Radoslav Ivančík, Jana Müllerová

Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí[1]

Anotácia: Dezinformácie predstavujú v dnešnej dobe veľmi vážnu hybridnú hrozbu, ktorej závažnosť je umocnená dynamickým rozvojom a masívnym využívaním sociálnych sietí v posledných rokoch. Tie sa v súčasnej modernej informačnej spoločnosti stali bojiskom, na ktorom prebiehajú nepriateľské hybridné aktivity a na ktorom sa zvádza intenzívny boj o srdcia a mysle ľudí. Je to bojové pole, na ktorom možno pozorovať využívanie rôznych vojenských i nevojenských stratégií, taktík a nástrojov, akými sú okrem iných aj dezinformácie. Aj preto je primárnym cieľom autorov štúdie poukázať v rámci interdisciplinárneho vedeckého výskumu s využitím relevantných vedeckých metód na nebezpečenstvo zneužívania sociálnych sietí na šírenie dezinformácií ako hybridnej hrozby zameranej na ovplyvnenie myslenia a správania ľudí a ohrozenie demokratických procesov vo vyspelých demokratických krajinách.

Kľúčové slová: dezinformácie, sociálne siete, hybridné hrozby, internet, technológie.

Úvod

V úvodných dvoch dekádach nového tisícročia sa v súvislosti so šírením a stále intenzívnejším využívaním informačných a komunikačných technológií výrazne zmenil spôsob života a charakter ľudskej spoločnosti, ako aj fungovanie všetkých jej oblastí,[2] od politickej, cez sociálnu, ekonomickú, až po bezpečnostnú. S kontinuálne sa zvyšujúcou internetizáciou a informatizáciou spoločnosti, prudkým rozvojom a masívnym využívaním nielen technológií, ale aj rôznych informačných a komunikačných systémov, prostriedkov a zariadení,[3] a s tým súvisiacim dynamickým nástupom nových médií sa objavila aj nová škála možností ako najrôznejšie informácie vyhľadávať, prijímať, tvoriť a šíriť. Zároveň sa však objavila aj nová, pomerne široká škála možností ako moderné technológie, zariadenia alebo médiá zneužiť[4] a prostredníctvom nich šíriť klamlivé, zavádzajúce a skreslené informácie s cieľom ovplyvniť konanie ľudí a získať politický, ekonomický alebo iný profit. Zneužívanie moderných technológií, prostriedkov a médií a šírenie takýchto informácií tak

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

[2] FRIANOVÁ, V. 2020. Kybernetická bezpečnosť ako jeden z „vedľajších produktov“ investovania štátu do obrany, ľudských zdrojov, výskumu a vývoja, s. 17.

[3] S rozvojom informačných a komunikačných technológii zaznamenávame masívne rozšírenie mobilného pripojenia na internet (GPRS, UMTS, LTE, WiFi), pričom čoraz viac používateľov sa na internet pripája prostredníctvom rôznych mobilných zariadení (HAJDÚKOVÁ, HRUŠKA, 2018, s. 133).

[4] Bližšie pozri: KUCHTOVÁ, 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; ZACHAR, Š. 2018. Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2018, s. 217-224; KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2020, s. 78-87; KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018; ANDRASSY, V. – GREGA, M. 2015. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18; RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie*. Bratislava : Akadémia Policajného zboru, 2018, s. 161-173; alebo TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru, 2020, s. 146-152.

predstavuje veľmi nebezpečnú hrozbu, ktorá môže byť súčasťou hybridných hrozieb, resp. súčasťou hybridnej vojny.

Aj preto je primárnym cieľom autorov článku, s využitím relevantných metód kvalitatívneho teoretického interdisciplinárneho vedeckého výskumu (najmä analyticko-syntetickej metódy, kvalitatívnej, obsahovej a komparatívnej analýzy, metódy teoretického zovšeobecňovania poznatkov, ako aj metódy štúdia dokumentov a ďalších výskumných metód), prispieť k vedecko-odbornej diskusii o otázkach šírenia dezinformácií ako nástroja hybridnej vojny a hybridných hrozieb a úlohách, ktoré pritom zohrávajú sociálne siete.

1 Teoretické východiská skúmania hybridnej vojny a hybridných hrozieb

Termíny hybridné hrozby a hybridná vojna sú predmetom viacerých publikácií, štúdií alebo článkov, v ktorých sa zahraniční[5] alebo domáci[6] autori zaoberajú hybridnými hrozbami či hybridnou vojnou všeobecne alebo sa zameriavajú vo svojom výskume na ich jednotlivé aspekty. Z toho dôvodu je možné stretnúť sa s ich viacerými definíciami. Jedna z nich hovorí, že *„pojem hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi aktérmi, ktorej účelom je podkopať alebo poškodiť cieľ kombináciou otvorených a skrytých vojenských a nevojenských prostriedkov“*.[7]

Glenn definuje hybridné hrozby ako *„nepriateľa, ktorý súčasne a adaptabilne používa rôzne kombinácie politických, ekonomických, sociálnych a informačných prostriedkov a zároveň konvenčné, nepravidelné, katastrofické, teroristické a rozvratné kriminálne metódy vedenia boja“*.[8] Podľa Hoffmana *„hybridné hrozby zahŕňajú celú škálu konvenčných i nekonvenčných spôsobov boja a neregulárnej taktiky, ako aj kriminálne a teroristické činy, ktoré zahŕňajú neobmedzené násilie, nátlak, spoločenské nepokoje a rozvrat“*.[9]

Pod pojmom hybridná vojna možno chápať *„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*

[5] Bližšie pozri napríklad: VOERZIO, M. 2021. *Hybrid War: Attack on the West*. Garden City: Babelcube, 2021; DVORAK, J. 2016. *Complexity in Modern War: Examining Hybrid War*. Springfield: Missouri State University, 2016; GRISCIOLI, G. 2016. *Intelligence. The Hybrid War*. Roma: Aracne, 2016; MILLER, M. 2015. *Hybrid Warfare: Preparing for Future Conflict*. Montgomery: Air War College, 2015; alebo MURRAY, W. - MANSOOR, P. R. 2012. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge: Cambridge University Press, 2012

[6] Bližšie pozri napríklad: IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 130-156; 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. s. 174-184; ZACHARIDESOVÁ, N. 2021. Moderné spôsoby vedenia vojny. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 54-67; HAJDUKOVÁ, S. 2021. Konflikty v šedej zóne a hybridná vojna. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 68-82; LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, 2020, s. 102-105; JIRÁSKOVÁ, S. 2019. Ekonomická vojna ako jedna z podôb hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2019 – zborník príspevkov z 10. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika, s. 205-213; alebo LUKÁČOVÁ, J. 2017. Hybridné hrozby a ich vplyv na bezpečnostné prostredie – teória, vývoj a prax. In *Vojenské reflexie*, roč. 15, č. 1, s. 163-172. ISBN 1337-8163.

[7] Hybrid CoE. 2022. Hybrid Threats. In *Hybrid Centre of Excellence*, 2022.

[8] GLENN, R. W. *Thoughts on Hybrid Conflict*. In *Small Wars Journal*, 2009.

[9] HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007.

nepriateľa, chaos a rozvrat systému výkonu štátnej moci a oslabenie morálky spoločnosti".[10] Hybridnú vojnu možno tiež chápať ako *„súbor letálnych a neletálnych prostriedkov, ktoré štátny alebo neštátny aktér využíva k presadeniu svojich záujmov proti vôli iného aktéra. Hybridná vojna pritom kombinuje hneď niekoľko spôsobov vedenia boja: klasické vojenské operácie, operácie v kybernetickom priestore alebo kybernetické útoky, špionáž, šírenie nepravdivých informácií s cieľom pôsobiť na verejnú mienku nepriateľa a pod."*.[11]

Ďalšia z definícií hovorí, že *„hybridná vojna je ozbrojený konflikt vedený kombináciou nevojenských a vojenských prostriedkov s cieľom ich synergickým efektom prinútiť protivníka k vykonaniu takých krokov, ktoré by sám o sebe nevykonal. Aspoň jednou stranou konfliktu je štát. Hlavnú úlohu pri dosiahnutí cieľov vojny hrajú nevojenské prostriedky v podobe informačných a psychologických operácií, propagandy, ekonomických sankcií, embárg, kriminálnych aktivít, teroristických aktivít a iných subverzívnych aktivít podobného charakteru, ktoré sú vedené proti celej spoločnosti, najmä proti jej politickým štruktúram, orgánom štátnej správy a samosprávy, ekonomike štátu, morálke obyvateľstva a ozbrojeným silám"*.[12]

Dá sa tiež povedať, že *„v prípade hybridnej vojny ide o spôsob vedenia moderného ozbrojeného konfliktu. Konfliktu, ktorý nezačína výstrelom a už vôbec nie vyhlásením vojny. Konfliktu, o ktorom napadnutá spoločnosť spočiatku ani nevie, dokonca ani netuší alebo si nepripúšťa, že bola napadnutá a nachádza sa vo vojne. Ide o dynamickú kombináciu vojenských, politických, diplomatických, ekonomických, humanitárnych, diverzných, teroristických a kriminálnych aktivít realizovaných štátnymi i neštátnymi aktérmi, pravidelnými i nepravidelnými formáciami, pri využití propagandy a realizácii informačných, kybernetických a psychologických operácií"*.[13]

