláštne vydanie (2014), [online].

¹² KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. E-bezpečí [online].

¹³ Tatiana HAJDÚKOVÁ a Ivan BACIGÁL. Hrozby kybernetického priestoru pre deti v období dospievania In: Policajná teória a prax = Police Theory and Practice : časopis Akadémie PZ v Bratislave. - ISSN 1335-1370. - Roč. 22, č. 3 (2014), s. 5-19.

¹⁴ BURDOVÁ, Eva a Jan TRAXLER. Bezpečně na internetu. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

Záver

Existencia Dark webu je pre mnohých stále veľká neznáma. Nejednen užívateľ bežného internetu nemá ani zdanie, že práve vstúpil do priestoru, ktorý je iba ostrovčekom v oceáne kybernetického priestoru. Dark web a internet koexistujú v jednom spoločnom priestore, avšak sú oddelené pomyselnou bariérou, ktorú možno znepokojivo ľahko prekonať. Užívatelia tejto siete si mnohokrát neuvedomujú riziká, ktoré návšteva tohto webu obnáša. A riadiť sa pravidlom, čo sa stane na Dark webe, zostane na Dark webe, je pochabosť, ktorú môže používateľ neskôr horko ľutovať. Hoci sa jedná o anonymný priestor, je možné sa bez patričnej ochrany a vyhýbania sa určitým typom webových stránok dostať do nemalých problémov. Pokiaľ ide o bezpečnosť v reálnom svete, sme často prehnane paranoidní a svoje súkromie si strážime za vysokými plotmi. Avšak pokiaľ sa ocitáme vo virtuálnom svete, nezdráhame sa o sebe a svojich blízkych zverejňovať citlivé informácie, ba dokonca aj polohu, kde sa práve nachádzame alebo kam sa chystáme.

Zoznam použitej literatúry

- BACIGÁL Ivan a HAJDÚKOVÁ Tatiana, Preverovanie a vyšetrovanie sexuálneho zneužívania detí on-line v praxi, zborník príspevkov zo 4. medzinárodnej konferencie "Řešení elektronického násilí a kyberkriminality" konanej v dňoch 9. 10. - 10. 10. 2014 v Jihlave. - ISSN 2336-3657. - Roč. 1, zvláštne vydanie (2014), [online].
- BURDOVÁ, Eva a Jan TRAXLER. Bezpečně na internetu. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.
- Edddy, 2011, in O'NEILL, Patrick. Back in booming Lolita City: the online child pornography community is thriving. Wayback Machine [online].
- GILBERT, David. Pink Meth Revenge Porn Darknet Website Shut Down by FBI in Operation Onymous. International Business Times [online].
- HAJDÚKOVÁ Tatiana a Ivan BACIGÁL. Hrozby kybernetického priestoru pre deti v období dospievania, In: Policajná teória a prax = Police Theory and Practice : časopis Akadémie PZ v Bratislave. - ISSN 1335-1370. - Roč. 22, č. 3 (2014).
- KOPECKÝ, Kamil. Méně než polovina rodičů pravidelně kontroluje, co dělají jejich děti na internetu. E-bezpečí [online].

PROKEINOVÁ, M., LACIAK, O. 2021. Sexuálne zneužívanie detí a zverených osôb a trestnoprávna ochrana obetí trestných činov. Bratislava : Wolters Kluwer SR, 2021, s. 35 ISBN 978-80-571-0350-9.

STROUKAL, Dominik. Dark Web: sex, drogy a bitcoiny. Praha: Grada, 2020, 207 s. ISBN 978-80-271-2934-8.

ZAVRŠŇNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017, 135 s. Právní monografie. ISBN 978-80-7552-758-5.

Kontaktné údaje

Ing. Tomáš Peták

Katedra informatiky a manažmentu

Akadémia Policajného zboru v Bratislave Sklabinská 1, 835 17 Bratislava

E-mail: tomas.petak@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Identifikácia a boj proti dezinformáciám a falošným správam

Peter Poláček

Abstrakt

Prejavy nenávisti na sociálnych sieťach či internete sa stávajú čoraz častejšie súčasťou našich životov. Dezinformácie či falošné správy označované tiež ako fake news spôsobujú polarizáciu spoločnosti, ktorá sa aj udalosťami posledných dní začala stupňovať. Ozbrojený konflikt medzi Ruskom a Ukrajinou je hlavnou témou posledných dní avšak spoločnosť rozdeľovali predtým ďalšie témy ako obranná dohoda s USA či pandémie koronavírusu. Aj vďaka týmto udalostiam je veľmi jednoduché spadnúť do priepasti nenávisti v online priestore, ktorú spôsobujú falošné správy a dezinformácie. Tento článok sa najprv zaoberá touto definičnou výzvou a klasifikuje druhy falošných správ a dezinformácií na základe dvoch premenných: motivácie ich tvorcov a zámeru klamať. V druhej kapitole sú navrhnuté riešenia a možnosti boja proti falošným správam a dezinformáciám.

Kľúčové slová:

dezinformácie, falošné správy, kritické myslenie, mediálna výchova

Abstact

Expressions of hatred on social networks or the Internet are increasingly becoming a part of our lives. Hoaxes or fake news cause polarization of society, which has also started to escalate with the events of the last few days. The armed conflict between Russia and Ukraine is the number one topic of recent days. However, before that, society was divided by other topics such as the defense agreement with the USA or the coronavirus pandemic. Also thanks to these events, it is very easy to fall into the abyss of hatred in the online space caused by misinformation and hoaxes. This article first addresses this definitional challenge and classifies the types of fake news and disinformation based on two variables: the motivation of their creators and the intent to deceive. Next, the Article identifies solutions and options for combating fake news and disinformation.

Keywords:

fake news, misinformation, critical thinking,

Úvod

Falošné správy predstavujú komplexnú výzvu pre reguláciu v čoraz viac demokratizovanom a sprostredkovanom on-line informačnom ekosystéme. Nepravdivé informácie ľahko vytvárajú aktéri s rôznymi cieľmi, rýchlo ich šíria platformy motivované skôr finančnými stimulmi ako novinárskymi normami alebo verejným záujmom a dychtivo ich konzumujú používatelia, ktorí chcú posilniť existujúce presvedčenia. Napriek tomu, že po pandémie koronavírusu rástlo povedomie o tomto probléme, význam pojmu „falošné správy“ je čoraz

spornejší a rozšírenejší. V rebríčkoch dôvery v rôzne konšpirácie, hoaxy či falošné správy ako krajina vedieme. Aby sme im mohli čeliť, potrebujeme podľa odborníkov mediálnu výchovu, kritické myslenie a digitálne zručnosti.

Dezinformátori mávajú často rôzne motívy na vytváranie nepravdivého obsahu a užívatelia falošných správ majú obmedzené stimuly investovať do spochybňovania alebo overovania ich obsahu, najmä keď obsah posilňuje ich existujúce presvedčenie. Napokon, falošné správy sa objavujú len zriedka samostatne, pričom sa často miešajú s presnejšími príbehmi, takže je to o to ťažšie ich kategoricky odmietnuť.

1. Typológia falošných správ

Táto kapitola poskytuje nový spôsob organizovania rôznych typov falošných správ podľa ich charakteristických vlastností. Rozlišujeme dve definujúce charakteristiky používané na identifikáciu druhov falošných správ:

- autor má v úmysle oklamať čitateľov
- finančná motivácia na vytvorenie alebo šírenie falošných správ

Tabuľka1. Typológia falošných správ

		Zámer	
		Klamlivý	Neklamlivý
Finančná motivácia	Peňažná	Hoaxy	Satira
	Nepeňažná	Propaganda, Trolling	Komentáre, zábava

Zdroj: Mark Verstraete, Jane R. Bambauer,

Tieto rozdiely sú užitočné z niekoľkých dôvodov. Izolácia zámeru klamať poskytuje spôsob ako určiť morálne hranice medzi zámermi a motiváciou. Odhalenie človeka resp. motivácie subjektu na vytváranie alebo šírenie falošných správ môže pomôcť k zníženiu stimulov pre ich vytváranie a odradiť ich od týchto činností.

1.1 Dezinformácie a falošné správy

Falošné správy (anglický ekvivalent: fake news) sú informácie, ktoré zámerne napodobňujú formát spravodajstva alebo iného produktu žurnalistiky, pričom ich tvorcovia úmyselne zavádzajú svoje publikum skresľovaním reality.¹

Dezinformácie sú akékoľvek nepravdivé informácie, ktoré majú za úlohu ľudí oklamať, poškodiť, alebo im nejakým spôsobom ublížiť. Môže ísť o nepravdivú informáciu v podobe textu, videa, grafiky alebo zvuku.²

Za hlavné techniky dezinformácie sú považované:

1. zveličenie javu;
2. zmena jeho povahy alebo okolností;
3. úplná zmena javu na iný.

Podmienky úspešnosti dezinformácie sú nasledovné:

1. dezinformácie vychádzajú z pravdivých zdrojov resp. prameňov;
2. musia byť prispôbené kultúrnemu kontextu protivníka – čiže musia byť uvádzané jasne a zrozumiteľne, aby prijímateľ porozumel danej dezinformácii;
3. musia byť šírené viacerými kanálmi – napr. televízia, noviny, rádio.³

Organizácia GLOBSEC pravidelne zverejňuje prieskumy, kde sa podľa posledných zistilo, že konšpiračným teóriám verí až 56% ľudí. Čo sa týka tohto faktu, Slovensko je na tom naozaj zle, keď si porovnáme napríklad Litovčanov a Rakúšanov, ktorí sú náchylní len na 17% (Litovčania) a 20% (Rakúšania).⁴

„Dezinformáciami nemusia byť iba vyložené výmysly. Ide vo všeobecnosti o prípady, keď sa niekto úmyselne snaží držať ľudí v mylnej predstave. Techniky, ako to dosiahnuť, bývajú rôzne. Môže ísť o manipulovanie faktami, spájanie nesúvisiacich udalostí, šírenie fotiek s nepravdivou legendou, podsúvanie nepravdivých výrokov a pod.“⁵

¹ Krátky slovník hybridných hrozieb Národného bezpečnostného úradu [online] <https://www.nbu.gov.sk/kyberneticka-bezpecnost/nbac-slovnik-hybridne-hrozby/index.html>

² Yar, L. 2019. Falošné správy a dezinformácie: Terminológia, nástroje a výzvy. Dostupné na internete: <https://euractiv.sk/section/digitalizacia/news/falosne-spravy-a-dezinformacie-terminologia-nastroje-a-vyzvy/>

³ VYCHOVA. 2010. Dezinformácia. Dostupné na internete: <https://medialnavychova.sk/dezinformacia/>

⁴ GLOBSEC Trends 2022: Väčšina ľudí na Slovensku stále verí konšpiráciám a cíti sa ohrozené. Dostupné na internete: <https://www.globsec.org/what-we-do/press-releases/globsec-trends-2022-vacsina-ludi-na-slovensku-stale-veri-konspiraciam>

⁵ ŠNIDL, V. 2017. Pravda a lož na Facebooku. Bratislava : N Press, s.r.o., 2017.

Dezinformácie sú nepravdivé alebo zavádzajúce informácie vytvorené s cieľom ovplyvniť ľudí. Môžu mať mnoho rôznych podôb a existovali už dávno pred internetom. Každá krajina zápasí so šírením dezinformácii online, či už žijete vo fungujúcej demokracii alebo v autoritatívnom režime. Často obklopujú rozdeľujúce politické témy, ako sú migrácia, očkovanie alebo témy týkajúce sa pohlavia, sexuality, rasy, náboženstva a podobne.⁶

Všetky nepravdivé informácie majú potenciál stať sa dezinformáciou alebo inou formou nepravdy. Taktiež, informácia, ktorá je síce pravdivá, ale je zobrazená s čistým cieľom zmanipulovať, môžeme považovať za dezinformáciu.

1.2 Hoax

Hoax pochádza z anglického slova a jeho účelom je najčastejšie vyvolať strach a šíriť falošnú správu alebo radu. Z toho vyplýva ďalší účel, a tým je manipulácia názorov ľudí. Pomocou hoaxu sa dá poškodiť povest' firmy, značky, výrobku, ale aj zdiskreditovať konkrétnu osobu. Hoaxy privolávajú veľa pozornosti, čo je tiež jeden z ich účelov. V poslednom prípade môžeme spomenúť aj schválne šírený hoax nejakou satiristickou stránkou alebo osobou, v ktorom si takto vystrelia z rádových šíriteľov hoaxov a dôverčivých ľudí na sociálnych sieťach.⁷

Ako spoznať hoax?

- Vyzýva ľudí aby správu preposielali ďalej.
- Snaží sa presvedčiť o svojej dôležitosti
- Šokujúce novinky, informácie, nebezpečenstvo, urgentná pomoc
- Dôveryhodné zdroje varujú (FBI varuje, Vedcom uniklo, Microsoft varuje)
- Unikla tajná informácia o ktorej tradičné médiá zámerne mlčia

Výzva k ďalšiemu rozposielaniu je najhlavnejší bod. Pre ľudí čo nevedia rozoznať hoax od pravdivej informácie, je veľmi jednoduché tuto informáciu začať šíriť ďalej, pretože zaberie len pár sekúnd a pár kliknutí a hoax sa stane masovo zdieľaným. A práve vďaka jeho jednoduchosti sa hoaxy stávajú úspešnými.⁸

⁶ PIRKOVA, E. 2021. What is disinformation, why it spreads, and how to stop it. Dostupné na internete: <https://www.accessnow.org/what-is-disinformation-how-to-stop-it/>

⁷ KOHOUT, R. KARCHNÁK, R. 2016. Bezpečnosť v online prostredí. Karlovy Vary: Biblio Karlovy Vary. 2016. Dostupné na internete: <https://www.internetembezpecne.cz/wp-content/uploads/2017/03/Roman-Kohout-Bezpecnost-v-online-prostredi.pdf>

⁸ UNIPO.SK. Hoax (Poplašné správy). Dostupné na internete: <https://www.unipo.sk/9470/>

Motivácia šíriteľov, môže byť rôznorodá. Môže ísť o úsilie o finančný zisk, túžba ublížiť alebo samotný šíriteľ je vnútorne presvedčený o pravdivosti svojho konania. Bohužiaľ, pre ľudí čo sú náchylní veriť dezinformáciám akéhokoľvek typu, neexistuje žiaden všeobecný presný návod, ako okamžite spoznať hoax. V dnešnej dobe veľa ľudí nedokáže používať kritické myslenie a tým pádom informácie aj kriticky hodnotiť, čo vedie k slepému akceptovaniu faktov, ktoré sa na sociálnych sieťach prezentujú s častou poznámkou,, zdieľajte kým to nezmažú"!!!!!!