V súvislosti s hybridnou vojnou sa pomerne často spomína informačná vojna. V jej prípade ide o všeobecný pojem zahŕňajúci niekoľko typov vedenia bojovej činnosti, ktoré majú určité spoločné vlastnosti. Ako už vyplýva z názvu, dôraz je kladený na informácie, ktoré sú v tomto type konfliktu (vojny) brané ako kľúčový element, nutný k dosiahnutiu víťazstva. Rôzni autori vysvetľujú pojem informačná vojna rôznymi spôsobmi, a preto podobne ako pri hybridnej vojne, aj v prípade informačnej vojny je možné sa stretnúť v odbornej literatúre s viacerými definíciami.[14]

Jedna z najvšeobecnejších a zrejme aj najjednoduchších a zároveň najčastejšie používaných definícií charakterizuje informačnú vojnu ako *„boj o kontrolu nad informačnými aktivitami protivníka a snahu uchrániť svoje vlastné"*.[15] Iná, komplexnejšia definícia hovorí, že: *„Informačná vojna predstavuje široké spektrum aktivít, ktorých nástrojom alebo cieľom sú informácie a informačné technológie. Medzi tieto aktivity patrí napríklad šírenie dezinformácií, psychologické operácie a kybernetické útoky – narušovanie komunikačných sietí a prieniky do nich za účelom získania strategických informácií. Tieto aktivity môžu prebiehať aj v čase mieru bez toho, aby museli vôbec nejakému konfliktu predchádzať.*

---

[10] MANKO, O. - MIKHIEIEV, Y. 2018. Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. In *Connections*, 2018, s. 13.
[11] DANYK, Y. – MALIARCHUK, T. – BRIGGS, C. 2017. Hybrid War: High-tech, Information and Cyber Conflicts. In *Connections*, 2017.
[12] KŘÍŽ, Z. – SCHEVCUK, Z. – ŠTEVKOV, P. 2015. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy*. Ostrava: Jagelo 2000, 2015, s. 8.
[13] IVANČÍK, R. 2016. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 148.
[14] IVANČÍK, R. 2021. Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti. In *Politické vedy*, 2021, roč. 24, č. 1, s. 140.
[15] BAYER, M. 2006. Strategic Information Warfare: An introduction. In Cyberwar, Netwar and the Revolution in Military Affairs, 2006, s. 36.

Hlavným cieľom informačnej vojny nie je protivníka oslabiť zvonku, ale oslabiť, dezorientovať a destabilizovať ho zvnútra".[16]

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. Možno ju preto charakterizovať ako *„koncepciu zameranú na získanie informačnej dominancie (prevahy)".*[17] Informačná dominancia je pritom definovaná ako *„schopnosť zhromažďovať, spracovávať a šíriť informácie, zatiaľ čo sa využívajú alebo potláčajú snahy protivníka robiť to isté".*[18] Z uvedených definícií jasne vyplýva, že informačná vojna je užší pojem ako hybridná vojna.

2 Dezinformácie ako hybridná hrozba

Dezinformácie, ako vyplýva z vyššie uvedeného, predstavujú neoddeliteľnú súčasť hybridných hrozieb, nakoľko účelom ich využitia v hybridnej vojne je pôsobenie na protivníka s cieľom oslabiť, dezorientovať, destabilizovať, narušiť jeho politické štruktúry, fungovanie štátnych i neštátnych orgánov, jeho bezpečnosť, obranu, ekonomiku, schopnosť reakcie na hrozby, a tiež ovplyvniť verejnú mienku a morálku obyvateľstva.

V úzkej súvislosti s pojmom dezinformácie je potrebné bližšie sa pozrieť aj na ďalšie pojmy ako sú falošné správy (niekedy označované ako „fake news") a propaganda. Tieto dva pojmy sa vo verejnej diskusii pomerne často zamieňajú alebo používajú ako synonymá. Niektorí autori považujú za falošné správy všetky správy, ktoré nie sú postavené na faktoch, ale napriek tomu sú vydávané za pravdivé spravodajstvo,[19] alebo za správy, ktoré popierajú zásady kvalitnej a objektívnej žurnalistiky.[20] Ďalší autori zase rozlišujú médiá, ktoré šíria falošné správy a tzv. politické médiá, ktoré spravodajstvo upravujú takým spôsobom, že sa snažia nastoliť politickú agendu spriaznenej politickej strany či hnutia.[21] Silverman zasa tvrdí, že falošné správy predstavujú spravodajstvo, ktoré sa nezakladá na pravde a je tvorené za účelom finančného zisku. Motivácia k zisku je kľúčová, pretože pri absencii finančného motívu ide o propagandu.[22] Propagandu potom možno charakterizovať ako šírenie falošných správ, ktoré nie sú vyrábané s cieľom ekonomického zisku, ale sú to informácie, ktoré majú prinútiť myslieť či konať určitým spôsobom. Väčšinou sa spája s politickými, náboženskými alebo ideologickými cieľmi.

Termín dezinformácie zastrešuje obe skupiny falošných správ bez ohľadu na to, či ide o šírenie propagandy alebo o falošné správy publikované s cieľom pritiahnuť pozornosť čitateľov, a tým zvýšiť zisky z predaja reklamy a inzercie. Východisko predstavuje definícia pojmu dezinformácie, ktorú pripravila a predstavila nezávislá skupina odborníkov pre falošné správy a online dezinformácie. Podľa tejto expertnej skupiny: *„Dezinformácie predstavujú všetky formy falošných, podvodných, nepravdivých a zavádzajúcich správ, ktoré sú vytvárané,*

---

[16] HALPIN, E. – TREVORROW, P. – WEBB, D. – WRIGHT, S. 2006. *Cyberwar, Netwar and the Revolution in Military Affairs*, s. 79.

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

[18] US DoD. 2000. *United States Department of Defense: Joint Vision 2020*.

[19] ALLCOTT, H. – GENTZKOW, M. 2017. Social Media and Fake News in the 2016 Election. In *Journal of Economic Perspectives*, 2017, roč. 31, č. 2, s. 212.

[20] BAYM, G. 2005. The daily show: discursive integration and the reinvention of political journalism. In *Political Communication*, 2005, roč. 22, č. 3, s. 261.

[21] VARGO, C. J. a kol. The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. In *New Media & Society*, 2017, roč. 20, č. 5, s. 2031.

[22] SILVERMAN, C. 2016. This analysis shows how viral fake election news stories outperformed real news on Facebook. In *Buzzfeed*, 2016.

prezentované a šírené s úmyslom spôsobiť verejnú škodu alebo získať profit".[23] Do tohto vymedzenia pojmu ale nespadajú neúmyselné chyby pri informovaní, ani politická satira.

Podobnú definíciu možno nájsť v Krátkom slovníku hybridných hrozieb Národného bezpečnostného úradu: *„Dezinformácia je overiteľne nepravdivá, zavádzajúca alebo manipulatívne podaná informácia, ktorá je zámerne vytvorená, prezentovaná a šírená s jednoznačným úmyslom klamať alebo zavádzať, spôsobiť nejakú ujmu alebo zabezpečiť nejaký zisk (napríklad hospodársky či politický). Dezinformácia často obsahuje element, ktorý je zjavne pravdivý, čo jej dodáva na dôveryhodnosti a môže tak skomplikovať jej odhalenie. Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira a paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené"*.[24]

V slovenskom prostredí sú pomerne často využívané aj ďalšie definície nachádzajúce sa v príslušných slovníkoch. Napríklad v Slovníku cudzích slov je dezinformácia vymedzená veľmi stručne ako „*nesprávna, vedome skreslená informácia*".[25] V Slovníku súčasného slovenského jazyka je už dezinformácia definovaná obšírnejšie ako „*nepravdivá, vedome skreslená informácia, ktorej cieľom je ovplyvniť určitú skupinu ľudí, prípadne celú populáciu*".[26] V anglofónnom jazykovom prostredí sa môžeme stretnúť tiež s viacerými vymedzeniami pojmu dezinformácia. Napríklad v Oxfordskom anglickom výkladovom slovníku je dezinformácia definovaná stručne ako „*úmyselne poskytovaná falošná informácia*",[27] v Cambridgeskom slovníku anglického jazyka ako „*nepravdivá informácia šírená s cieľom oklamať ľudí*",[28] a v MacMillanovom výkladovom slovníku ako „*nepravdivá informácia, ktorá má presvedčiť ľudí, aby verili niečomu, čo v skutočnosti nie je pravda*".[29]