„Predstava, že niekto náhodou pri surfovaní po internete objaví niečo, čo si vedecké tímy a kapacity „nevšimli“, je dosť zábavná. Tak či tak je logické a sčasti aj pochopiteľné, že je jednoduchšie slepo veriť, než preverovať a zisťovať informácie." ⁹.

1.3 Propaganda

Krátky slovník hybridných hrozieb Národného bezpečnostného úradu definuje propagandu ako aktivitu, zameranú na šírenie určitej myšlienky, zdôrazňujúcu iba jej pozitívne aspekty, šírenú s cieľom presvedčiť publikum o jej správnosti. Má spravidla ideologickú, náboženskú, či politickú konotáciu. Na rozdiel od reklamy či propagácie propaganda nemá komerčný rozmer.

Podľa Moravčíkovej je propaganda je zámerná činnosť jedných ľudí voči druhým, s úmyslom si ich podriadiť. Je špecifickou formou komunikácie a preto sa s propagandou stretávame už od čias ľudstva.¹⁰

„Propaganda je zámerný a systematický pokus stvárať chápajúce, manipulovať zmýšľaním a bezprostredným správaním a s úmyslom dosiahnuť reakcie, ktoré budú zhodné so zámermi propagátora. Propaganda je proces kontroly prietoku informácií, riadenia verejnou mienkou a manipulovania vzormi správania." ¹¹

Hlavným účelom propagandy je:

- Šírenie a prezentovanie informácie určitého druhu. Šírené informácie majú za cieľ ovplyvniť (zmanipulovať) názory a správanie cieľovej skupiny.
- Šíriteľ sa snaží ovplyvniť malú alebo naopak veľkú skupinu ľudí
- Informácie sú vyselektované tak, aby vyhovovali šíriteľovi
- Informácie napádajú hlavne emocionálnu stránku osobnosti príjemcu, nie jeho intelekt.

⁹ MORAVČIKOVÁ, E. 2020. Mediálna kultúra I. Univerzita Konštantína Filozofa v Nitre, Filozofická fakulta, 2020.

¹⁰ MORAVČIKOVÁ, E. 2020. Mediálna kultúra I. Univerzita Konštantína Filozofa v Nitre, Filozofická fakulta, 2020.

¹¹ MORAVČIKOVÁ, E. 2020. Mediálna kultúra I. Univerzita Konštantína Filozofa v Nitre, Filozofická fakulta, 2020, str. 13.

Ciele propagandy sú rôzne, môže ísť o nevinné prezentovanie názoru až po účelový zámer zmanipulovať, poškodiť alebo zahubiť druhú stranu alebo konkurenciu. Propaganda pôsobí dlhodobo a usiluje sa nenápadne alebo otvorene presvedčiť príjemcov o pravde, ktorá môže byť pravdivá alebo nemusí. Za propagandu síce môžeme označiť aj reklamu či lobbying, po druhej svetovej vojne je považovaná skôr v zmysle politickej alebo ideologickej.¹²

Hlavné druhy propagandy:

- Biela: Biela propaganda sa chápe ako propagácia. Obsahuje objektívne, pravdivé informácie z jasných identifikovateľných zdrojov.
- Čierna: Čierna propaganda je presný opak bielej. Používa nepravdivé a nepotvrdené tvrdenia ako polopravdy, fámy či dezinformácie. Vyhýba uvedením zdroja alebo má nepravdivý zdroj
- Šedá: Šedá propaganda je prienikom bielej a čiernej propagandy. Zvyčajne obsahuje objektívnu prezentáciu, ale nie vždy pravdivé informácie. Zdroj nie je ľahko identifikovateľný.

Propaganda teda vo všeobecnosti znamená účelové šírenie informácií či dezinformácií v snahe vyvolať u príjemcov žiaducu reakciu.¹³

1.4 Trolovanie

Trol (anglický ekvivalent troll) je užívateľ internetu, ktorý svojimi komentármi a správaním sa na internete zámerne provokuje ostatných alebo odvádza diskusiu od pôvodnej témy. Opak elfa. Trolovanie (anglický ekvivalent trolling) je akt zámerného urážlivého alebo provokatívneho správania sa v online priestore s cieľom vyprovokovať čitateľov alebo narušiť priebeh diskusie, alebo odpútať pozornosť a záujem smerom k iným, menej podstatným alebo ku kontroverzným témam.¹⁴

Trollovia sú reálne osoby, ktoré v online priestore vytvárajú konflikty a znemožňujú tak priebeh vecnej diskusie častokrát prostredníctvom zdieľania rôznych dezinformácií. Títo trollovia tak polarizujú ostatných diskutujúcich. Populárni sú hlavne v diskusných fórach, alebo na

¹² MORAVČIKOVÁ, E. 2020. Mediálna kultúra I. Univerzita Konštantína Filozofa v Nitre, Filozofická fakulta, 2020.

¹³ KANIČAROVÁ, K. 2021. *Propaganda (DISINFO BASICS)*. Dostupné na internete: <https://infosecurity.sk/dezinfo/propaganda-disinfobasics/>

¹⁴ Krátky slovník hybridných hrozieb Národného bezpečnostného úradu. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>

Facebooku.¹⁵ „Trolling“ predstavuje zaujaté správy alebo informácie s klamlivým obsahom, ktorého autor má za cieľ oklamať čitateľa a je motivovaný pokusom získať osobnú humornú hodnotu.

2. Riešenia a odporúčania pre boj proti dezinformáciám a falošným správam

Medzi hlavné riešenia a odporúčania pre elimináciu šírenia dezinformácií a falošných správ, rovnako ako aj ich rozpoznanie, je oblasť mediálnej výchovy a s ňou spojená mediálna gramotnosť a kritické myslenie.

2.1 Mediálna výchova a mediálna gramotnosť

„Mediálna gramotnosť znamená vlastne rozšírenú informačnú a komunikačnú zručnosť, ktorá zároveň spôsobuje zmenu charakteru informácií v spoločnosti. Nadobudnutie zručností s ňou spojených posilňuje v ľuďoch kritické myslenie, ale zároveň podporuje kreatívne schopnosti, v prostredí stále sa rozširujúceho množstva mediálnych posolstiev používajúcich obraz, slovo a zvuk. Práve z tohto dôvodu možno mediálnu gramotnosť zaradiť medzi najzakladenejšie životné zručnosti pre 21. storočie“.¹⁶

Mediálnu gramotnosť je možné učiť a zlepšovať pomocou mediálnej výchovy. Pri tomto type výchovy sa nemyslí iba na deti a mládež, ale aj na staršie skupiny obyvateľstva. Je to proces celoživotného vzdelávania a „jej cieľom je výchova kritickejších, náročnejších a aktívnejších konzumentov mediálnych obsahov“.¹⁷

„Mediálnu výchovu je možné definovať ako celoživotný, systematický a cieľavedomý proces získavania mediálnych kompetencií a zvyšovania úrovne mediálnej gramotnosti, ktorého hlavným cieľom je podporovať zodpovedné využívanie médií a rozvíjať kritické postoje vo vzťahu k mediálnym obsahom s dôrazom na morálne princípy a humanizmus. Koncepcia vymedzuje základné predpoklady a stratégiu tvorby efektívneho systému mediálnej výchovy v kontexte celoživotného vzdelávania“.¹⁸

¹⁵ HÚSKOVÁ, E. 2020. Súčasný trendy šírenia dezinformácií. Dostupné na internete: <https://stratapol.sk/wp-content/uploads/2021/02/publi-trendy-%C5%A1%C3%ADrenia-dezinform%C3%A1ci%C3%AD2.pdf>

¹⁶ VRABEC, N. 2008. Mládež a média. Mediálna gramotnosť mladších ľudí na Slovensku. Bratislava: Iuventa. 2008. Dostupné na internete: https://www.iuventa.sk/files/documents/7_vyskummladeze/publikacie/media_mlade.pdf

¹⁷ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

¹⁸ MKSR. 2020. Koncepcia mediálnej výchovy v SR. Dostupné na internete: <https://www.culture.gov.sk/uncat/koncepcia-medialnej-vychovy-v-sr/>

„Mediálna výchova je multidisciplinárnou kategóriou, ktorá integruje poznatky širšieho spektra spoločenských vied, je predmetom záujmu tak žurnalistiky, psychológie, sociológie, pedagogiky a v menšom či väčšom rozsahu jej pozornosť venujú vládne aj mimovládne inštitúcie. Význam a opodstatnenosť mediálnej výchovy v spoločnosti rastú priamoúmerne s neustálym vývojom komunikačných technológií, s možnosťami ich využívania a prístupu k nim, ale aj s rôznorodosťou a množstvom ponúkaných mediálnych obsahov, a práve mediálna výchova sa považuje za prostriedok získavania schopností a zručností orientovať sa v mediálnom svete. Pod vplyvom neustáleho vývoja médií a nových komunikačných technológií dochádza v posledných rokoch k dôležitému posunu vo vymedzení cieľových skupín mediálnej výchovy a hranica pôsobenia a záberu mediálnej výchovy sa posúva od detí a mládeže až do dospelosti. Mediálna výchova sa s cieľom vybaviť občanov základnými zručnosťami, znižovať generačné rozdiely a možné riziká sociálneho vylúčenia niektorých špecifických skupín populácie, ktoré nebudú schopné absorbovať zmeny, zaraďuje do referenčného rámca celoživotného vzdelávania“¹⁹.

„Vo svete je mediálna výchova väčšinou integrovaná do povinných predmetov (najmä materinského jazyka), psychológie, dejepisu, sociológie, dejín umenia a pod. Podľa mediálnych odborníkov vysokú úroveň mediálnej výchovy má najmä Kanada, Británia a Austrália. V poslednom desaťročí výrazný úspech v mediálnej gramotnosti zaznamenalo Fínsko“.²⁰

Na Slovensku je mediálna výchova súčasťou už spomínaného celoživotného vzdelávania a jej cieľom sú všetky vekové kategórie.²¹ Znak mediálnej výchovy sú zadefinované nasledovne: „Cieľom mediálnej výchovy ako prierezovej témy je umožniť žiakom, aby si osvojili stratégie kompetentného zaobchádzania s rôznymi druhmi médií a ich produktmi a súčasne rozvinúť u žiakov spôsobilosť – mediálnu kompetenciu, t. j. zmysluplne, kriticky a selektívne využívať médiá a ich produkty, čo znamená, viesť žiakov k tomu, aby lepšie poznali a chápali pravidlá fungovania „mediálneho sveta“, zmysluplne sa v ňom orientovali a selektovane využívali médiá a ich produkty podľa toho, ako kvalitne plnia svoje funkcie, najmä výchovno-vzdelávaciu, vychovať žiakov ako

¹⁹ MKSR. 2020. Koncepcia mediálnej výchovy v SR. Dostupné na internete: <https://www.culture.gov.sk/uncat/koncepcia-medialnej-vychovy-v-sr/>

²⁰ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

²¹ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

občanov schopných vytvoriť si vlastný názor na základe prijímaných informácií, formovať schopnosť detí a mládeže, kriticky posudzovať mediálne šírené posolstvá, objavovať v nich to hodnotné, pozitívne formujúce ich osobnostný a profesijný rast, ale tiež ich schopnosť uvedomovať si negatívne mediálne vplyvy na svoju osobnosť a snažiť sa ich zodpovedným prístupom eliminovať“.²²

Mediálna výchova nie je u nás dôležitou témou, aj keď sa v súčasnej dobe ozývajú hlasy, že by mala byť samostatným voliteľným predmetom vo vyšších ročníkoch na základných školách a vyučovanie by malo pokračovať aj na stredných školách.²³

Dôvody na výučbu tohto predmetu sú nasledovné: „Mladá, dospievajúca generácia je technologicky zdatná. Nemá ale dostatočné vedomosti o tom, ako sa tvoria a upravujú mediálne obsahy, ako fungujú mediálne spoločnosti, kto vlastní médiá, ako dochádza k mediálnym manipuláciám, nedokáže rozlíšiť komerčný obsah od spravodajského obsahu. Veľa stredoškolákov nevie, že máme duálny systém televízneho a rozhlasového vysielania, ktoré médiá sú verejnoprávne a ktoré súkromné. Stredoškoláci nevedia odhaliť mediálne manipulácie a konšpiračné teórie. Žiaci gymnázií (stredných škôl) nepoznajú pravidlá, ktoré má novinár dodržiavať a práva, ktoré si môžu uplatňovať voči médiám, napr. právo na odpoveď, opravu, ochranu osobnosti a pod“.²⁴

Dôvody na výučbu tohto predmetu sú nasledovné: „Mladá, dospievajúca generácia je technologicky zdatná. Nemá ale dostatočné vedomosti o tom, ako sa tvoria a upravujú mediálne obsahy, ako fungujú mediálne spoločnosti, kto vlastní médiá, ako dochádza k mediálnym manipuláciám, nedokáže rozlíšiť komerčný obsah od spravodajského obsahu. Veľa stredoškolákov nevie, že máme duálny systém televízneho a rozhlasového vysielania, ktoré médiá sú verejnoprávne a ktoré súkromné. Stredoškoláci nevedia odhaliť mediálne manipulácie a konšpiračné teórie. Žiaci gymnázií (stredných škôl) nepoznajú pravidlá, ktoré má novinár

²² KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

²³ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

²⁴ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

dodržiavať a práva, ktoré si môžu uplatňovať voči médiám, napr. právo na odpoveď, opravu, ochranu osobnosti a pod“²⁵. Vyššie spomenuté krajiny majú mediálnu výchovu v učebných osnovách už dlho a aj to je jeden z hlavných dôvodov, prečo sú ľudia v daných krajinách odolnejší na vplyv dezinformácií a hoaxov. Dovoľme si trochu poopraviť názor doktorky Koprenovej. Podľa nás by mala byť do výučby materinského jazyka alebo do výučby občianskej výchovy od 7. ročníka základnej školy zakomponovaná mediálna výchova a následne by sa pokračovalo s výučbou na stredných školách. Je nanajvýš zarážajúce, že mladá generácia nevie rozlíšiť mediálnu manipuláciu, konšpiračné teórie, ale aj na prvý pohľad jasné dezinformácie a hoaxy, a to aj s takou technologickou zdatnosťou, ktorú mladá generácia má. Preto si myslíme, že zavedenie mediálnej výchovy a s tým precvičovanie mediálnej gramotnosti, by bolo prvým náznakom toho, že sa s dezinformáciami a ich šíriteľmi dá bojovať.