Hoci sa v niektorých médiách objavujú informácie o dezinformáciách ako o novej bezpečnostnej hrozbe, nie je to tak. Dezinformácie v žiadnom prípade nie sú výdobytkom 21. storočia alebo súčasnej informačnej spoločnosti. O stratégii nepriameho boja s využitím klamstva a falošných, podvodných správ písal už v Číne v 6. storočí p. n. l. Sun Tzu vo svojom diele Umenie vojny.[30] Učebnicové príklady využívania dezinformácií v praxi môžeme nájsť aj v antickom Grécku z obdobia grécko-perzských vojen, keď napríklad aténsky vojvodca Temistokles v niektorých bitkách porazil perzského kráľa Xerxesa s pomocou falošných správ poslaných po zdanlivo ujdených otrokoch. Ďalším dobrým príkladom využívania dezinformácií z dávnych čias môže byť stratégia, ktorú využíval mongolský dobyvateľ Džingischán. Ten pred útokom posielal na nepriateľské územie špiónov, ktorí sa infiltrovali medzi obyvateľstvo a šírili falošné správy o blížiacej sa obrovskej a krutej mongolskej armáde. Týmto spôsobom sa snažil už vopred oslabiť a demoralizovať nepriateľa a získať výhodu. Ako sa potvrdilo, táto taktika bola úspešná, keďže bol schopný vyhrať viacero bitiek, v ktorých nepriateľ bol v značnej presile.[31] Pochopiteľne, vytváranie a šírenie

---

[23] EK. 2018. *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*, s. 10.
[24] Krátky slovník hybridných hrozieb. 2022. *Dezinformácia*.
[25] Slovník cudzích slov. 2015. *Dezinformácia*.
[26] Slovník súčasného slovenského jazyka. 2015. *Dezinformácia.*
[27] Oxford Learner´s Dictionary. 2021. *Disinformation*.
[28] Cambridge Dictionary. 2021. *Disinformation*.
[29] MacMillan Dictionary. 2021. *Disinformation*.
[30] Sun Tzu (v 6. st. p. n. l.) bol čínsky generál, filozof, stratég a taktik, ktorého dielo *Umenie vojny* malo veľký vplyv na východné i západné vojenské myslenie a mnohí slávni vojvodcovia sa inšpirovali týmto dielom. Dodnes sa študuje na mnohých vojenských akadémiách. Generál, známy aj ako Majster Sun, sa pritom vo svojom diele oveľa viac ako na samotný ozbrojený zápas, boj, zameriava na alternatívy k bitke, ako sú lúpež, zdržiavanie, použitie špiónov, klamstiev a falošných, podvodných informácií alebo vytváranie a udržiavanie aliancií.
[31] DAVISON, W. P. 1971. Some Trends in International Propaganda. In *The Annals of the American Academy of Political and Social Science*.

najrôznejších dezinformácií sa úspešne využívalo aj v ďalších, známych, či menej známych vojnách a ozbrojených konfliktoch vrátane dvoch najväčších – v 1. a 2. svetovej vojne.

To, čo sa v prvých dvoch dekádach tretieho milénia zmenilo, to sú prostriedky využívané na šírenie dezinformácií. 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. Sociálne siete vytvorili nový priestor, v ktorom si ľudia vytvárajú názory na dianie okolo seba – na rôzne udalosti, osobnosti, procesy, politiky atď. Zároveň je to priestor, v ktorom je pomerne ľahké podsúvať ľuďom rozličné skreslené, vymyslené, nepravdivé informácie či informácie vytrhnuté z kontextu, a tým ich ovplyvňovať želaným smerom.

Šírenie dezinformácií je považované za hybridnú bezpečnostnú hrozbu predovšetkým preto, že podrývajú dôveru občanov v demokratické inštitúcie a demokratické procesy a šíria nenávistnú ideológiu. Viacerí autori sa zhodujú v tom, že veľké množstvo dezinformácií a dezinformačných webových stránok prezentuje a šíri najmä krajne pravicovú ideológiu.[32] Tento fenomén sme mohli pozorovať napríklad pri voľbách vo viacerých európskych štátoch, kedy dezinformačné stránky v rôznych krajinách podporovali krajne pravicových kandidátov a šírili dezinformácie o ich protikandidátoch, migrantoch a pod. V Holandsku to bol Geert Wilders, vo Francúzsku Marine Le Pen a v Nemecku zasa predstavitelia strany Alternatíva pre Nemecko. Z pohľadu šírenia násilnej propagandy je dominantným aktérom predovšetkým Islamský štát, ktorý je mimoriadne efektívny pri šírení naratívov na sociálnych sieťach.[33]

Príkladom štátneho aktéra, ktorý dezinformácie využíva vo veľkej miere pre svoje politické ciele, je Rusko, napríklad pri šírení dezinformácií v rámci konfliktu na Ukrajine[34] alebo pri šírení dezinformácií a propagandy v pobaltských krajinách a v Škandinávii.[35] Relatívne dobre je zmapovaných aj viacero mechanizmov, ktoré využíva ruská propaganda či už pri ovplyvňovaní demokratických procesov v západných krajinách alebo pri šírení dezinformácií a využívaní platených diskutérov. Šírenie ruskej propagandy je problémom identifikovaným nielen v jednotlivých európskych krajinách, ale aj na úrovni Európskej únie (ďalej len „EÚ“ alebo „Únia“) ako celku. Podľa Správy o strategickej komunikácii EÚ sa ruská propaganda týka šírenia viacerých meta-naratívov v kombinácii s konšpiračnými teóriami. Podsúvané meta-naratívy sa síce podľa predmetnej správy do veľkej miery menia v čase, ale konštantou je prezentovanie Západu na jednej strane ako agresívnej a expanzívnej entity, na druhej strane ako entity stojacej na pokraji kolapsu. Za najvýraznejších šíriteľov dezinformácií sa považujú portály Russia Today a Sputnik. Na šírenie dezinformácií sú využívané aj siete lokálnych médií a spriatelených think-tankov v cieľových krajinách.[36]

Dezinformácie, ako už bolo uvedené vyššie, predstavujú hybridnú bezpečnostnú hrozbu preto, že môžu ovplyvniť demokratické procesy v krajinách. V Spojených štátoch amerických stále prebieha niekoľko vyšetrovaní, ktoré majú za cieľ objasniť, akú úlohu zohralo šírenie dezinformácií na sociálnych sieťach v prezidentských voľbách v rokoch 2016 a 2020. Taktiež existujú dôvodné podozrenia, že časť obyvateľov Spojeného kráľovstva,

---

[32] BENNETT, L. – LIVINGSTON, S. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. In *European Journal of Communication*, 2018, roč. 33, č. 2, s. 122-139

[33] PRIER, J. 2017. Commanding the Trend: Social Media as Information Warfare. In Strategic Studies Quarterly, 2017, roč. 11, č. 4, s. 50-85

[34] DANYK, Y. – MALIARCHUK, T. – BRIGGS, C. 2017. Hybrid War: High-tech, Information and Cyber Conflicts. In *Connections*, 2017

[35] ARO, J. 2016. The Cyberspace War: Propaganda and Trolling as Warfare Tools. In *European View*, 2016, roč. 15, č. 1, s. 121-132

[36] KOVANIČ, M. 2017. Dezinformácie a ruská propaganda ako bezpečnostné hrozby. In *Bezpečnostní teorie a praxe*, 2017, č. 2, s. 125-126

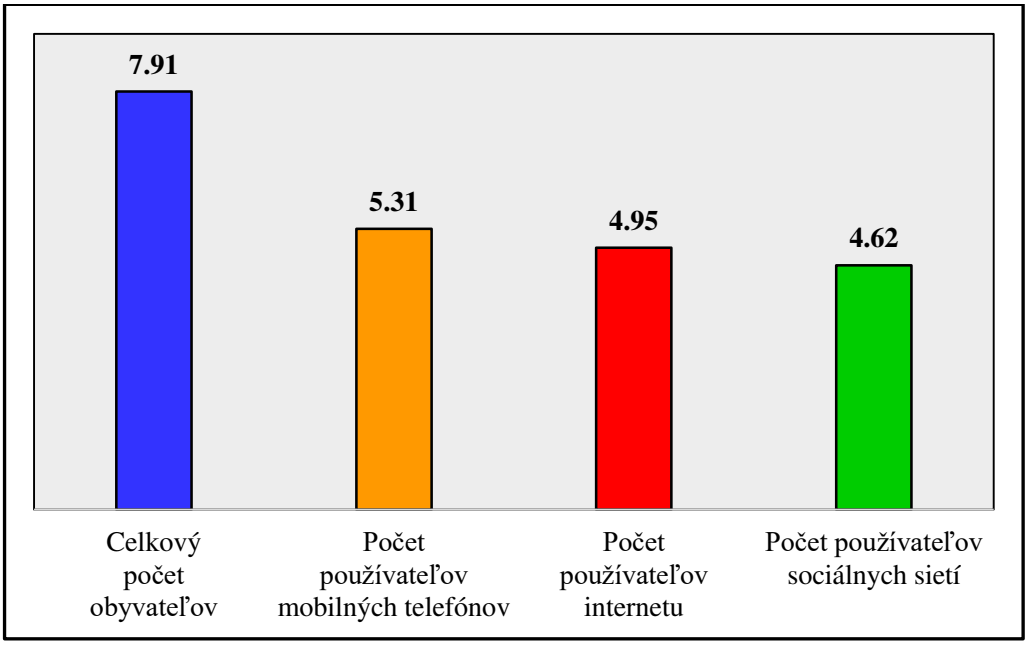
ktorá hlasovala za vystúpenie z Únie, tak urobila na základe rôznych nepravdivých informácií šírených primárne cez sociálne siete. Výsledok referenda bol tesný, 52 % za a 48 % proti vystúpeniu z EÚ, takže je možné sa domnievať, že nepravdivé informácie zohrali veľmi významnú, ak nie rozhodujúcu úlohu. Je dokázané, že vlastných obyvateľov, okrem iných politikov, klamali napríklad súčasný premiér Johnson alebo europoslanec Farage.[37]

Dezinformácie navyše podkopávajú dôveryhodnosť klasických informačných kanálov. Dnes je totiž veľmi jednoduché vytvoriť si stránku, ktorá sa tvári ako seriózny spravodajský server, avšak jej skutočným cieľom je šírenie dezinformácií, a to buď za účelom zisku z reklamy a inzercie alebo z politických, ideologických či náboženských dôvodov. Takéto webové stránky často šíria rôzne konšpiračné teórie a nedodržiavajú zásady serióznej žurnalistiky. Tým, že sami seba prezentujú ako dôveryhodné médiá, podrývajú dôveru ľudí v klasické seriózne spravodajstvo.

3 Dezinformácie a sociálne siete

Ako sme už uviedli vyššie, šírenie dezinformácií nie je fenomén, ktorý vznikol v 21. storočí. V skutočnosti platí, že tento fenomén je prakticky taký starý, ako ľudstvo samé. To, čo sa ale zásadne zmenilo, je spôsob, akým sú dezinformácie šírené. Zásluhu na tom má už spomínaný progres pri zavádzaní a využívaní rýchleho internetu, prehlbujúca sa informatizácia spoločnosti, masívne využívanie informačných a komunikačných technológií, systémov a prostriedkov, a v neposlednom rade fakt, že prakticky každý ich používateľ má neobmedzený prístup k informáciám 24 hodín denne 7 dní v týždni. Tento pokrok však prináša so sebou okrem mnohých pozitív aj viaceré negatíva, napríklad tie v podobe prijímania a šírenia dezinformácií.

Graf 1 Prehľad o používateľoch mobilných telefónov, internetu a sociálnych sietí v roku 2022 na celom svete (v mld.)



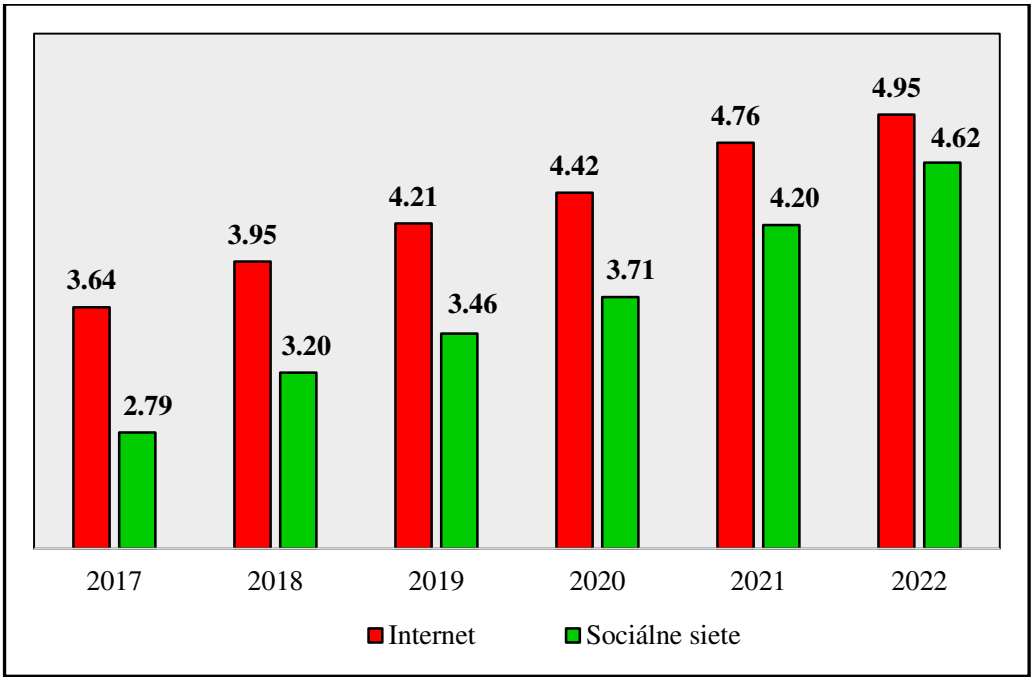
[37] TA3. 2017. Britský šéf diplomacie Johnson vraj klamal o výhodách Brexitu. In *TA3.com*, 2017; ONDERČANIN, L. 2019. Farage a Johnson: Klamali o brexite, opustili loď a opäť sú úspešní. In *Sme*, 2019; alebo TASR. 2019. Boris Johnson čelí žalobe za zavádzanie verejnosti o brexite. In *Tlačová agentúra Slovenskej republiky*, 2019.

Zdroj: DataReportal, 2022.[38]

Veľkú zásluhu na tom, že dezinformácie sú považované za stále väčší a naliehavejší bezpečnostný problém má práve rozvoj internetu a využívanie sociálnych sietí, ktoré predstavujú výborný nástroj na ich šírenie. Sociálne siete spájajú obrovské počty ľudí z rôznych častí celého sveta a umožňujú im komunikovať a navzájom si vymieňať informácie. Mobilný telefón používa dnes cca 5,31 miliardy obyvateľov, čo predstavuje viac ako dve tretiny (67,1 %) svetovej populácie, internet používa približne 4,95 miliardy ľudí, teda viac ako tri pätiny (62,5 %) svetovej populácie, a počet aktívnych používateľov sociálnych sietí dosahuje zhruba 4,62 miliardy, čo predstavuje podiel na celkovom obyvateľstve planéty na úrovni 58,4 % (graf 1). Sociálne siete používa pritom prostredníctvom mobilného telefónu až 95 % ich užívateľov.

O tom, aký dynamický je rast používateľov internetu a sociálnych sietí svedčí fakt, že za ostatných päť rokov celosvetovo stúpol počet používateľov internetu o viac ako jednu tretinu (o 36 %). Kým v roku 2017 používalo internet zhruba 3,64 miliardy ľudí, tak v roku 2022 to už bolo približne 4,95 miliardy. Rast používateľov sociálnych sietí je ešte dynamickejší, nakoľko stúpol v hodnotených rokoch o takmer dve tretiny (o 65,6 %). Kým v roku 2017 používalo sociálne siete približne 2,79 miliardy ľudí, v roku 2022 sú to už zhruba 4,62 miliardy (graf 2). Z nich jeden užívateľ strávi na sociálnych sieťach priemerne denne 2 hodiny a 27 minút a priemerne mesačne využíva 7,5 rôznych sociálnych sietí.[39]

Graf 2 Prehľad rastu používateľov internetu a sociálnych sietí v rokoch 2017 až 2022 (v mld.)



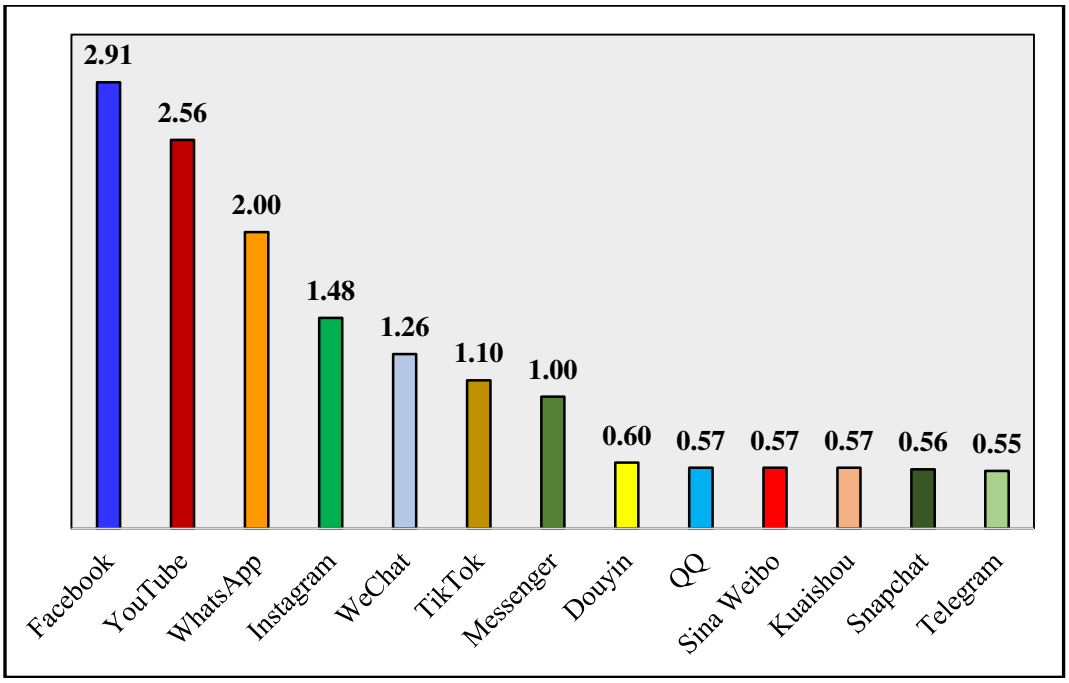
Zdroj: DataReportal, 2022[40]