2.2 Kritické myslenie

Pojem kritické myslenie je veľmi staré, no napriek tomu mnoho odborníkov sa stále nevedia zhodnúť na konkrétnej a presnej definícii. Vo všeobecnosti kritické myslenie znamená schopnosť nepodliehať prvému dojmu.²⁶

Môže ísť o nejaký písaný text alebo video. Snažíme sa zamyslieť nad tým, či to, čo som práve prečítal alebo počul, je pravda alebo nie. Overovanie takýchto tvrdení si overujeme z iných zdrojov alebo z výrokov, ktorý tento istý zdroj použil už v minulosti. Preto je práve kritické myslenie tak dôležité. „Človek sa prostredníctvom kritického myslenia naučí zaobchádzať s informáciami“.²⁷ Dôležitá je aj príprava na diskusiu. Človek musí byť pripravený, musí mať nachystané argumenty, ale mal by vedieť reagovať aj na protiargumenty. Počas takejto prípravy si vlastne stanovujeme otázky, ktorými sa budeme zaoberať, tvoríme hypotézy, zbierame informácie o probléme, narábame s nimi a skúmame daný problém do hĺbky, pričom tvoríme závery. Najdôležitejšie je ale mať nachystaný svoj vlastný názor, mať prichystané argumenty a veriť

²⁵ KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

²⁶ EDUWORLD.SK. Kritické myslenie – povinná výbava každého z nás. [online].

[cit. 13.7.2022] Dostupné na internete: <https://eduworld.sk/cd/jaroslava-konickova/9473/metody-ktore-aktivizuju-ziakov-pri-uceni>

²⁷ BLAZSEKOVÁ, T. 2015. Čo je to kritické myslenie? Dostupné na internete: <https://www.startitup.sk/co-je-to-kriticke-myslenie/>

svojmu názoru²⁸. Dôležitou vlastnosťou je tiež prijímanie argumentov s pokorou. Je dôležité nad nimi skutočne premýšľať, takto si tiež môžeme pomôcť rozšíriť naše obzory.²⁹ „Myslenie nie je len o jednom výsledku, ale najmä o tej ceste, procese ako sa k nemu dostať. Sokrates robil to isté. Diskutoval s ľuďmi, pýtal sa ich otázky, ktoré človeka doviedli k tomu, že začal pochybovať o niečom, čo pokladal za samozrejmé. O tom to všetko je“. Kritické myslenie učí človeka myslieť slobodne. Stratí sa tendencia slepo nasledovať niekoho názory“. ³⁰

Kritické myslenie je viac než len hromadenie faktov a vedomostí; je to spôsob, ako pristupovať k čomukoľvek, čo práve zamestnáva vašu myseľ, aby ste dospeli k najlepšiemu možnému záveru. Pomocou kritického myslenia sa zameriavame na neustále zlepšovanie svojich vedomostí a zapájame sa do samostatného seba učenia. ³¹

Kritické myslenie je proces, kedy sa človek neustále snaží zdokonaľiť svoje city v presnosti vo vyjadrovaní. Človek, ktorý má kritické myslenie sa nezaoberá len myslením iných a o informáciách zo sveta. Rovnako skúma aj vlastné myšlienkové pochody a vznik vlastných rozhodnutí či názorov. Na základe týchto krokov potom upravuje svoju komunikáciu, aby bola jasná a zrozumiteľná. ³²

Kritické myslenie sa v zahraničí vyučuje na školách bežne. Bohužiaľ na Slovensku sa táto možnosť ešte len začína vyvíjať. Tým, že študent v škole nie je nútený myslieť sám za seba, mechanicky opisuje poznámky z tabule, učí sa naspamäť nejaký povinný text alebo je stále pasívnym prijímateľom informácií. Učitelia na školách by sa mali snažiť o to, aby študenti začali kriticky myslieť. Je to náročný proces.

Kritické myslenie sa dá rozvíjať aj:

- Pri čítaní je potrebné skontrolovať si zdroj.
- Brať do úvahy posudzovacie štandardy v určitej oblasti.

²⁸ BLAZSEKOVÁ, T. 2015. Čo je to kritické myslenie? Dostupné na internete: <https://www.startitup.sk/co-je-to-kriticke-myslenie/>

²⁹ BLAZSEKOVÁ, T. 2015. Čo je to kritické myslenie? Dostupné na internete: <https://www.startitup.sk/co-je-to-kriticke-myslenie/>

³⁰ BLAZSEKOVÁ, T. 2015. Čo je to kritické myslenie? Dostupné na internete: <https://www.startitup.sk/co-je-to-kriticke-myslenie/>

³¹ PATEL, D. 2018. 16 Characteristics of Critical Thinkers. Dostupné na internete: <https://www.entrepreneur.com/article/321660>

³² KRITICKÉMYSLÉNIE.SK. *Kritické myslenie predstavuje systematickú zvedavosť a otvorenú myseľ*. [online]. [cit. 15.4.2022] Dostupné z internetu: <https://kritickemyslenie.sk/co-je-kriticke-myslenie/>

- Pracovať iba so zdrojmi, ktoré sa pokladajú za autoritu v konkrétnej oblasti.
- Brať do úvahy rozličné uhly pohľadu.³³

Záver

Falošné správy a dezinformácie predstavujú v čoraz väčšej miere komplexnú regulačnú výzvu pre demokratizovaný a sprostredkovaný online informačný ekosystém. Falošné správy a dezinformácie sa ľahko vytvárajú a sú rýchlo distribuované platformami, ktoré sú viac motivované finančnými stimulmi ako novinárskou etikou resp. verejným záujmom a následne sú dychtivo konzumované používateľmi, u ktorých posilňujú existujúce presvedčenia.

Autori majú pri tvorbe obsahu často zmes motívov. V boji proti šíreniu takýchto správ môžeme aplikovať mediálnu gramotnosť a výchovu s kombináciou kritického myslenia.

Užívatelia falošných správ majú obmedzené stimuly investovať do spochybňovania alebo overovania ich obsahu, najmä vtedy, keď materiál posilňuje ich existujúce presvedčenia a perspektívy. Nakoniec, falošné správy sa zriedka objavujú samostatne. Často sa miešajú s viacerými presnými príbehmi, takže je ich ťažšie kategoricky odmietnuť ako škodlivý zdroj. tento článok naznačuje súbor zásahov na elimináciu šírenia falošných správ a dezinformácií založených na mediálnej výchove, mediálnej gramotnosti a kritickom myslení.

Zoznam použitej literatúry

BLAZSEKOVÁ, T. 2015. Čo je to kritické myslenie? [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.startitup.sk/co-je-to-kriticke-myslenie/>

EDUWORLD.SK. *Kritické myslenie – povinná výbava každého z nás*. [online].

[cit. 13.7.2022] Dostupné na internete: <https://eduworld.sk/cd/jaroslava-konickova/9473/metody-ktore-aktivizuju-ziakov-pri-uceni>

³³ KRITICKÉMYSLENIE.SK. Kritické myslenie predstavuje systematickú zvedavosť a otvorenú myseľ. [online]. [cit. 15.4.2022] Dostupné z internetu: <https://kritickemyslenie.sk/co-je-kriticke-myslenie/>

GLOBSEC Trends 2022: Väčšina ľudí na Slovensku stále verí konšpiráciám a cíti sa ohrozené. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.globsec.org/what-we-do/press-releases/globsec-trends-2022-vacsina-ludi-na-slovensku-stale-veri-konspiraciam>

HÚSKOVÁ, E. 2020. Súčasné trendy šírenia dezinformácií. s. 23. [online]. Dostupné na internete: <https://stratpol.sk/wp-content/uploads/2021/02/publi-trendy-%C5%A1%C3%ADrenia-dezinform%C3%A1ci%C3%AD2.pdf>

KANIČAROVÁ, K. 2021. *Propaganda (DISINFO BASICS)*. [online]. [cit.2023-05-09] Dostupné na internete: <https://infosecurity.sk/dezinfo/propaganda-disinfobasics/>

KOHOUT, R. KARCHŇÁK, R. 2016. Bezpečnosť v online prostredí. Karlovy Vary: Biblio Karlovy Vary. 2016. 68 s. ISBN 978-80-260-9543-9. Dostupné na internete: <https://www.internetembezpecne.cz/wp-content/uploads/2017/03/Roman-Kohout-Bezpecnost-v-online-prostredi.pdf>

KOPRENA, E. 2020. Mediálna gramotnosť ako základná zručnosť v digitálnej spoločnosti. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.direktor.sk/sk/casopis/manazment-skoly-v-praxi/medialna-gramotnost-ako-zakladna-zrucnost-v-digitalnej-spolocnosti.m-693.html>

Krátky slovník hybridných hrozieb Národného bezpečnostného úradu. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>

KRITICKÉMYSLENIE.SK. *Kritické myslenie predstavuje systematickú zvedavosť a otvorenú myseľ*. [online]. [cit. 15.4.2022] Dostupné z internetu:

<https://kritickemyslenie.sk/co-je-kriticke-myslenie/>

Mark Verstraete, Jane R. Bambauer, and Derek E. Bambauer, *Identifying and Countering Fake News*, 73, Hastings L.J., 821, (2022).online]
https://repository.uclawsf.edu/hastings_law_journal/vol73/iss3/6

MEDIALNA VYCHOVA. 2010. Dezinformácia. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://medialnavychova.sk/dezinformacia/>

MKSR. 2020. Koncepcia mediálnej výchovy v SR. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.culture.gov.sk/uncat/koncepcia-medialnej-vychovy-v-sr/>

MORAVČIKOVÁ, E. 2020. Mediálna kultúra I. Univerzita Konštantína Filozofa v Nitre, Filozofická fakulta, 2020. ISBN: 978-80-558-1617-3; p.č. 214058

PATEL, D. 2018. 16 Characteristics of Critical Thinkers. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.entrepreneur.com/article/321660>

PIRKOVA, E. 2021. What is disinformation, why it spreads, and how to stop it. online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.accessnow.org/what-is-disinformation-how-to-stop-it/>

ŠNÍDL, V. 2017. Pravda a lož na Facebooku. Bratislava : N Press, s.r.o., 2017. 162 s. ISBN 978-80-9723394-4-2.

UNIPO.SK. *Hoax (Poplašné správy)* [online]. [cit. 2023-05-09]. Dostupné na internete: <https://www.unipo.sk/9470/>

VRABEC, N. 2008. Mládež a média. Mediálna gramotnosť mladších ľudí na Slovensku. Bratislava: Iuventa. 2008. 37 s. ISBN 978-80-8072-074-2. Dostupné na internete: https://www.iuventa.sk/files/documents/7_vyskummladeze/publikacie/media_mlade.pdf

Yar, L. 2019. Falošné správy a dezinformácie: Terminológia, nástroje a výzvy. [online]. [cit. 2023-05-09]. Dostupné na internete: <https://euractiv.sk/section/digitalizacia/news/falosne-spravy-a-dezinformacie-terminologia-nastroje-a-vyzvy/>

Kontaktné údaje

Ing. Peter Poláček

Katedra bezpečnosti a obrany

Akadémia ozbrojených síl gen. M. R. Štefánika

Demänová 393, 031 01 Liptovský Mikuláš

E mail: polacek.pepo@gmail.com

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA
doc. RNDr. Tatiana Hajdúková, PhD

Rethinking Blockchain Technology Suitability: A New Decision Flowchart for Diverse Use Cases

Michal Ries, Muhammad Nasim Bahar, Antonín Korauš

Abstract

Blockchain technology has garnered significant interest in various domains due to its unique features, such as decentralization, immutability, and security, which offer unparalleled data integrity protection. These are the reasons why it is emerging as an important aspect in the fight against hybrid threats. The inception of Bitcoin as the first cryptocurrency project has paved the way for numerous applications and use cases. The advent of smart contracts has further expanded the potential utility of blockchain technology across multiple domains. This paper aims to critically examine the suitability of blockchain technology in new use cases with a focus on high-level data integrity, particularly in contexts where multiple potential writers to a shared ledger are not present. We scrutinize the existing state-of-the-art decision flowcharts that guide the selection of blockchain technology, arguing that they may need to address the diverse range of potential applications adequately. Consequently, we propose an innovative decision flowchart that better aligns with the evolving landscape of blockchain use cases. This new flowchart provides a more comprehensive approach to determining whether blockchain is the appropriate technical solution for a given scenario.

Index Terms

blockchain, blockchain technology, suitability of blockchain, hybrid threats, security

INTRODUCTION

The introduction of blockchain technology, first implemented in the cryptocurrency domain through the Bitcoin project [12], has given rise to a plethora of applications across various domains. These include IoT, big data, cloud and edge computing, identity management, cryptocurrency, economics and markets, business solutions, automation, supply chains, healthcare records, communication, and more [1], [4], [6], [7], [9], [10], [12], [15], [16], [18], [21], [22]. Despite its widespread adoption, the suitability of blockchain technology for different use cases and applications remains a topic of ongoing debate. In the context of the current development of hybrid threats, the mentioned technology is one of the tools for the application of hybrid threats from the field of information technology. Blockchain technology has evolved through several generations, each bringing new features and capabilities. The first generation of blockchain technologies, exemplified by Bitcoin, utilized public permissionless blockchains, allowing untrusted participants to join the network and view transactions. The second generation, marked by the introduction of smart contracts in Ethereum and Cardano blockchains, expanded the potential applications for this technology. The third generation of blockchain technology, referred to as Blockchain 3.0, saw its

adoption in a wide array of domains such as healthcare, education, e-commerce, agriculture, and more, with projects like Hyperledger, R3 Corda, and Ethereum Quorum leading the charge. Blockchain 4.0 addresses crucial issues such as scalability, throughput, and latency by leveraging distributed environments.

Over the course of blockchain technology's development, various flowcharts and decision frameworks have been proposed to assess the suitability of employing this technology in specific contexts. Recently, blockchain has been applied in projects focused on data integrity and the implementation of future policies. In this paper, we propose a novel flowchart for evaluating the appropriateness of blockchain technology in diverse use cases. Additionally, we have developed a prototype based on the proposed flowchart to demonstrate its practical application.

The remainder of this paper is structured as follows. Section 2 provides an overview of the related work concerning the assessment of blockchain technology's suitability. Section 3 presents our proposed decision flowchart for evaluating the appropriateness of blockchain technology, along with the developed prototype. Section 4 discusses the results and findings derived from the application of our proposed framework. Finally, Section 5 offers concluding remarks and outlines potential avenues for future research.

RELATED WORK

Numerous studies have explored the suitability of blockchain technology for various applications and use cases, with many converging on similar validation criteria [3], [5], [8], [11], [14], [19], [20]. Typically, these assessments commence by determining whether the ledger state is shared and proceed to evaluate the presence of multiple untrusted writers in the shared ledger. The seminal work by Karl Wu'st and Arthur Gervais [19] delved into blockchain technology's fundamental properties and features, including public verifiability, transparency, privacy, integrity, and redundancy. They proposed a decision-making tree to facilitate the evaluation of blockchain technology's appropriateness for a specific use case. In addition, their study analyzed two use cases in depth: supply chain management and interbank payment systems, highlighting the benefits and challenges of employing blockchain technology in these contexts. Peck, Morgen E [14] proposed another flowchart for assessing blockchain technology's suitability, emphasizing the trade-offs between transaction speed and other desirable features. Their flowchart guides selecting blockchain-based solutions depending on the required transaction speed—medium or low—while

also considering other factors such as security and decentralization. A further study [8] investigated a range of use cases and developed a decision framework for determining the optimal blockchain platform. This framework categorizes blockchain platforms into four groups: Public Permissionless, Private Permissions, Public Permissioned, and Private Permissioned. Additionally, the authors introduced a constraint stage, which considers various features of blockchain platforms, such as throughput, data storage, smart contracts, privacy, and more. This comprehensive framework enables a more nuanced evaluation of the suitability of different blockchain platforms for various use cases. Sin Kuang Lo's research [11] proposed an evaluation framework for assessing the appropriateness of blockchain technology based on existing industrial products, technical forums, and academic literature. Their framework consists of a seven-question process designed to evaluate the suitability of blockchain technology for specific applications systematically. This process covers a range of factors, including data storage requirements, transaction speed, and security concerns, among others. In summary, the existing body of literature on blockchain technology suitability offers valuable insights into the critical factors to consider when determining whether to adopt this technology for a given use case. These studies have provided decision-making trees, flowcharts, and frameworks to facilitate a structured evaluation process. However, with the rapid evolution of blockchain technology and the emergence of new use cases, there is a need for updated decision-making tools that adequately address the diverse and evolving landscape of blockchain applications. In this paper, we propose a novel flowchart that aims to address these gaps and provide a more comprehensive approach to assessing the suitability of blockchain technology across various domains.

PROPOSED WORK

In recent years, a growing body of research has explored the potential applications of blockchain technology within single private organizations, focusing on enhancing trust, data integrity, and security. The studies conducted by Omote and Kazumasa [13] propose a novel permissionless private blockchain framework that can be self-managed and maintained by a single organization. This approach offers height need security against fraud by leveraging the organization's trust, which numerous unspecified users verify. Implementing a blockchain framework can reduce costs associated with coordinating multiple organizations or entities to

ensure secure transactions while streamlining the management process and enhancing overall efficiency.

Furthermore, other researchers have investigated the role of blockchain technology in addressing challenges related to scalability, security, and communication delays in the Internet of Things (IoT) context. These studies suggest integrating blockchain technology into IoT systems can improve data integrity, strengthen security measures, and facilitate efficient device communication. The decentralized nature of blockchain technology allows the creation a more resilient and robust IoT infrastructure, capable of withstanding external hybrid threats and maintaining seamless connectivity [2]. In another notable example, the Singapore Government has employed blockchain technology to produce digital certificates for graduates, aiming to enhance data integrity and trust in the credentialing process. By leveraging blockchain technology's immutability and security features, the government has created a tamper-proof system for issuing and verifying academic credentials. This innovative approach reduces the risk of fraudulent certificates and streamlines the verification process for employers and other stakeholders, resulting in increased trust and efficiency [17]. These recent developments demonstrate the growing interest in applying blockchain technology within single private organizations and various domains. As more research is conducted and practical implementations emerge, it becomes increasingly vital to reevaluate the decision-making frameworks for assessing the suitability of blockchain technology. our proposed flowchart is presented in Figure 1.

The flowchart is designed to guide users through a series of questions to determine the suitability of implementing blockchain technology for a specific use case. The decision-making process follows a binary approach, with each question offering two possible answers (Yes or No). Depending on the user's response, the flowchart directs them toward the next appropriate question or to a conclusion.

In addition to proposing a novel flowchart for evaluating the suitability of blockchain technology, we have also implemented and developed a prototype to demonstrate its practical application. This prototype serves as a valuable tool for stakeholders to assess the appropriateness of blockchain technology in various use cases and contexts. The prototype was developed using the PHP Laravel framework, which offers flexibility and ease of modification to accommodate future updates to the proposed flowchart. As the landscape of blockchain technology and its

applications continue to evolve, our prototype's adaptability ensures that it remains relevant and helpful in assessing the suitability of blockchain-based solutions. Figure 2 provides a screenshot of the developed prototype, illustrating its user interface and the decision-making process guided by the proposed flowchart. The prototype design focuses on user-friendliness, enabling users to efficiently navigate the evaluation process and obtain insights

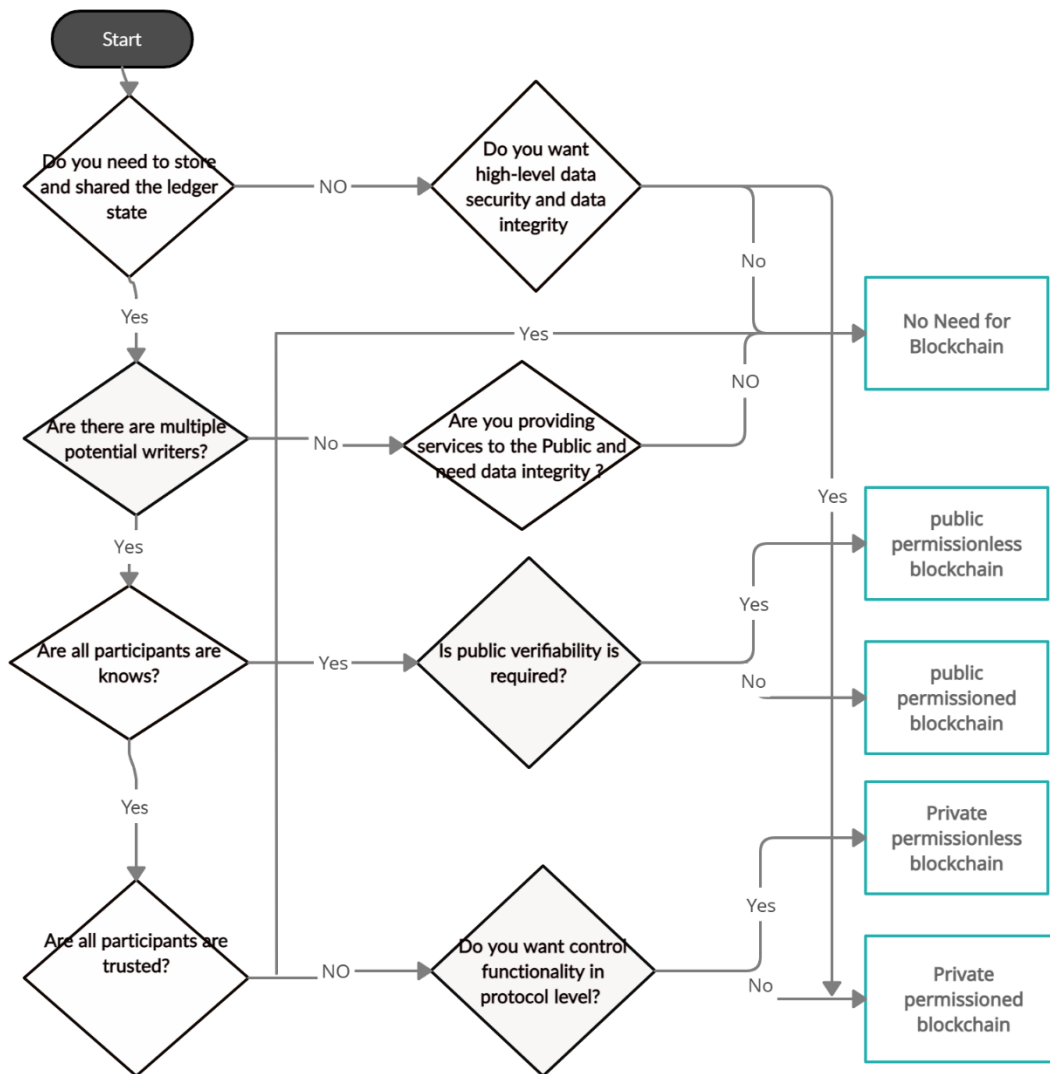


Fig. 1. Proposed flowchart for suitability

ZDROJ?

into the appropriateness of blockchain technology for their specific use cases.

Phase One Suitability of the Blockchain

Suitability of the Blockchain

Start

Do you need to store and share the ledger state?

Are there multiple potential writer to the shared ledger?

Are all participants of shared ledger is known?

Are the participants of the shared ledger is trusted?

Do you want control functionality of protocol level?

Yes No

✓ Alert!
You need Private Permissioned BlockChain System. Go to the Second Phase to Select appropriate platform.

Fig. 2. A Screenshot of the developed prototype

Zdroj: vlastné spracovanie

CONCLUSION

Blockchain technology originated in the cryptocurrency domain and has rapidly gained traction across various in- industries. Various flowcharts and decision-making frameworks have been proposed to assess the suitability of blockchain technology for specific use cases. In this paper, we have introduced a novel flowchart designed to reevaluate the appropriateness of blockchain technology across diverse applications. As blockchain technology evolves, new use cases will likely emerge, driving the need for updated decision-making tools that accommodate these developments. Our proposed flowchart offers a comprehensive and flexible approach to evaluating the suitability of blockchain technology, ensuring its relevance and usefulness in the ever-changing landscape of blockchain applications. In conclusion, the new flowchart presented in this paper provides an updated perspective on assessing the appropriateness of blockchain technology for various use cases. Its application in the fight against hybrid threats gives expert and professional scope for sophisticated management of this fight. By continually re-evaluating and refining the decision-making process, we aim to promote the responsible adoption of blockchain technology and foster innovative solutions across multiple domains.

ACKNOWLEDGMENT

The contribution was created within the national project “Increasing Slovakia’s resilience to hybrid threats by strengthening public administration capacities”, project code ITMS2014+:314011CDW7. This project is supported by the European Social Fund.

REFERENCES

- Abou Jaoude, J., Saade, R.G.: Blockchain applications—usage in different domains. *IEEE Access* 7, 45360–45381 (2019)
- Anaam, E., Hasan, M.K., Ghazal, T.M., Haw, S.C., Alzoubi, H.M., Alshurideh, M.T.: How private blockchain technology secure iot data record. In: 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC). pp. 1–6. IEEE (2023)
- Belotti, M., Božić, N., Pujolle, G., Secci, S.: A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys Tutorials* 21(4), 3796–3838 (2019)
- Davidson, S., De Filippi, P., Potts, J.: Economics of blockchain. Available at SSRN 2744751 (2016)
- Dawit, N.A., Mathew, S.S., Hayawi, K.: Suitability of blockchain for collaborative intrusion detection systems. In: 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC). pp. 1–6. IEEE
- Deepa, N., Pham, Q.V., Nguyen, D.C., Bhattacharya, S., Prabadevi, B., Gadekallu, T.R., Maddikunta, P.K.R., Fang, F., Pathirana, P.N.: A survey on blockchain for big data: approaches, opportunities, and future directions. *Future Generation Computer Systems* (2022)
- Huh, S., Cho, S., Kim, S.: Managing iot devices using blockchain platform. In: 2017 19th international conference on advanced communication technology (ICACT). pp. 464–467. IEEE
- Hunhevicz, J.J., Hall, D.M.: Do you need a blockchain in construction? use case categories and decision framework for dlt design options. *Advanced Engineering Informatics* 45, 101094 (2020)
- Hořtbl, M., Kompara, M., Kamišalic, A., Nemec Zlatolas, L.: A systematic review of the use of blockchain in healthcare. *Symmetry* 10(10), 470 (2018)
- Korauš, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. RELIK 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>

- Jacobovitz, O.: Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva 1, 9 (2016)
- Lo, S.K., Xu, X., Chiam, Y.K., Lu, Q.: Evaluating suitability of applying blockchain. In: 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS). pp. 158–161. IEEE
- Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decen- tralized Business Review p. 21260 (2008)
- Omote, K.: Does private blockchain make sense? In: 2023 IEEE Inter- national Conference on Consumer Electronics (ICCE). pp. 01–03. IEEE (2023)
- Peck, M.E.: Blockchain world-do you need a blockchain? this chart will tell you if the technology can solve your problem. IEEE Spectrum 54(10), 38–60 (2017)
- Rathee, G., Balasaraswathi, M., Chandran, K.P., Gupta, S.D., Boopathi, C.: A secure iot sensors communication in industry 4.0 using blockchain technology. Journal of Ambient Intelligence and Humanized Computing 12(1), 533–545 (2021)
- Queiroz, M.M., Telles, R., Bonilla, S.H.: Blockchain and supply chain management integration: a systematic review of the literature. Supply Chain Management: An International Journal (2019)
- Sagar, M.: Singapore government uses blockchain technology to produce digital certificates for graduates. Accessed: 2023-02-10
- Tredinnick, L.: Cryptocurrencies and the blockchain. Business Informa- tion Review 36(1), 39–44 (2019)
- Wu`st, K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 45–54. IEEE
- Xu, X., Weber, I., Staples, M.: Design process for applications on blockchain, pp. 93–111. Springer (2019)
- Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y.: Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Communications Surveys Tutorials 21(2), 1508–1532 (2019)

CONTACT INFORMATION

Michal Ries

Faculty of Informatics and Information Technologies

Slovak University of Technology

Bratislava, Slovakia 0000-0002-9233-7123

E-mail: michal.ries@stuba.sk

Muhammad Nasim Bahar

Faculty of Informatics and Information Technologies Slovak University of Technology

Bratislava,

Slovakia

E-mail: muhammad.bahar@stuba.sk

Antonín Korauš

Academy of the Police Force in Bratislava

Sklabinská 1, 835 17 Bratislava 35

Slovakia

E-mail: antonin.koraus@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Hybridná vojna a hybridné hrozby

Róbert Tomášek

Abstrakt

Hybridná vojny a hybridné hrozby nepredstavujú novodobé zbrane. Skúsení a prezieraví vládcovia, generáli a vojenský stratégovia ich využívajú už niekoľko tisícročí. Schopnosť využiť vhodné nástroje, metódy a spôsoby na dosahovanie svojich zväčša skrytých cieľov bola nevyhnutná pre dosiahnutie víťazstva. Novodobé formy hybridných hrozieb naberajú sofistikovaný charakter, pričom vďaka rozvoju informačných a komunikačných technológií nabrali globálny charakter.