Celosvetovo najpopulárnejšiu sociálnou sieťou je Facebook, ktorý v januári 2022 využívalo približne 2,91 miliardy aktívnych používateľov, druhou v poradí je YouTube s 2,56 miliardou aktívnych používateľov a treťou WhatsApp, ktorú v súčasnosti aktívne

[38] DR. 2022. Global Digital Overview. In *DateReportal*, 2022.
[39] DR. 2022. Global Digital Overview. In *DateReportal*, 2022.
[40] DR. 2022. Global Digital Overview. In *DateReportal*, 2022.

používajú cca dve miliardy ľudí. Medzi ďalšie populárne sociálne siete, ktoré majú viac ako jednu miliardu aktívnych používateľov patria Instagram, WeChat, TikTok a Messenger. S viac ako pol miliardou aktívnych používateľov sa môžu pochváliť sociálne siete Douyin, QQ, Sina Weibo, Kuaishou, Snapchat a Telegram. (graf 3).

Graf 3 Prehľad sociálnych sietí s najväčším počtom aktívnych používateľov v roku 2022 (v mld.)



Zdroj: DataReportal, 2022[41]

Takmer neobmedzený dosah v kombinácii s vysokou rýchlosťou informačného toku, nízkych nákladov a dostupnosti 24/7 vytvára ideálne podmienky na to, aby sa dezinformácie šírili virálne.[42] Hoci klasické spravodajské médiá ešte stále predstavujú pre väčšinu ľudí primárny zdroj informácií, skutočnosť, že stále viac ľudí využíva sociálne siete najmä ako zdroj na sledovanie nových udalostí vo svete a doma, ešte umocňuje naliehavosť hrozby, akú dezinformácie šírené na sociálnych sieťach predstavujú. Sociálne siete navyše vytvárajú sociálne bubliny. To znamená, že ľudia majú tendenciu spájať sa na sociálnych sieťach s ľuďmi s podobným svetonázorom, čím následne vytvárajú tzv. uzavreté homofilné skupiny, kde sa jednotliví ich členovia navzájom utvrdzujú vo svojich názoroch.[43] Ľudia tak postupne prestávajú vnímať širšie súvislosti a kriticky uvažovať o argumentoch, ktoré sa v takýchto skupinách používajú. Problém nastáva najmä vtedy, keď sa v predmetných skupinách začnú šíriť dezinformácie.

Všetky vyššie uvedené faktory spôsobujú, že sociálne siete sa stali nástrojom na mobilizáciu, šírenie rôznych naratívov, vedenie hybridných operácií a v niektorých prípadoch dokonca aj nástrojom pre vedenie bojových operácií v skutočnom svete. Štátni aj neštátni aktéri začínajú v čoraz väčšej miere používať sociálne siete ako nástroj na ovplyvňovanie správania, postojov, nálad a názorov svojej cieľovej skupiny. Tento trend

[41] DR. 2022. Global Digital Overview. In *DateReportal*, 2022
[42] BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 69
[43] PRIER, J. 2017. Commanding the Trend: Social Media as Information Warfare. In *Strategic Studies Quarterly*, 2017, roč. 11, č. 4, s. 59

sa označuje ako weaponizácia sociálnych sietí, čo znamená, že sa menia na bojisko, kde je na cieľovú skupinu útočené prostredníctvom dezinformácií.[44]

Používatelia sociálnych sietí si riziko, ktoré z toho plynie, často ani neuvedomujú a plne dôverujú online prostrediu. Domnievajú sa, že keď kontrolujú okruh ľudí, ktorí majú prístup k ich obsahu, že majú pod kontrolou aj informácie, ktoré sa k nim dostávajú. Dezinformácie sa najčastejšie šíria prostredníctvom dvoch sociálnych sietí – Facebook a Twitter.

Facebook je, ako už bolo uvedené vyššie, najväčšia a najobľúbenejšia sociálna sieť na svete, a preto je hlavným cieľom prakticky všetkých dezinformačných kampaní. Facebook je na rozdiel od Twitteru založený na podstatne osobnejšom kontakte medzi požívateľmi, pretože oni sami rozhodujú o tom, kto sa stane ich priateľom, a tým získa prístup k ich obsahu. Používatelia potom väčšinou pristupujú nekriticky k informáciám, ktoré ich kontakty na Facebooku šíria a keďže ich pokladajú za dôveryhodné, zväčša si tieto informácie ďalej neoverujú. Ďalším spôsobom, akým sa dezinformácie môžu k používateľovi na Facebooku dostať, sú príspevky publikované rôznymi facebookovými stránkami.

Používateľ si ich vyberá na základe svojho vlastného rozhodnutia, a to väčšinou vtedy keď:

- stránka od začiatku jasne šíri dezinformácie, avšak používateľ s týmto druhom správ sympatizuje a zdieľa názory stránky,
- stránka spočiatku produkuje neutrálny obsah, s ktorým sa používateľ stotožňuje, rozhodne sa ho sledovať, no v ďalšej fáze táto stránka začne šíriť dezinformácie, s cieľom následne ovplyvniť postoje, názory a hodnoty používateľa, ktorý s takýmto typom informácií pôvodne nesympatizoval.[45]

Najväčšiu zásluhu na šírení dezinformácií majú tie príspevky, ktoré sa aj vďaka používanému algoritmu stávajú virálne. Facebook v podstate ponúka tri možnosti operácií, ktoré môžu byť využité k vedeniu hybridnej vojny:

- cielené získavanie osobných dát používateľov,[46] ktoré sú neskôr využívané k šíreniu dezinformácií, ktorých obsah je prispôsobovaný preferenciám používateľa;
- produkovanie obsahu;
- umelé šírenie obsahu (realizované spravidla pomocou strojov, nie skutočných používateľov).

Twitter síce nie je taký populárny ako Facebook, aktuálne má približne 436 miliónov aktívnych užívateľov,[47] no aj napriek tomu sa stáva jedným z hlavných cieľov predovšetkým pre politickú manipuláciu, pretože ho vo veľkom využívajú najmä západní politickí predstavitelia, tradičné médiá a svetoví myslitelia. Vďaka funkcii, ktorá umožňuje sledovať jednotlivé témy v podobe vlákien, sa pre mnohých ľudí, predovšetkým v Spojených štátoch amerických a v západnej Európe, stáva čoraz častejším zdrojom denných správ. Oproti Facebooku ponúka Twitter menej osobný kontakt medzi jednotlivými používateľmi. Používatelia, ktorí navzájom sledujú svoj obsah, sa vo väčšine prípadov osobne nepoznajú, a rovnako aj obsah, ktorý na Twitter pridávajú, je menej osobný, ako je to v prípade Facebooku.

---

[44] BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 76.

[45] BITENIECE, N. a kol. 2017. *Digital Hydra: Security Implications of False Information Online*.

[46] Toto bol prípad škandálu britskej spoločnosti Cambridge Analytica, ktorá získavala osobné dáta od stoviek tisíc používateľov. Vďaka týmto získaným dátam potom vedela personalizovať obsah informácií, ktoré používateľom poskytovala. Cambidge Analytica poskytovala dáta pre politické kampane v rôznych krajinách sveta. V súčasnosti sa objavujú podozrenia, že toto nebol ojedinelý prípad a týmto spôsobom môžu fungovať ďalší štátni alebo neštátni aktéri (The Guardian, 2022).

[47] DR. 2022. Global Digital Overview. In *DateReportal*, 2022.

Účelom Twitteru je predovšetkým publikovanie názorov k jednotlivým témam. Dĺžka jedného príspevku je v súčasnosti obmedzená na 280 znakov,[48] čo automaticky vedie tomu, že príspevky majú charakter krátkych výrokov. Keďže obmedzený počet znakov neumožňuje argumenty rozvíjať a uvádzať zdroje, ktoré by podporovali jednotlivé tvrdenia, nevyvolávajú takéto príspevky u používateľov zvýšenú opatrnosť, naopak, považujú ich za vierohodné. Najväčší podiel na šírení dezinformácií šírených na tejto sociálnej platforme majú tzv. trolovia[49] a falošné profily v podobe botov.[50] Šírenie dezinformácií prebieha najčastejšie tak, že sa na jednu konkrétnu tému automaticky vygeneruje množstvo príspevkov, ktoré túto tému dostanú do tzv. trendov, ktoré sa zobrazujú všetkým používateľom Twitteru.[51]

4 Šírenie dezinformácií na sociálnych sieťach

Dezinformácie sú na sociálnych sieťach šírené viacerými spôsobmi. Medzi tie, ktoré sú v súčasnosti využívané najčastejšie patrí najmä využívanie:

- hybridných internetových trolov,
- automatických botov s umelou inteligenciou,
- algoritmov na vytváranie tzv. efektu ozveny.