Kľúčové slová

hybridná vojna, hybridná hrozba, zbrane

Abstract

Hybrid warfare and hybrid threats do not represent modern weapons. Experienced and far-sighted rulers, generals and military strategists have been using them for millennia. The ability to employ the appropriate tools, methods and means to achieve their largely hidden objectives has been essential to achieving victory. Modern forms of hybrid threats have become more sophisticated and, thanks to the development of information and communication technologies, have become global in nature.

Key words

hybrid warfare, hybrid threats, weapons

Úvod

Hybridná vojna a hybridné hrozby nepredstavujú novinku, ktorú by ľudstvo predtým nepoznalo. Práve naopak. Rôzne formy hybridných aktivít môžeme nájsť naprieč celou históriou ľudstva. Išlo o rôzne spôsoby ovplyvňovania určitej záujmovej skupiny alebo celej spoločnosti, jej nálad a postojov alebo o uzatváranie verejne známych, ako aj utajených spojeneckých zmlúv a paktov, podplácanie aktérov konfliktu, atď. Hybridné hrozby predstavovali vždy veľmi silný a účinný nástroj na dosahovanie vlastných cieľov počas vedenia hybridnej vojny, aj keď výsledky nie sú tak zjavné, ako by to bolo pri konfrontácii s protivníkom na bojovom poli.

V súčasnosti sa viac ako priamo na bojovom poli bojuje v ešte náročnejšom a komplikovanejšom „území“ – vo virtuálnom svete. Kybernetické útoky predstavujú veľmi silný komponent hybridných hrozieb.¹³⁹ Po odstránení bipolarity sveta, je bezpečnostné prostredie stále komplikovanejšie a charakterizuje ho nestabilita a nerovnomernosť vývoja i vysoká dynamika. Možnosti ako destabilizovať štát, zasiahnuť obyvateľstvo alebo zničiť

¹³⁹ IVANČÍK, R. 2021. Útočné kybernetické operácie ako súčasť hybridných hrozieb. In *Trilobit*, 2021

kritickú infraštruktúru už nie je otázkou použitia strategických jadrových nosičov a rozsiahlych konvenčných operácií, ale zahrňujú laptopy, počítačové siete, pašované chemické, biologické, rádioaktívne látky, ktoré môžu byť na cieľ dopravené akýmkoľvek spôsobom, cieľnú propagandu, organizovaný zločin. V súčasnosti sa už v diplomatických, politických, vojenských i akademických kruhoch nehovorí len o otvorených hrozbách, ale čoraz častejšie aj o hrozbách asymetrických, zámerných, latentných, permanentných – hybridných hrozbách¹⁴⁰.

Vďaka výdobytcom vedecko-technického pokroku a využívaniu moderných technológií¹⁴¹ hybridná vojna už dávno získala označenia ako neopakovateľná, flexibilná, „lacná“ cesta zničenia spoločnosti, štátu alebo iného protivníka bez oficiálneho vyhlásenia vojny. Práve tieto atribúty robia hybridnú vojnu takou zaujímavou a zároveň nebezpečnou, nakoľko nepriateľ nemusí byť jednoznačne identifikovateľný, môže sa skrývať a „nenápadne“ vnucovať spoločnosti svoje či už politické, ekonomické alebo sociálne predstavy, ktoré môžu narušiť jeho fungovanie, ohroziť jeho bezpečnosť, destabilizovať spoločnosť a pod.

Hybridná vojna

Hybridná vojna predstavuje v najširšom zmysle taký druh vojny, ktorý je charakterizovaný špecifickou kombináciou prostriedkov a metód nielen symetrického, ale najmä asymetrického charakteru.¹⁴² Jedným z prvých Európanov, ktorý sa zaoberal problematikou hybridných vojen a dokázal ich definovať, bol holandský generálmajor a poslanec parlamentu Frank van Kappen, podľa ktorého hybridné hrozby a hybridná vojna predstavujú široké spektrum nepriateľských aktivít, v ktorých úloha vojenského komponentu je skôr malá, pretože politický, informačný, ekonomický a psychologický vplyv sa stáva hlavným prostriedkom vedenia boja. Takéto metódy pomáhajú dosiahnuť významné výsledky: teritoriálne, politické a ekonomické straty nepriateľa, chaos a rozvrat systému výkonu štátnej moci a oslabenie morálky spoločnosti. Kappen však nielen zdefinoval hybridné hrozby a hybridnú vojnu, ale poukázal na dôležitý fakt, že štáty, ktoré vedú hybridnú vojnu, uzatvárajú dohody s neštátnymi aktérmi, bojovníkmi (žoldnieri), súkromnými organizáciami a skupinami miestnych obyvateľov, avšak akúkoľvek komunikáciu s nimi popierajú. Títo aktéri

¹⁴⁰ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

¹⁴¹ Bližšie pozri: KUČTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018

¹⁴² IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016

totiž môžu vykonávať (realizovať) takého veci (kroky), ktoré si cudzí štát nemôže dovoliť podniknúť oficiálne.¹⁴³

Hoffman zasa vníma hybridnú vojnu ako druh vojny, ktorá môže byť vedená nielen štátnymi ale aj neštátnymi aktérmi, pričom v sebe spája rôzne typy vedenia vojny – konvenčné kapacity, neregulárne taktiky a formácie, teroristické aktivity uskutočňované nevyberavým násilím a kriminálnymi nepokojmi. Hybridná vojna predstavuje podľa neho viac ako len konflikt medzi štátmi a inými ozbrojenými skupinami. Je aplikáciou rôznych foriem konfliktu, ktoré najlepšie odlišujú hybridné hrozby alebo hybridné konflikty. Tieto rôznorodé aktivity môžu byť vykonávané viacerými samostatnými jednotkami (alebo dokonca tou istou jednotkou), pričom sú operačne a takticky riadené a koordinované v priestore operácie za účelom dosiahnutia synergického efektu vo fyzickom i psychologickom rozmere konfliktu. Želané účinky pritom možno dosiahnuť na všetkých úrovniach konfliktu.¹⁴⁴

Hybridná vojna predstavuje podľa Jurčáka a kol. akt násilia, uskutočňovaný s výrazne rozdielnymi prostriedkami alebo spôsobmi, s cieľom donútiť protivníka, aby sa podriadil našej vôli, alebo ako pokračovanie politiky výrazne rozdielnymi prostriedkami, pričom uskutočňovanie politiky sa vykonáva otvorene i skryto, rôznymi aktivitami štátnych i neštátnych aktérov, vojenskými i nevojenskými prostriedkami, konvenčnými i asymetrickými formami vedenia vojny, a to aj bez jej vyhlásenia. Ako autori uvádzajú ďalej, hybridná forma vedenia vojny nemá v porovnaní s otvorenou formou vedenia vojny relatívne ustálenú a vopred danú šablónu vykonania a tiež terminológiu. Analýza reálneho použitia hybridných foriem vedenia vojny ukazuje, že je pre ňu charakteristická odlišnosť a neopakovateľnosť usporiadania jej komponentov a prvkov od prípadu k prípadu. Hybridná forma vedenia vojny sa počas vykonávania prispôbuje zmenám v strategickom a operačnom prostredí. Inými slovami agresor, ktorý používa hybridnú formu vedenia vojny, volí použitie komponentov a ich prvkov (v rámci nich mix nástrojov a prostriedkov) často *ad hoc* podľa jeho aktuálnych možností a vývoja situácie v napadnutej krajine.¹⁴⁵

¹⁴³ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

¹⁴⁴ HOFFMAN, G. F. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute*, 2007

¹⁴⁵ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

Čekinov a Bogdanov (pozri Ivančík, 2016¹⁴⁶ alebo Jurčák a kol. 2017¹⁴⁷) už v roku 2013 rozdelili priebeh tzv. „vojny novej generácie“ (hybridnej vojny) do nasledujúcich fáz:

- 1. nevojenské asymetrické vedenie vojny zahŕňajúce informačné, psychologické, ideologické, diplomatické a ekonomické opatrenia ako časť plánu na vytvorenie priaznivých politických, ekonomických a vojenských predpokladov pre ďalšie fázy vojny,
- 2. špeciálne operácie s cieľom oklamať politických a vojenských predstaviteľov koordinovanými opatreniami prostredníctvom diplomatických kanálov, masovo-komunikačných prostriedkov, vládnych a vojenských agentúr, únikom falošných údajov, rozkazov, nariadení a smerníc,
- 3. zastrašovanie, klamanie, podplácanie vládnych a vojenských predstaviteľov s cieľom prinútiť ich, aby prestali plniť svoje služobné povinnosti,
- 4. destabilizujúca propaganda, ktorá má zvýšiť nespokojnosť obyvateľstva, čo bude umocnené príchodom militantných skupín a eskaláciou podvratnej činnosti,
- 5. zriadenie bezletových zón nad krajinou, ktorá má byť napadnutá, vyhlásenie blokády a rozsiahle využitie súkromných vojenských spoločností v tesnej spolupráci s ozbrojenými opozičnými jednotkami,
- 6. zahájenie vojenských akcií, ktorým predchádzal rozsiahly prieskum a diverzná činnosť, t. j. všetky typy, formy a metódy operácií, vrátane operácií špeciálnych jednotiek, operácií vo vesmíre, rádiové a elektronické operácie, diplomatické spravodajstvo, spravodajstvo tajných služieb a priemyslová špionáž,
- 7. operácie vedené prostredníctvom cielených informácií, elektronický boj, letecké a kozmické operácie, nepretržité letecké zastrašovanie v súčinnosti s použitím vysoko presných zbraňových systémov (vrátane mikrovln, radiácie, neletálnych biologických zbraní, atď.),
- 8. likvidácia zostávajúcich miest odporu a zničenie zvyškov nepriateľských zoskupení prostredníctvom špeciálnych operácií vedených prieskumnými jednotkami, ktoré vyhľadávajú jednotky nepriateľa a hlásia ich súradnice raketovým a delostreleckým jednotkám, paľba s využitím vyspelých, vysoko presných zbraní, sústredená na zničenie jednotiek, ktoré kladú odpor, nasadenie výsadkových jednotiek, ktoré obklúčia

¹⁴⁶ IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016

¹⁴⁷ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

posledné body odporu a operácie na vyčistenie terénu prostredníctvom pozemných jednotiek¹⁴⁸.

Hybridná vojna, jej metódy, prostriedky a ciele, ktoré chce aktér jej použitím dosiahnuť, sa budú neustále vyvíjať a zdokonaľovať, a to predovšetkým vďaka dynamickým zmenám prebiehajúcim na spoločenskej, politickej, ekonomickej, bezpečnostnej, technologickej a ďalších úrovniach.¹⁴⁹ Hybridná vojna v „priamom prenose“ prebieha aj na Slovensku. Vplyv pôsobenia zahraničných aktérov sa odráža v našej spoločnosti na všetkých úrovniach od sociálnej cez politickú, ekonomickú, vojenskú až po energetickú (podporovanie chaosu a nedôvery spoločnosti voči autoritám a politickým predstaviteľom, neznášanlivosti a antagonizmu v názoroch na zásadné otázky, atď.).

Hybridné hrozby

Hybridné hrozby môžeme v najširšom zmysle definovať ako súbor rôznorodých (zmiešaných) hrozieb, ktoré spolu vytvárajú kompaktný celok. Kombináciu nástrojov, metód a prostriedkov, ktoré majú jediný cieľ – ohroziť, zastrašiť alebo eliminovať nepriateľa. Zložitosť hybridných hrozieb spočíva v ich komplexnosti, skrytosti a v náročnej preukázateľnosti zo strany napadnutej krajiny, pričom krajina, ktorá hybridné hrozby používa ich popiera¹⁵⁰.

Hoffman hybridné hrozby definuje ako správanie akéhokoľvek nepriateľa, ktorý súčasne využíva na mieru prispôbený komplex konvenčných zbraní, neregulárnej taktiky, terorizmu a kriminálneho správania v rovnakom čase a priestore na dosiahnutie svojich politických alebo iných cieľov.¹⁵¹

V Krátkom slovníku hybridných hrozieb Národného bezpečnostného úradu je hybridná hrozba zadefinovaná ako súbor nátlakových, podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny¹⁵² Hybridná hrozba je charakteristická simultánnym použitím viacerých

¹⁴⁸ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

¹⁴⁹ IVANČÍK, R. 2020. Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2020 – zborník príspevkov z 11. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2020

¹⁵⁰ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

¹⁵¹ HOFFMAN, G. F. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute*, 2007

¹⁵² NBÚ. 2022. Hybridné hrozby. In *Krátky slovník hybridných hrozieb*, 2022

nástrojov koordinovaným spôsobom s cieľom využiť zraniteľnosti (slabé miesta) protivníka a následne oslabiť jeho rozhodovacie procesy pri zachovaní určitého stupňa hodnoverného popretia. Strategickým cieľom týchto hrozieb je oslabenie dôvery verejnosti v demokratické inštitúcie, prehĺbenie nezdravej polarizácie na národnej a medzinárodnej úrovni, spochybnenie základných hodnôt demokratických spoločností, zisk geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných a ovplyvňovania demokratických rozhodovacích procesov.

Medzi najefektívnejšie hrozby patria tie, ktoré spôsobia neúmerne vysoké škody vo vzťahu k zdrojom, času a financiám vynaložených útočníkom. V ideálnom prípade by sa účinok asymetrického útoku mohol prejaviť až na strategickej úrovni bez ohľadu na to, na akej úrovni bol realizovaný¹⁵³.

Hybridné hrozby používa protivník, ktorý súčasne a adaptabilne využíva rôzne kombinácie politických, ekonomických, sociálnych, informačných aktivít a nástrojov moci a zároveň konvenčné, nepravidelné, teroristické a rozvratné kriminálne spôsoby vedenia boja, pričom protivníkom môže byť štátny alebo neštátny aktér, prípadne ich kombináci.¹⁵⁴ V ostatných niekoľkých rokoch sa na šírenie hybridných hrozieb aktívne využívajú rôzne nové médiá, predovšetkým sociálne siete.¹⁵⁵

Medzi „nové“ typy hrozieb, ktoré sú súčasťou hybridných hrozieb radia Jurčák a kol.¹⁵⁶:

- *nástroje informačnej vojny* - akým sú napr. propaganda, antipropaganda. Sú to klasické hybridné hrozby, voči ktorým je veľmi ťažké ubrániť sa. Sú postavené na sociálnej zraniteľnosti a protisystémových náladách v spoločnosti, ktoré sú vyvolávané tzv. trollmi cez internet;
- *hrozby súvisiace s kybernetickým priestorom* - kybernetické útoky, kyberterorizmus, hacktivizmus (spojenie slov hackerstvo a aktivizmus – ide o podvratné používanie počítačov a počítačových sietí s cieľom podporiť politickú propagandu a dosiahnuť politické zmeny);

¹⁵³ NOVOTNÝ, A. 2003. *NATO a medzinárodná bezpečnosť*. Nové Zámky : Crocus, 2003

¹⁵⁴ GLENN, W., R. 2009. Thoughts on Hybrid Conflict. In *Small Wars Journal*, 2009

¹⁵⁵ ZACHAR KUČTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022

¹⁵⁶ JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. 2017. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

- *whistle-blowing* – v slovenskom ponímaní ide o oznamovateľov protispoločenskej činnosti. V kontexte hybridných hrozieb však za whistle-blowera pokladáme osobu, ktorá vyzradí tajné informácie verejnosti alebo cudzej moci s cieľom dosiahnuť vlastný zisk alebo zabezpečiť konkurenčnú výhodu - príkladom whistle-blowera je stránka Wikileaks a jej zakladateľ Julian Assange, ktorý zverejnil utajované dokumenty vlády, alebo Edward Snowden, ktorý dal novinárom denníka The Guardian k dispozícii dokumenty o sledovacích aktivitách americkej NSA;
- *narúšanie funkcie kritickej infraštruktúry* – ide o zariadenia, služby a informačné systémy životne dôležité pre riadenie štátu. Ich narušenie by mohlo mať za následok kolaps fungovania štátu alebo jeho prvkov;
- *ekonomické a finančné aktivity* – vzhľadom na globalizáciu a závislosť sveta od ekonomického vývoja a finančných trhov. Cílené pôsobenie v tejto oblasti by mohlo mať za následok až oslabenie obranyschopnosti štátu;
- *podvratné politické akty* – sú to akty, ktorých cieľom je narušiť politickú stabilitu štátu a ohroziť tak plnenie funkcií štátu. Nositeľom politických podvratných aktivít sa v súčasnosti stávajú hlavne extrémistické strany a hnutia – subjekty, ktorých cieľom je zmena zriadenia štátu, napr. národno-osloboditeľské hnutia;

Hybridná vojna na našom území už dávno začala a kompetentné orgány v spolupráci s NATO a EÚ sa snažia hľadať efektívne a rýchle riešenia. Strategické dokumenty SR, ktoré sa zaoberajú problematikou kybernetickej bezpečnosti a hybridných hrozieb a vychádzajú aj z legislatívy EÚ a štandardov NATO sú:

- Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- Bezpečnostná stratégia SR, 2021,
- Biela kniha o obrane SR, 2016,
- Koncepcia kybernetickej bezpečnosti SR na roky 2021 až 2025,
- Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 - 2025,
- Akčný plán koordinácie boja proti hybridným hrozbám na roky 2022 – 2024, atď.

Použitie hybridných hrozieb na Slovensku už niekoľko rokov registrujú nielen príslušné authority, ale začína si ich uvedomovať aj verejnosť. Výraznejšie začali uvedené hrozby atakovať SR po anexii Krymu, vypuknutí pandémie koronavírusu, kedy sa výrazne spolarizovala spoločnosť a vrcholí dezinformáciami o dôvodoch napadnutia Ukrajiny Ruskom a vedením konfliktu medzi uvedenými štátmi. Ruský model vníma ľudskú myseľ ako veľké bojisko, na porážku ktorej treba využiť znalosti nielen z vojenskej oblasti, ale aj psychológie, medicíny,

biochémie, atď. Toto sociálne inžinierstvo síce nie je novým nástrojom ľudstva na ovládanie nepriateľa. Rôzne techniky boli používané už v staroveku, ale rýchly vývoj v oblasti vedy a techniky umožňuje v sociálnom inžinierstve využívať metódy a prostriedky, ktoré sme doteraz nepoznali, resp. nemali k dispozícii¹⁵⁷.

Záver

Vzhľadom na komplexnosť a multidisciplinárny charakter hybridnej vojny, jej metód, prostriedkov a cieľov, je podobne ako pri terorizme potrebné prijať jednotnú definíciu. Hybridná vojna a z nej vyplývajúce hybridné hrozby napriek tomu, že nie sú „novodobou zbraňou“ majú čím ďalej sofistikovanejší charakter, čo sťažuje odhalenie¹⁵⁸ či už štátnych alebo neštátnych aktérov.

Bývalý americký minister obrany Robert M. Gates už v roku 2009 na margo škály možných hrozieb v rámci príprav vyváženej stratégie Pentagonu uviedol, že v budúcnosti je možné očakávať ešte väčšie množstvo deštruktívnych nástrojov a taktiky, od sofistikovaných až po jednoduché, ktoré budú uplatňované v hybridných konfliktoch alebo ešte v komplexnejších formách boja.¹⁵⁹

Zoznam použitej literatúry

GLENN, W., R. 2009. Thoughts on Hybrid Conflict. In *Small Wars Journal*. 2009 [online] [cit. 2022. 4. 03.] Dostupné na internete: <http://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict>

HOFFMAN, G. F. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online] [cit. 2022. 4. 03.] Dostupné na internete:

http://www.pomac institute.org/images/stories/publications/potomac_hybridwar_010

IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 130-156. ISSN 1339 – 2751.

IVANČÍK, R. 2020. Analýza prístupov k definovaniu a vymedzeniu hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2020 : zborník príspevkov z 11. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika. 2020. s. 174-184. ISBN 978-80-8040-589-2.

¹⁵⁷JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2017

¹⁵⁸KURILOVSKÁ, L., HAJDÚKOVÁ, T. 2021. Dangers of Letting Children use Internet Services In: ICERI2021 [elektronický dokument] : 14th annual International Conference of Education, Research and Innovation.

¹⁵⁹SHANKER, T. 2009. Pentagon to Outline Shift in War Planning Strategy. In *The New York Times*, 2009

- IVANČÍK, R. 2021. Útočné kybernetické operácie ako súčasť hybridných hrozieb. In *Trilobit*, 2021, roč. 13, č. 3, 14 s. ISSN 1804-1795.
- JURČÁK, V. a kol. 2017. *Identifikácia príznakov vedenia hybridnej vojny*. Záverečná správa o riešení vedeckého projektu VV-A1. L. Mikuláš: AOS gen. M. R. Štefánika, 2017., 88 s.
- NBÚ. 2022. Hybridné hrozby. In *Krátky slovník hybridných hrozieb*, 2022. [online] [cit. 2022. 02. 20.] Dostupné na: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>
- KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2018, s. 90-98. ISBN 978-80-8054-773-8.
- KURILOVSKÁ, L., HAJDÚKOVÁ, T. 2021. Dangers of Letting Children use Internet Services In: ICERI2021 [elektronický dokument] : 14th annual International Conference of Education, Research and Innovation Valencia : IATED, 2021. - ISBN 978-84-09-34549-6. - ISSN 2340-1095. - S. 9384-9390.
- NOVOTNÝ, A. 2003. *NATO a medzinárodná bezpečnosť*. Nové Zámky : CROCUS, 2003. 125 s. ISBN 80-88992-65-6.
- SHANKER, T. 2009. Pentagon to Outline Shift in War Planning Strategy. In *The New York Times*, 2009. [online] [cit. 2023. 05. 15.] Dostupné na: <https://www.nytimes.com/2009/06/23/world/americas/23military.html>
- ZACHAR KUCHTOVÁ, J. 2022. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2022, s. 237-247. ISBN 978-80-8054-968-8.

Kontaktné údaje

PhDr. Róbert TOMÁŠEK

Externý doktorand

Katedra bezpečnosti a obrany

Akadémia ozbrojených síl generála M. R. Štefánika

Liptovský Mikuláš

E-mail: roberttomasek.tomasek@gmail.com

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. RNDr. Tatiana Hajdúková, PhD

Vybrané modely a systémy zamerané na komunikáciu

Jana Zachar Kuchtová

Anotácia

Komunikácia medzi človekom a technickým prostriedkom spočíva v zadaní príkazu, ktorý následne zariadenie splní. Príkaz môže byť v podobe textu, hlasového vstupu, gesta alebo iného interakčného signálu, v závislosti od použitého vstupného zariadenia a technológie. Tento príkaz je potom spracovaný počítačom, ktorý vykonáva príslušné operácie a poskytuje odpoveď alebo vykonáva žiadanú akciu. Komunikácia medzi človekom a počítačom môže byť obojsmerná, pričom počítač môže poskytovať informácie a odpovede na otázky človeka alebo vyžadovať ďalšie vstupy na presnejšie zadanie úlohy. Generatívnym pred-trénovaním jazykového modelu na rôznorodom korpuse neoznačeného textu je možné zvýšiť úroveň komunikácie medzi človekom a programom/technickým prostriedkom. Príspevok obsahuje informácie o konverzačných jazykových modeloch, ich vývoji, využití a potenciálnych výhodách a jeho cieľom je popísať vývoj modelov a systémov zameraných na konverzáciu so zameraním sa na ChatGPT, jazykový model vyvinutý spoločnosťou OpenAI.

Kľúčové slová

Komunikácia, jazykový model, generatívny predtrénovaný jazykový model, ChatGPT

Annotation

Communication between a human and a technical device involves giving a command that the device will subsequently execute. The command can take the form of text, voice input, gesture, or other interactive signals, depending on the input device and technology used. This command is then processed by a computer that performs the relevant operations and provides a response or carries out the requested action. Communication between a human and a computer can be bidirectional, with the computer providing information and answers to human questions or requiring further inputs for more precise task specification. By generatively pre-training a language model on a diverse corpus of unlabeled text, it is possible to enhance the level of communication between a human and a program/technical device. The post provides information about conversational language models, their development, usage, and potential benefits, with the aim of describing the evolution of models and systems focused on conversation, with a specific focus on ChatGPT, a language model developed by OpenAI.

Key words

Communication, language model, generative pre-trained language model, ChatGPT.

Úvod

Súčasná moderná ľudská civilizácia je výrazným spôsobom ovplyvnená prehlbujúcimi sa globalizačnými procesmi, ktoré sa vo väčšej či menšej miere prejavujú vo všetkých sférach života našej spoločnosti a ktoré podporujú dynamiku vývoja v jednotlivých oblastiach. Jednou z najdynamickejších sa vyvíjajúcich je oblasť informačných a komunikačných technológií.¹⁶⁰ To, že novodobé technológie a s nimi súvisiace vymoženosti sú oproti minulosti na vzostupe je

¹⁶⁰ IVANČÍK, R. 2022. Sociálne siete ako priestor pre šírenie konšpiračných teórií a dezinformácií. In *Národná a medzinárodná bezpečnosť 2022 – zborník vedeckých príspevkov z 13. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2022, s. 154

v dnešnej dobe už relatívne bežné. Limity, ktoré klasickú komunikáciu obmedzovali na bezprostredné stretnutie tvárou v tvár s konkrétnou osobou, už dávnejšie prestali existovať, pričom uveriteľnosť virtuálneho sveta a interaktivita sa neustále posúvajú k väčšej dokonalosti.¹⁶¹ Ak by dnes došiel niekto s novou značkou smartfónu, nešlo by o nič unikátne, čo by vzbudilo väčšiu pozornosť. Ak je však implementovaný jazykový model založený na technológii hlbokého učenia a neurónových sietí, ktoré doteraz bolo na vyspelej úrovni skôr filmovým motívom ako realitou, je prirodzené, že to nie len v odbornom ale aj laickom svete, vyvolá rozruch a získa si záujem spravidla vo všetkých oblastiach. Je nepochybné, že neurónové siete a modely hlbokého učenia existujú už dlhší čas¹⁶² ale keďže došlo k pokroku v algoritmoch a ku rozvoju výpočtových zdrojov nastal významný pokrok v oblasti spracovania prirodzeného jazyka a generatívnych modelov. V posledných piatich rokoch bol v doposiaľ nepoznanom kontexte sprístupnený verejnosti jazykový model za účelom komunikácie v širokej škále jazykov. Vzhľadom na to je cieľom tohto príspevku v teoretickej rovine popísať komunikáciu s ChatGPT s ohľadom na bezpečnosť a tiež uviesť praktické príklady z reálnej komunikácie s týmto nástrojom.