4.1 Využívanie hybridných internetových trolov

Medzi základné prostriedky na šírenie dezinformácií na sociálnych sieťach patrí využívanie tzv. internetových trolov, ktorí majú za cieľ šíriť alebo deštruovať určitý naratív. Pôsobenie internetových trolov nesúvisí priamo s rozvojom sociálnych sietí. Prvé prípady internetových trolov sa objavili v diskusiách na rôznych webových stránkach a blogoch ešte pred vznikom sociálnych sietí. Pôvodne išlo o označovanie používateľov, ktorí mimoriadne agresívne prejavovali svoje názory a skrývali sa za anonymitu, ktorú internet už v tej dobe poskytoval.[52] Títo trolovia sa vyznačovali veľmi vulgárnym jazykom.

Postupne, ako sa sociálne siete stávali čoraz populárnejšie a stále častejšie dochádzalo k ich weaponizácii,[53] menilo sa aj správanie trolov na sociálnych sieťach. Niektorými odborníkmi sú takýto internetoví trolovia označovaní ako hybridní trollovia. V ich prípade ide o určitý druh bojovníkov v mediálnom priestore, ktorí sú zväčša najatí štátnymi alebo neštátnymi aktérmi, ktorí okrem toho, že šíria dezinformácie, šíria aj naratívy svojich zamestnávateľov (najímateľov) a, naopak, snažia sa zničiť naratív nepriateľa. S týmto cieľom

[48] V rámci jedného príspevku bolo možné pred rokom 2017 napísať text s maximálnom počtom 140 znakov. V roku 2017 prišla zmena, keď limit stúpol na 280 znakov, no ani takýto rozsah mnohým používateľom nestačil. Twitter preto umožnil rozdeliť dlhší príspevok na viacero častí, ktorý sa zobrazuje ako samostatné vlákno. Zdá sa, že v blízkej budúcnosti bude možné na Twitteri uverejňovať texty bez obmedzenia počtu znakov. Ponúkne to nový obsahový formát „Twitter Articles“.

[49] Trol je užívateľ internetu, ktorý svojimi komentármi a správaním sa na internete zámerne provokuje ostatných alebo odvádza diskusiu od pôvodnej témy (Krátky slovník hybridných hrozieb, 2022).

[50] Bot je počítačový program, ktorý autonómne vykonáva automatické úlohy na internete, napr. simuláciu ľudskej komunikácie v rámci komunikácie so zákazníkom (chatbot). Bot môže byť zneužitý na šírenie správ na sociálnych sieťach, útoky na internetové služby či zvyšovanie počtu reakcií na konkrétny príspevok - tzv. lajkov (Krátky slovník hybridných hrozieb, 2022).

[51] BITENIECE, N. a kol. 2017. *Digital Hydra: Security Implications of False Information Online*.

[52] HANNAN, J. 2018. Trolling ourselves to death? Social media and post-truth politics. In European Journal of Communication, 2018. roč. 33, č. 2, s. 214 - 226.

[53] Pri weaponizácii sociálnej siete dochádza k útočeniu nepriateľskými informáciami na cieľovú skupinu, k mobilizácii členov cieľovej skupiny, ako aj k vedeniu informačných operácií s cieľom ovplyvňovať správanie, postoje, nálady a názory cieľovej skupiny (Krátky slovník hybridných hrozieb, 2022).

produkujú veľké množstvo príspevkov, v ktorých využívajú rôzne manipulatívne techniky.[54] Hybridní trolovia sú agresívni a svojich názorových oponentov často vulgárne urážajú, čím ich, a aj ďalších čitateľov či diskutujúcich, čo nezdieľajú názorové presvedčenie trolov, odrádzajú od ďalšej diskusie.[55]

Hybridných internetových trolov využíva na šírenie dezinformácií predovšetkým Rusko. Prebiehajúce vyšetrovania naznačujú, že v Petrohrade existuje centrála, v ktorej podľa odhadov pracuje zhruba štyristo takýchto hybridných trolov, ktorých hlavnou pracovnou úlohou je vykonávať trolovanie[56] na sociálnych sieťach. Bývalí zamestnanci centrály tvrdia, že sa tu ľudia striedajú v dvanásťhodinových pracovných zmenách a ich mesačný zárobok je okolo tisíc amerických dolárov. V jednej miestnosti pracuje asi dvadsať ľudí, ktorí sa riadia presne stanovenými scenármi a inštrukciami. Na každú miestnosť dohliadajú traja editori, ktorí sú oprávnení udeľovať pokuty v prípade, že nie sú dosiahnuté stanovené denné limity príspevkov alebo sa príspevky neriadia zavedeným manuálom.[57]

4.2 Využívanie botov a umelej inteligencie

Druhým, veľmi často využívaným nástrojom pre šírenie dezinformácií, je využívanie tzv. botov.[58] Bot je niečo, čo sa tvári ako skutočný používateľ sociálnych sietí, no v skutočnosti ide o počítačový softvér, ktorý je naprogramovaný, aby v pravidelných intervaloch automaticky vytváral a šíril určitý druh príspevkov. Týmito príspevkami sa potom snaží zahltiť verejný priestor na sociálnych sieťach a takto presadzovať svoj naratív. Boti sa snažia správať ako reálni ľudia, preto často využívajú umelú inteligenciu v snahe napodobniť ľudské správanie. V súčasnosti sa odhaduje, že boti predstavujú približne 5 až 15 % všetkých používateľov na Twitteri, pričom podobný pomer sa odhaduje aj pre najväčšiu sociálnu sieť Facebook, kde boti predstavujú asi 5 až 11 % všetkých používateľov.[59]

Využívanie botov bolo veľmi populárne hlavne pred americkými prezidentskými voľbami v roku 2016. Odhaduje sa, že v kľúčovom období medzi jarou a jeseňou roku 2016 až 30 % všetkých správ odoslaných v Spojených štátoch amerických prostredníctvom sociálnych sietí nebolo vytvorených ľudským používateľom, ale botmi. Boti sú, ako je naznačené vyššie, využívaní najmä na Twitteri a na Facebooku. Podľa výskumov je až 20 % príspevkov, ktoré patria Islamskému štátu, automaticky generovaných botmi.[60] Ešte znepokojujúcejšie je zistenie, ktoré prináša Centrum výnimočnosti Severoatlantickej aliancie pre strategickú komunikáciu.[61] Podľa ich správ je v Poľsku a v pobaltských krajinách až 70 % všetkých rusko-jazyčných príspevkov, v ktorých sa hovorí o NATO, dielom botov.[62]

---

[54] BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 79.

[55] ARO, J. 2016. The Cyberspace War: Propaganda and Trolling as Warfare Tools. In *European View*, 2016, roč. 15, č. 1, s. 127.

[56] Trolovanie predstavuje 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 (Krátky slovník hybridných hrozieb, 2022).

[57] Bližšie pozri: PRIER, J. 2017. Commanding the Trend: Social Media as Information Warfare. In *Strategic Studies Quarterly*, 2017, roč. 11, č. 4; BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2; alebo ARO, J. 2016. The Cyberspace War: Propaganda and Trolling as Warfare Tools. In *European View*, 2016, roč. 15, č. 1.

[58] BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 79.

[59] BITENIECE, N. a kol. 2017. *Digital Hydra: Security Implications of False Information Online*.

[60] BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 81 – 82.

[61] Centrum výnimočnosti pre strategickú komunikáciu je medzinárodná vojenská organizácia s akreditáciou NATO, ktorá nie je súčasťou veliteľskej štruktúry NATO a nie je podriadená žiadnemu inému subjektu NATO.

4.3 Zneužívanie algoritmov

Tretím pomerne často využívaným nástrojom na šírenie dezinformácií je zneužívanie algoritmov, ktoré na sociálnych sieťach fungujú. Ide o algoritmy, ktoré používateľom sociálnych sietí odporúčajú rôzne príspevky na základe ich správania na danej sociálnej sieti. Berú do úvahy aj príspevky, na ktoré klikli ich známi, a príspevky, ktoré čítajú používatelia stránok a skupín, ktorých sú členmi. Algoritmy používateľom podsúvajú príspevky, ktoré sú virálne, t. j. dosahujú veľký počet zdieľaní a tzv. lajkov. Týmto sa vytvára tzv. efekt ozveny. Stačí jedno kliknutie na určitý článok a sociálna sieť začne používateľovi automaticky ponúkať ďalšie články s podobnou tematikou. Čiže, ak používateľ klikne na hoax alebo falošnú správu raz, pretože ho upúta názov článku, sociálna sieť mu začne automaticky podsúvať ďalšie podobné články a príspevky. Aj na základe tohto aspektu sa aktéri šíriaci dezinformácie snažia zamerať na dych vyrážajúce a emocionálne citlivé témy, aby šokujúcim nadpisom donútili používateľov kliknúť na ich správu či príspevok. Používané algoritmy sledujú všetky články, príspevky a na základe toho vyhodnocujú frekvenciu výskytu jednotlivých slov. Tie s najväčšou frekvenciou výskytu potom označujú ako trendy, ktoré sa zobrazujú všetkým používateľom.[63] Na vytváranie trendov sa využíva kombinované úsilie trolov, botov a tiež používateľov. Tým, že umelo a hromadne šíria veľké množstvo príspevkov, algoritmy dokážu vyhodnotiť, že téma je medzi používateľmi populárna a následne dané príspevky automaticky ponúka ďalším používateľom.

Záver

Sociálne siete predstavujú jednu z najdynamickejšie sa rozvíjajúcich komunikačných a informačných platforiem. V priebehu niekoľkých pár rokov prešli mnohými významnými zmenami. Z malých, roztrúsených webových stránok miestnych komunít sa vyvinuli až na konsolidované spoločnosti s globálnym dosahom a vplyvom. Sociálne siete boli tiež súčasťou skoku do sveta mobilných technológií, ktoré majú obrovský vplyv na ľudské správanie vrátane vzorov používania sociálnych sietí. Postupom času sa menili aj motivácie používateľov zapájať sa do diskusií na sociálnych sieťach.

Prvotnú, čisto „sociálnu“ motiváciu postupne vystriedali iné motivácie, ako napríklad vyhľadávanie informácií, ktorých poskytovanie priblížilo sociálne platformy oveľa bližšie k tradičným médiám. V tomto informačnom prostredí postupne nastala dramatická zmena, ktorú možno nazvať weaponizáciou sociálnych sietí, čo znamená transformáciu sociálnych sietí na bojové pole, na ktorom prebiehajú nepriateľské hybridné aktivity vykonávané na cieľovom publiku v šedej zóne[64] medzi mierom a vojnou.

Sídli v Rige v Lotyšsku a prispieva k zlepšeniu strategických komunikačných schopností v rámci Aliancie a spojeneckých krajín. Strategická komunikácia je neoddeliteľnou súčasťou úsilia o dosiahnutie politických a vojenských cieľov Aliancie, preto je čoraz dôležitejšie, aby Aliancia komunikovala vhodným, včasným, presným a citlivým spôsobom o svojich vyvíjajúcich sa úlohách, cieľoch a misiách. Poslaním centra je poskytnúť konkrétny príspevok k strategickým komunikačným schopnostiam NATO, spojencov NATO a partnerov NATO. Jeho sila je budovaná nadnárodnými a medzisektorovými účastníkmi z civilného a vojenského, súkromného a akademického sektora a využitím moderných technológií, virtuálnych nástrojov na analýzy, výskum a rozhodovanie. Srdcom NATO StratCom COE je rôznorodá skupina medzinárodných expertov s vojenským, vládnym a akademickým zázemím – školiteľov, pedagógov, analytikov a výskumníkov. Bližšie pozri: NATO. 2022. NATO Centre of Excellence for Strategic Communications, 2022

[62] BITENIECE, N. a kol. 2017. *Digital Hydra: Security Implications of False Information Online*.

[63] PRIER, J. 2017. Commanding the Trend: Social Media as Information Warfare. In *Strategic Studies Quarterly*, 2017, roč. 11, č. 4, s. 62.

[64] Šedá zóna predstavuje priestor, v ktorom sa vedie hybridná vojna, pričom sa využíva nejednoznačnosť vnútroštátneho a medzinárodného práva. Ide o aktivity jedného štátu, ktoré škodia inému štátu, pričom právne

Vďaka svojim výnimočným vlastnostiam, akými sú globálny dosah, vysoká dostupnosť, nízke náklady, obrovský objem a rýchlosť výmeny informácií a do určitej miery aj anonymita používateľov, sú sociálne siete atraktívne pre viacerých aktérov s nepriateľskými agendami. Paradoxne to, čo bolo veľkou výhodou, stalo sa viditeľnou slabinou. Platformy, ktoré sa podľa definície zrodili ako „sociálne", stali sa priestorom veľkého množstva aktivít, ktoré majú jednoznačne antisociálny charakter.

Preto považujeme za opodstatnené nazývať sociálne siete bojiskom, na ktorom prebieha intenzívny boj o srdcia a mysle ľudí. Je to bojové pole, na ktorom možno pozorovať rôzne vojenské i nevojenské stratégie a taktiky a využívanie nástrojov, akými sú dezinformácie, propaganda, falošné správy, konšpiračné teórie, vyhrážanie sa protivníkom, mobilizácia priaznivcov, koordinácia akcií a aktivít a pod. Dynamický rozvoj technológií pritom zohráva významnú úlohu, vďaka čomu sú všetky tieto činnosti jednoduchšie a efektívnejšie. Ľudským aktérom vo veľkej miere pomáhajú alebo ich dokonca nahrádzajú roboty a rôzne aplikácie, pričom obsah (správa, informácia) sa stáva – vďaka rozvoju multimédií – čoraz atraktívnejším.

V tejto súvislosti sa vynára otázka, čo môže demokratický svet urobiť, aké opatrenia môže prijať, aby dokázal efektívne a účinne čeliť nepriateľským aktivitám na sociálnych sieťach a celkovo hybridným hrozbám, keďže protivníci nedodržiavajú rovnaké právne pravidlá a etické princípy ako demokratické spoločnosti a nezdieľajú demokratické hodnoty. Navyše, kým protivníci sú prefíkaní, rýchli, flexibilní a prispôsobiví vzhľadom na osobitný charakter ich organizácií, ich zriadenia, tak demokratické krajiny a inštitúcie sú povinné dodržiavať špecifické postupy so zdĺhavými rozhodovacími procesmi.

Sociálne siete, ako sa teda ukazuje, sú veľmi mocným a efektívnym nástrojom na manipuláciu s populáciou v hromadnom meradle. Ich súčasné masové používanie uľahčuje šírenie dezinformácií štátnym aj neštátnym aktérom viac ako kedykoľvek predtým. Aj preto je veľmi dôležité nielen pokračovať vo výskume v tejto oblasti, ale ho ešte viac prehlbovať. Dosiahnuté výsledky výskumu by mali prispieť k tomu, aby nebolo možné používať, resp. zneužívať sociálne siete ako hybridnú zbraň na ovplyvnenie myslenia a správania ľudí a ohrozenie demokratických procesov prebiehajúcich vo vyspelých demokratických krajinách.

Literatúra

ALLCOTT, H. – GENTZKOW, M. 2017. Social Media and Fake News in the 2016 Election. In *Journal of Economic Perspectives*, 2017, roč. 31, č. 2, s. 211-236. ISSN 1944-7965. [online] [cit. 08.04.2022] Dostupné z: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211>.

ANDRASSY, V. – GREGA, M. 2015. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18. ISSN 1338-4880.

ARO, J. 2016. The Cyberspace War: Propaganda and Trolling as Warfare Tools. In *European View*, 2016, roč. 15, č. 1, s. 121-132. ISSN 1865-5831. [online] [cit. 09.04.2022] Dostupné z: <http://dx.doi.org/10.1007/s12290-016-0395-5>.

BAYER, M. 2006. Strategic Information Warfare: An introduction. In Halpin, E. et al. (eds.): *Cyberwar, Netwar and the Revolution in Military Affairs*, 2006. [online] [cit. 07.04.2022] Dostupné z: <https://link.springer.com/chapter/10.1057/9780230625839_3>.

BAYM, G. 2005. The daily show: discursive integration and the reinvention of political journalism. In Political Communication, 2005, roč. 22, č. 3, s. 259–276. ISSN 1091-7675.

---

ale nejde o vojnové činy. Ide o tzv. činy pod hranicou ozbrojeného konfliktu (Krátky slovník hybridných hrozieb, 2022).

BENNETT, L. – LIVINGSTON, S. 2018. The disinformation order: Disruptive communication and the decline of democratic institutions. In *European Journal of Communication*, 2018, roč. 33, č. 2, s. 122-139. ISSN 0267-3231. [online] [cit. 09.04.2022] Dostupné z: <http://dx.doi.org/10.1177/0267323118760317>.

BIAŁY, B. 2017. Social Media—From Social Exchange to Battlefield. In *The Cyber Defense Review*, 2017, roč. 2, č. 2, s. 69-90. ISSN 2474-2120. [online] [cit. 18.04.2022] Dostupné z: <https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Social%20Media%20From%20Social%20Exchange_Bialy.pdf?ver=2018-07-31-093711-437>.

BITENIECE, N. – BERTOLIN, G. – AGARWAL, N. – BANDELI, K. K. – SEDOVA, K. 2017. *Digital Hydra: Security Implications of False Information Online*. Riga : NATO Strategic Communications Centre of Excellence, 2017. 85 s. ISBN 978-9934-564-18-5.

Cambridge Dictionary. 2021. *Disinformation*. [online] [cit. 09.04.2022] Dostupné z: <https://dictionary.cambridge.org/dictionary/english/disinformation>.

DAVISON, W. P. 1971. Some Trends in International Propaganda. In *The Annals of the American Academy of Political and Social Science*, 1971, s. 1-13. [online] [cit. 09.04.2022] Dostupné z: <https://doi.org/10.1177/000271627139800102>.