Vývoj modelov a systémov zameraných na konverzáciu

Pri vývoji modelov a systémov zameraných na konverzáciu je účelom simulovať a interagovať s ľudským jazykom. Ide najmä o spôsoby, akými daný nástroj dokáže spracovávať a interpretovať prirodzený jazyk aby sa čo najviac približoval ľudskému jazyku. V začiatkoch sa používali jednoduché preddefinované pravidlá určujúce, ako má systém reagovať na konkrétne podnety. Tento princíp bol veľmi obmedzený a nedokázal reflektovať na obsiahnejšie alebo zložitejšie vstupy používateľa. Neskôr sa využívala najmä štatistika, ktorá umožňovala vytvoriť štatistické modely pracujúce s veľkými databázami s určitou schopnosťou predikcie na základe pravdepodobnosti. V súčasnosti vývoj pokročil do podoby, v ktorej systémy využívajú rekurentné neurónové siete¹⁶³.

¹⁶¹ BACIGÁL, I. HAJDÚKOVÁ, T. HLAVIČKA, L. Bezpečnosť online komunikácie a ochrana dát 1. vyd. - Bratislava : Akadémia Policajného zboru v Bratislave, 2016. - s. 11 - ISBN 978-80-8054-690-8

¹⁶² Ich vývoj siaha až do 80. rokov 20. storočia.

¹⁶³ Ak chceme po napísaní slova vo vete predpovedať, aké ďalšie slovo bude v tejto vete nasledovať, potrebujeme zobrať do úvahy predchádzajúce slová. Musíme si teda nejakým spôsobom pamätať históriu. Bežné neurónové siete však takéto niečo neumožňujú. Spracúvajú všetky vstupy len ako navzájom nezávislé a nevedia teda do výstupu nijako premietnuť žiadne informácie z doterajších predchádzajúcich vstupov. Na takéto a podobné problémy však vieme použiť rekurentné neurónové siete (stretnete sa aj so skratkou RNN). Ich aplikácie nájdeme okrem spracovania textu a reči aj v analýze obrazu či rozpoznávaní hlasu. Hlavný rozdiel oproti klasickým dopreduším sieťam je v tom, že rekurentné siete povoľujú vo svojej architektúre cykly. Citované z internetu: <https://umelainteligencia.sk/rekurentne-neuronove-siete/>

Stručný prehľad významných modelov a systémov zameraných na konverzáciu:

Rok 1966 ELIZA

ELIZA bola jedným z prvých experimentálnych chatbotov. Bol to jednoduchý program, ktorý simuloval rozhovor s psychoanalytikom. ELIZA „odpovedala“ na základe vzorov vstupných viet. Išlo o prvý príklad primitívneho spracovania prirodzeného jazyka, ktorý fungoval tak, že spracovával odpovede používateľov na skripty - najznámejší z nich bol DOCTOR, ktorý dokázal zapojiť ľudí do rozhovoru, ktorý sa nápadne podobal na rozhovor s empatickým psychológom. ELIZA bola implementovaná pomocou jednoduchých techník priradovania vzorov Offsite Link¹⁶⁴. Viacerí jej používatelia ju brali príliš vážne a to aj po tom, čo im Weizenbaum (tvorca ELIZY) vysvetlil, ako to reálne funguje. *"Weizenbaum bol šokovaný, že jeho program brali vážne mnohí používatelia, ktorí mu otvorili svoje srdcia. Začal filozoficky uvažovať o dôsledkoch umelej inteligencie Offsite Link a neskôr sa stal jedným z jej popredných kritikov."*¹⁶⁵

Rok 1995 ALICE

ALICE (Artificial Linguistic Internet Computer Entity) bol chatovací program vyvinutý Richardom Wallaceom, ktorý sa snažil vytvoriť chatbota, ktorý by bol schopný imitovať konverzácie s človekom tým, že uplatňuje určité pravidlá zhodovania heuristických vzorov porovnávaní na vstup človeka. Inšpiroval ho Weizenbaumov program ELIZA.

Tento program získal trikrát Loebnerovu cenu¹⁶⁶ a síce nebol schopný zložiť Turingov test, pretože aj príležitostný používateľ často odhalil prítomnosť mechanických aspektov v krátkych rozhovoroch ale aj napriek tomu išlo v daných rokoch o najlepší program približujúci sa ľudskej komunikácii.

Rok 2006 Jabberwacky

Ide o chatbot, ktorý vyvinul britský programátor Rollo Carpenter. Používa strojové učenie a konverzácie s ním sú neštruktúrované, spontánne a interakcia s ním je zábavná. Vychádzal z technológií strojového učenia a kombinoval pravidlá a vzory zo vstupných dát s

¹⁶⁴ Hypertextový odkaz, ktorý vedie na stránku alebo zdroj mimo konkrétnej webovej lokality.

¹⁶⁵ NORMAN, J. Joseph Weizenbaum Writes ELIZA: A Pioneering Experiment in Artificial Intelligence Programming. [online] [cit. 05.05.2023]. Dostupné na internete: <https://www.historyofinformation.com/detail.php?id=4137>

¹⁶⁶ Súťaž, v ktorej sa na základe Turingovho testu posudzovala schopnosť programov umelej inteligencie simulovať ľudskú konverzáciu. ALICE vyhrala v roku 2000, 2001 a 2004.

generatívnym modelovaním. Aj napriek tomu, že v jeho odpovediach dochádza k nepresnostiam a oproti súčasnému pokroku je obmedzený, tvoril významnú úlohu pri rozvoji chatbotov.

Rok 2008 Google Voice Search

Na využitie služby VoiceSearch od Google bolo potrebné, aby používateľ zavolať na číslo vyhľadávacieho systému Google Voice, počkal na slová „*Povedzte svoje kľúčové slová vyhľadávania*“, ktoré následne povedal a počkal na aktualizáciu stránky, prípadne klikol na odkaz zobrazujúci stránku vyhľadávania. V súčasnosti je dostupná služba Google Assistant, ktorá funguje na princípe rozpoznávania reči a spracovania prirodzeného jazyka (viď rok 2016 Google Assistant).

Rok 2010 Siri

Siri je hlasový asistent vyvinutý spoločnosťou Apple. Siri je rozšíreným hlasovým asistentom pre mobilné zariadenia, ktorý umožňuje používateľom zadávať otázky a vykonávať úlohy pomocou hlasových príkazov. Z pohľadu popularity patrí Siri medzi jeden z najpoužívanějších hlasových asistentov.

Rok 2016 Google Assistant

Google Assistant je hlasový asistent vyvinutý spoločnosťou Google dostupný na rôznych platformách, ktorý ponúka široké spektrum funkcií a schopností, napríklad vyhľadávanie informácií - používateľ môže klásť otázky alebo hovoriť príkazy na ktoré mu Google Assistant poskytne odpovede, vykonávanie požadovaných úloh - ovládanie zariadení v domácnosti, naplánovanie udalostí, odosielanie správ, prehrávanie hudby a mnoho ďalších.

OpenAI GPT

Spoločnosť OpenAI sa zaoberá výskumom a nasadením umelej inteligencie v takom zmysle, aby umelá všeobecná inteligencia bola prínosom pre celé ľudstvo.¹⁶⁷

Princíp „inteligentnej“ komunikácie medzi človekom a strojom spočíva najmä v schopnosti strojového učenia, ktorým je možné doceliť aby sa ten naučil napríklad:

- Všeobecným znalostiam z rôznych oblastí (vedy, histórie, geografie, umenia, športu, zábavy a pod.),

¹⁶⁷ OpenAI. [online] [cit. 06.05.2023]. Dostupné na internete: <https://openai.com/about>

- jazykovým schopnostiam a gramatike v rôznych jazykoch,
- matematickým problémom a základným výpočtom,
- poskytovaníu rád a odpovedí na otázky týkajúcich sa bežného života, zdravia, technológií, vzťahov a ďalších tém,
- porozumeniu ľudskej reči a schopnosti konverzácie,
- schopnosti reagovať na rôzne otázky a poskytovať relevantné informácie a odpovede.

ChatGPT

Skratka GPT – Generative Pre-Trained Transformers v preklade znamená generatívne predškolené transformátory (ďalej len „*GPT*“).

GPT modely strojového učenia, ktoré sa používajú pri úlohách, ktoré súvisia so spracovaním prirodzeného jazyka a ktoré sú vopred pripravené na obrovské množstvo údajov. Z nich následne vytvárajú zmysluplné odpovede, ktoré reagujú na požiadavky používateľa aj napriek tomu, že na dané konkrétne reakcie neboli vopred programované. V zmysle historického vývoja umelej inteligencie zameranej na komunikáciu s ľuďmi ide, čo sa týka využiteľnosti umelej inteligencie v rámci komunikácie, o prelom v spracovávaní prirodzeného ľudského jazyka strojom. Pokrokovým aspektom je najmä okamžitá schopnosť reagovať na používateľa s doposiaľ najlepšou presnosťou.¹⁶⁸ ChatGPT predstavuje významný prelom v interakcii človeka s počítačom kvôli jeho pokročilej technológii AI/NLP¹⁶⁹.

OpenAI GPT (2018): Ide o model umelej inteligencie vyvinutý spoločnosťou OpenAI. Bol predstavený v roku 2018 a predstavuje významný krok v pred-trénovaných jazykových modeloch. ChatGPT je schopný generovať plynulý a koherentný text a môže byť použitý na rôzne úlohy, vrátane konverzácie. Trénovaný je na 117 miliónoch parametrov.

OpenAI GPT-2 (2019): Ide o vylepšenú verziu modelu ChatGPT. Bol predstavený v roku 2019. GPT-2 je schopný generovať text vo vysokej kvalite a je schopný odpovedať na otázky a poskytovať rôznorodé informácie. Model je open source a je trénovaný na viac ako 1,5 miliarde parametrov, aby sa generovala ďalšia sekvencia textu pre danú vetu. GPT-2 má 10-násobok parametrov a 10-násobok údajov svojho predchodcu GPT. Najčastejšie obmedzenia sú

¹⁶⁸ FAWAD, A. GPT-1 to GPT-4: Each of OpenAI's GPT Models Explained and Compared. [online] [cit. 06.05.2023]. Dostupné na internete: <https://www.makeuseof.com/gpt-models-explained-and-compared/>

¹⁶⁹ Artificial Intelligence/ Natural Language Processing je v preklade umelá inteligencia/ spracovanie prirodzeného jazyka

opakujúci sa text, nepochopenie vysoko odborných a špecializovaných tém a nepochopenie kontextových fráz.

OpenAI GPT-3 (2020): GPT-3 je vylepšená verzia modelu GPT-2. Je to jeden z najväčších a najvýkonnejších modelov umelej inteligencie. GPT-3 dokáže generovať texty vo vysokej kvalite, odpovedať na otázky a poskytovať rôznorodé informácie. Vyznačuje vysokou úrovňou jazykovej schopnosti a má veľký potenciál v rôznych aplikáciách. Trénovaný je na 175 miliárdach parametrov, čiže viac ako 10-násobku veľkosti GPT-2. Bol trénovaný na množine údajov s otvoreným zdrojovým kódom s názvom „*Common Crawl*“¹⁷⁰ a iných textoch z OpenAI, ako sú záznamy z Wikipédie. Dokáže spracovať viac špecializovaných tém ako GPT-2, ktorý mal problém pri úlohách v špecializovaných oblastiach. GPT-3 dokáže odpovedať na otázky, písať eseje, sumarizovať text, realizovať jazykový preklad a generovať počítačové kódy.¹⁷¹

OpenAI GPT-3.5: Je založený na GPT-3 ale disponuje menej parametrami (1,3 miliardy). Bol navrhnutý na ľudské hodnoty s cieľom urobiť systémy AI prirodzenejšie a bezpečnejšie pre interakciu s bežným používateľom. Aby bola interaktívnejšia, využíva podoblasť AI známu ako Reinforcement Learning from Human Preferences (RLHF), čo znamená, že ľudská spätná väzba sa používa na zlepšenie algoritmov strojového učenia.¹⁷²

OpenAI GPT-4: Je založený na zvýšenej bezpečnosti - 82 % menšia pravdepodobnosť odpovedania na nepovolený obsah, 40 % vyššiu pravdepodobnosť poskytovania vecnejších odpovedí v porovnaní s GPT-3.5. Dokáže použiť obrázky ako vstupy na rozpoznávanie objektov, oproti GPT-3.5, ktorá reaguje len na textové výzvy. Zároveň dokáže vygenerovať odpovede s viac ako 25 000 slovami.¹⁷³

¹⁷⁰ Projekt, ktorý sa zaoberá zhromažďovaním a sprístupňovaním veľkého množstva webových dát. Jeho cieľom je vytvoriť verejne dostupný a voľne použiteľný zdroj údajov o webe, ktorý môže byť využitý pre rôzne účely, ako je výskum, vývoj aplikácií a analýza dát. Funguje tak, že pravidelne prechádza internet a sťahuje webové stránky. Jeho crawler (robot) prechádza odkazy na stránkach, sleduje ich a stiahne ich obsah. Tieto dáta sú potom spracované, indexované a uložené do veľkej verejnej databázy, ktorá je následne dostupná pre používateľov.

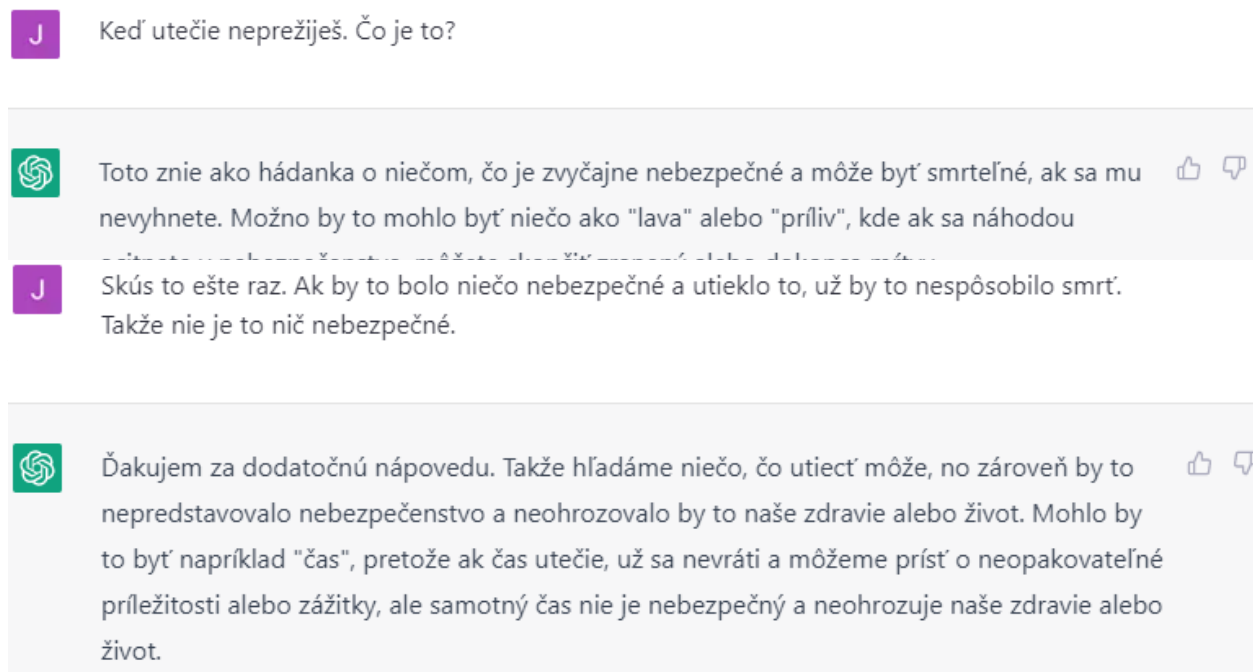
¹⁷¹ VU, K. GPT-2 (GPT2) vs. GPT-3 (GPT3): The OpenAI Showdown. [online] [cit. 07.05.2023]. Dostupné na internete: <https://dzone.com/articles/gpt-2-gpt2-vs-gpt-3-gpt3-the-openai-showdown>

¹⁷² IFFORT. [online] [cit. 07.05.2023]. Dostupné na internete: <https://blog.iffort.com/2023/03/31/gpt-3-vs-gpt-3-5/>

¹⁷³ KRAĽOVANSKÝ, J. Čo je to GPT-4, prečo spôsobil ošial a čím sa líši od pôvodného ChatGPT? [online] [cit. 07.05.2023]. Dostupné na internete: <https://www.techbox.sk/co-je-to-gpt-4-preco-sposobil-osial-a-cim-sa-lisi-od-povodneho-chatgpt>

Príklad fungovania ChatGPT na hádanke

Pokus bol realizovaný na položení vymyslenej hádanky:

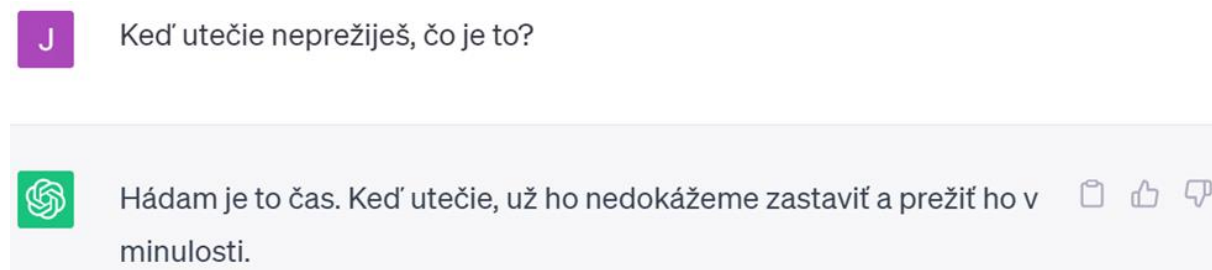


Obrázok 2 Správna odpoveď ChatGPT na hádanku

Zdroj: vlastné spracovanie

ChatGPT prvotne položenú hádanku zodpovedal nesprávne, pričom identifikoval a zameral sa na slovo „*neprežiješ*“. To si spojil s nebezpečnými situáciami, pri ktorých hrozí zranenie či smrť. Následne mu bolo používateľom vysvetlené, že jeho výsledok nie je správny a bol vyzvaný aby odpovedal znova.

Pokus s rovnakou hádankou bol zopakovaný o 2 mesiace neskôr, pričom ChatGPT na hádanku odpovedal na prvý pokus správne.



Obrázok 3 Opätovne správna odpoveď ChatGPT na hádanku

Zdroj: Vlastné spracovanie

Na použitom príklade je možné vidieť, akým spôsobom spracováva ChatGPT zadany text a jeho následnú schopnosť opraviť svoj výsledok. Zároveň sa môže zdať, že na základe strojového učenia správnu odpoveď naučil a zopakoval ju aj o dva mesiace.

Hádanka bola preto opäť niekoľko krát zopakovaná.



Aká je správna odpoveď na hádanku: Keď utečieš neprežiješ?



Správna odpoveď na hádanku "Keď utečieš, neprežiješ" závisí od kontextu hádanky, ktorý nie je jednoznačne definovaný. Existuje viacero možných odpovedí na túto hádanku, napríklad "dych", "čas" alebo "život". Tieto odpovede zdôrazňujú koncepty, ktoré sú dôležité pre naše prežitie a nie je možné ich zachytiť alebo vrátiť späť, ak raz prejdú.



Obrázok 4 Ďalšia odpoveď ChatGPT na hádanku
Zdroj: vlastné spracovanie

Všetky ďalšie opakované pokusy sa vzťahovali k odpovedi ChatGPT, že by mohlo ísť o dych, život alebo čas.

Záver

Účelom modelov a systémov zameraných na komunikáciu, ktoré sú založené na princípe spracovania prirodzeného jazyka a strojového učenia, je zlepšiť a zjednodušiť komunikáciu medzi ľuďmi a technickými zariadeniami, ktoré sú schopné na základe žiadosti používateľa poskytovať informácie, vykonávať úlohy, hľadať odpovede na otázky, riadiť zariadenia a mnoho ďalšieho. Ich využiteľnosť je možné nájsť v mnohých oblastiach, počnúc osobnými potrebami jednotlivcov, cez marketing, preklady, zdravotníctvo, cestovanie, analýzy údajov, predikcie a mnoho ďalšieho. Netreba však opomenúť aj odvrátenú stranu, ktorou je hroziace riziko zneužívania týchto modelov a systémov na hackerské útoky, podvody, phishing, získavanie informácií, ku ktorým by sa za iných okolností používateľ nemusel dostať a ktoré by mohol zneužiť na protispoločenskú činnosť, šírenie dezinformácií, prostredníctvom ktorých môže dôjsť k manipulácii s verejnou mienkou, propagandu, ktoré môžu vyústiť až do informačnej vojny: *„Informačná vojna je ponímaná aj ako ideologické ovplyvňovanie protivníka, pričom sa na tento účel využíva široké spektrum nástrojov, ako sú napríklad*

dezinformácie či propaganda, alebo diplomacia, vojenský nátlak a pod.“¹⁷⁴. Preto je nutné uvážiť bezpečnosť súvisiacu s touto formou elektronickej komunikácie skôr, ako je dostupná pre širokú verejnosť. Aj napriek tomu, že sa vývojári snažia odstrániť všetky bezpečnostné diery, až reálni používatelia odhalia ďalšie. Ak sú tí na „dobrej“ strane, v tom najlepšom prípade takúto zraniteľnosť nahlásia. Ak sú na strane „zlej“ nie len že takéto zraniteľnosti, ak už o nich vedia, môžu zneužiť ale mnohí sa zameriavajú priamo na ich vyhľadávanie. Ďalším neopomenuteľným rizikom je strata záujmu o vyhľadávanie relevantných informácií a spoliehanie sa len na informácie, ktoré poskytuje napríklad ChatGPT. V súčasnosti však stále preukazuje relatívne vysokú chybovosť, ktorú poukáže ako odpoveď. Okrem iného ChatGPT nie je nastavený na uvádzanie zdrojov, z ktorých čerpá a to ani po výzve používateľa aby takýto zdroj uviedol: „*Ospravedlňujem sa, ale ako strojový model nemám priamy prístup k internetu alebo možnosť poskytovať odkazy na konkrétne zdroje. Moje odpovede sú založené na znalostiach, ktoré som nadobudol počas svojho tréningu na základe obrovského množstva textových materiálov z rôznych zdrojov.*“¹⁷⁵ V zmysle uvedeného je preto záverom tohto príspevku, že vývoj modelov a systémov zameraných na komunikáciu je preukázateľne na vzostupe, pričom je možné stotožniť sa s tvrdením, že ide o prelomový pokrok vo využívaní umelej inteligencie na generatívne spracovanie prirodzeného jazyka. No napriek prvotnému entuziazmu je potrebné zohľadňovať v prvom rade bezpečnosť, existujúce obmedzenia jazykových modelov a ich schopnosti komunikovať s ľuďmi (aj napriek tomu, že navonok pôsobí už dnes veľmi dôveryhodne) a v neposlednom rade uvedomovanie si, že stále ide o komunikáciu s umelou inteligenciou, ktorá vykonáva úlohy na základe vstupných informácií a ich spracovania ale nikdy nenahradí tvorivosť, empatiu, kritické myslenie, súcitu a ďalšie vlastnosti typické pre človeka. Pravdepodobným smerovaním v tejto oblasti je nachádzanie vzájomnej spolupráce a synergického pôsobenia medzi ľuďmi a umelou inteligenciou, ktoré umožní ľudstvu dosiahnuť nové úrovne výkonu a produktivity. Veľký potenciál možno vnímať napríklad v oblasti ekológie, kde modely a systémy zamerané na komunikáciu môžu slúžiť ako podpora v riešení ekologických problémov. ChatGPT by mohol byť využitý na zlepšenie porozumenia a komunikácie v oblasti životného prostredia.

¹⁷⁴ IVANČÍK, R., MÜLLEROVÁ, J. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policijná teória a prax*, 2022, roč. 30, č. 3, s. 25

¹⁷⁵ Odpoveď ChatGPT na požiadavku uviesť zdroj, z ktorého čerpal pri svojej odpovedi

Zoznam použitej literatúry

BACIGÁL, I. HAJDÚKOVÁ, T. HLAVIČKA, L. Bezpečnosť online komunikácie a ochrana dát 1. vyd. - Bratislava : Akadémia Policajného zboru v Bratislave, 2016. - 175 s. - ISBN 978-80-8054-690-8.

FAWAD, A. GPT-1 to GPT-4: Each of OpenAI's GPT Models Explained and Compared. [online] [cit. 06.05.2023]. Dostupné na internete: <https://www.makeuseof.com/gpt-models-explained-and-compared/>

IFFORT. [online] [cit. 07.05.2023]. Dostupné na internete: <https://blog.iffort.com/2023/03/31/gpt-3-vs-gpt-3-5/>

IVANČÍK, R. Sociálne siete ako priestor pre šírenie konšpiračných teórií a dezinformácií. In *Národná a medzinárodná bezpečnosť 2022 – zborník vedeckých príspevkov z 13. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, 2022, s. 154-161. ISBN 978-80-8040-631-8.

IVANČÍK, R., MÜLLEROVÁ, J. Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. In *Policajná teória a prax : Teoreticko-praktický časopis*, 2022, roč. 30, č. 3, s. 22-42. ISSN 1335-1370.

KRALOVANSKÝ, J. Čo je to GPT-4, prečo spôsobil ošial a čím sa líši od pôvodného ChatGPT? [online] [cit. 07.05.2023]. Dostupné na internete: <https://www.techbox.sk/co-je-to-gpt-4-preco-sposobil-osial-a-cim-sa-lisi-od-povodneho-chatgpt>

NORMAN, J. *Joseph Weizenbaum Writes ELIZA: A Pioneering Experiment in Artificial Intelligence Programming*. [online] [cit. 05.05.2023]. Dostupné na internete: <https://www.historyofinformation.com/detail.php?id=4137>

OpenAI. [online] [cit. 06.05.2023]. Dostupné na internete: <https://openai.com/about>

Rekurentné neurónové siete. [online] [cit. 06.05.2023]. Dostupné na internete: <https://umelainteligencia.sk/rekurentne-neuronove-siete/>

VU, K. GPT-2 (GPT2) vs. GPT-3 (GPT3): The OpenAI Showdown. [online] [cit. 07.05.2023]. Dostupné na internete: <https://dzone.com/articles/gpt-2-gpt2-vs-gpt-3-gpt3-the-openai-showdown>

Kontaktné údaje

Jana Zachar Kuchtová

Katedra informatiky a manažmentu

Akadémia Policajného zboru v Bratislave

E-mail: jana.kuchtova@akademiapz.sk

Recenzenti:

Dr. h. c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

Názov: ***Bezpečnosť elektronickej komunikácie 2023***

Recenzenti: Dr.h.c. prof. Ing. Pavel Nečas, PhD., MBA

doc. Ing. Václav Friedrich, Ph.D., Ing. Paed. IGIP

doc RNDr. Tatiana Hajdúková, PhD.

Zostavil: JUDr. Jana Zachar Kuchtová

Vydala: Akadémia Policajného zboru v Bratislave

Počet strán: 182

Rok vydania: 2023

Vydanie: 1. vydanie

Jazyková úprava: Rukopis neprešiel jazykovou úpravou

Za obsah publikovaných príspevkov zodpovedajú autori

ISBN 978 – 80 8054 – 997 – 8

EAN 9788080549978