DR. 2021. Global Digital Overview. In *DateReportal*, 2021. [online] [cit. 18.04.2022] Dostupné z: <https://datareportal.com/reports/digital-2021-global-overview-report>.

DVORAK, J. 2016. *Complexity in Modern War: Examining Hybrid War*. Springfield: Missouri State University, 2016. 178 s. ISBN 978-1-721-51009-2.

EC. 2018. Final report of the High Level Expert Group on Fake News and Online Disinformation. In *European Commission*, 2018. [online] [cit. 10.04.2022] Dostupné z: <https://www.ecsite.eu/activities-and-services/resources/final-report-high-level-expert-group-fake-news-and-online>.

EK. 2018. *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*. Brusel: Európska komisia, 2018. 44 s. ISBN 978-92-79-80420-5. [online] [cit. 09.04.2022] Dostupné z: <https://www.ecsite.eu/sites/default/files/amulti-dimensionalapproachtodisinformation-reportoftheindependenthighlevelgrouponfakenewsandonlinedisinformation.pdf>.

EP. 2016. Report on EU strategic communication to counteract propaganda against it by third parties. In *European Parliament*, 2016. [online] [cit. 10.04.2022] Dostupné z: <https://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html>.

EUEA. 2021. EUvsDisinfo. In *European Union External Action*, 2021. [online] [cit. 10.04.2022] Dostupné z: <https://counteringdisinformation.org/taxonomy/term/553>.

EUEA. 2021. *Questions and Answers about the East StratCom Task Force*. In *European Union External Action*, 2021. [online] [cit. 10.04.2022] Dostupné z: <https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en>.

GLENN, R. W. 2009. Thoughts on Hybrid Conflict. In *Small Wars Journal*, 2009. [online] [cit. 06.04.2022] Dostupné z: <https://www.smallwarsjournal.com/blog/188-glenn.pdf>.

GRISCIOLI, G. 2016. *Intelligence. The Hybrid War*. Roma : Aracne, 2016. 108 s. ISBN 978-88-5489-060-2.

HAJDUKOVÁ, S. 2021. Konflikty v šedej zóne a hybridná vojna. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 68-82. ISBN 978-80-7160-617-8.

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.

HALPIN, E. – TREVORROW, P. –WEBB, D. – WRIGHT, S. 2006. Cyberwar, Netwar and the Revolution in Military Affairs. London : Palgrave McMillan, 2006. 253 s. ISBN 978-1-349-54123-2.

HANNAN, J. 2018. Trolling ourselves to death? Social media and post-truth politics. In *European Journal of Communication*, 2018. roč. 33, č. 2, s. 214-226. ISSN 0267-3231. [online] [cit. 20.04.2022] Dostupné z: <http://dx.doi.org/10.1177/0267323118760323>.

HOFFMAN, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. In *Potomac Institute for Policy Studies*, 2007. [online] [cit. 06.04.2022] Dostupné z: <http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf>.

Hybrid CoE. 2022. Hybrid Threats. In *Hybrid Centre of Excellence*, 2022. [online] [cit. 06.04.2022] Dostupné z: <https://www.hybridcoe.fi/hybrid-threats/.

Hybrid CoE. 2022. What is Hybrid CoE? In *Hybrid Centre of Excellence*, 2022. [online] [cit. 10.04.2022] Dostupné z: <https://www.hybridcoe.fi/who-what-and-how/>.

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. [online] [cit. 06.04.2022] Dostupné z: <https://fmv.euba.sk/www_write/files/dokumenty/veda-vyskum/medzinarodne-vztahy/archiv/2016/2/mv_2016_2_130-156_ivancik.pdf>.

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 Milana Rastislava Štefánika. 2020. s. 174-184. ISBN 978-80-8040-589-2.

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. DOI: https://doi.org/10.24040/politickevedy.2021.24.1.135-152. [online] [cit. 06.04.2022] Dostupné z: <http://www.politickevedy.fpvmv.umb.sk/en/archive/2021/1-2021/ radoslav-ivancik.html>.

JIRÁSKOVÁ, S. 2019. Ekonomická vojna ako jedna z podôb hybridnej vojny. In *Národná a medzinárodná bezpečnosť 2019 – zborník príspevkov z 10. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, s. 205-213. ISBN 978-80-8040-582-3.

KORAUŠ, A. – KELEMEN P. 2018. Protection of persons and property in terms of cybersecurity. In *Ekonomické, politické a právne otázky medzinárodných vzťahov 2018 – zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava : Vydavateľstvo Ekonóm, 2018. ISBN 978-80-225-4506-8.

KOSTREC, M. 2020. Nebezpečné hrozby v digitálnom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2020, s. 78-87. ISBN 978-80-8040-819-3.

KOVANIČ, M. 2017. Dezinformácie a ruská propaganda ako bezpečnostné hrozby. In *Bezpečnostní teorie a praxe*, 2017, č. 2, s. 121-132. ISSN 1801-8211.

Krátky slovník hybridných hrozieb. 2022. *Dezinformácia*. [online] [cit. 20.04.2022] Dostupné nz: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/ kratky-slovnik-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 v Bratislave, 2018, s. 90-98. ISBN 978-80-8054-773-8.

LUKÁČOVÁ, J. 2017. Hybridné hrozby a ich vplyv na bezpečnostné prostredie – teória, vývoj a prax. In Vojenské reflexie, roč. 15, č. 1, s. 163-172. ISBN 1337-8163.

LUKÁČOVÁ, V. 2020. Hybridné hrozby v kybernetickom priestore. In *Aktuálne výzvy kybernetickej bezpečnosti : zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2020, s. 102-105. ISBN 978-80-8040-819-3.

MacMillan Dictionary. 2021. *Disinformation*. [online] [cit. 09.04.2022] Dostupné z: <https://www.macmillandictionary.com/dictionary/british/disinformation>.

MANKO, O. – MIKHIEIEV, Y. 2018. Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. In *Connections*, 2018. [online] [cit. 06.04.2022] Dostupné z: <https://connections-qj.org/system/files/4107_mikhieiev_manko.pdf>.

MILLER, M. 2015. *Hybrid Warfare: Preparing for Future Conflict*. Montgomery: Air War College, 2015. 34 s.

MURRAY, W. – MANSOOR, P. R. 2012. *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge : Cambridge University Press, 2012. 321 s. ISBN 978-1-107-02608-7.

NATO. 2022. NATO Strategic Communications Centre of Excellence. In *NATO*, 2022. [online] [cit. 10.04.2022] Dostupné z: <https://www.stratcomcoe.org/about-strategic-communications>.

NATO. 2022. We are NATO. In *NATO*, 2022. [online] [cit. 10.04.2022] Dostupné z: <https://www.nato.int/wearenato/>.

Oxford Learner´s Dictionary. 2021. *Disinformation*. [online] [cit. 09.04.2022] Dostupné z: <https://www.oxfordlearnersdictionaries.com/definition/english/disinformation?q=disinformation>.

PRIER, J. 2017. Commanding the Trend: Social Media as Information Warfare. In *Strategic Studies Quarterly*, 2017, roč. 11, č. 4, s. 50-85. ISSN 1936-1815. [online] [cit. 09.04.2022] Dostupné z: <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf>.

RÉVESZOVÁ, L. 2018. Počítačová kriminalita a dynamika jej vývoja v rokoch 2014 - 2017. In *Aktuálne výzvy kybernetickej bezpečnosti – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2018, s. 161-173. ISBN 978-80-8054-773-8.

SILVERMAN, C. 2016. This analysis shows how viral fake election news stories outperformed real news on Facebook. In *Buzzfeed*, 2016. [online] [cit. 08.04.2022] Dostupné z: <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.

Slovník cudzích slov. 2015. *Dezinformácia*. [online] [cit. 09.04.2022] Dostupné z: <https://slovnik.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=bernolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>.

Slovník súčasného slovenského jazyka. 2015. *Dezinformácia.* [online] [cit. 09.04.2022] Dostupné z: <https://slovnik.juls.savba.sk/?w=dezinformácia&s=exact&c=a861&cs=&d=kssj4&d=psp&d=sssj&d=orter&d=scs&d=sss&d=peciar&d=ssn&d=hssj&d=bernolak&d=noundb&d=orient&d=locutio&d=obce&d=priezviska&d=un&d=pskcs&d=psken#>.

TG. 2022. The Cambridge Analaytica Files. In *The Guardian*, 2022. [online] [cit. 18.04.2022] Dostupné z: <https://www.theguardian.com/news/series/cambridge-analytica-files>.

TOMÁŠEK, R. – TOMÁŠEKOVÁ, L. 2020. Kybernetické hrozby a kybernetický terorizmus. In *Aktuálne výzvy kybernetickej bezpečnosti: zborník príspevkov z vedeckej konferencie*

s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru v Bratislave, 2020, s. 146-152. ISBN 978-80-8040-819-3.
US DoD. 2000. *United States Department of Defense: Joint Vision 2020*. Washington: United States Government Printing Office, 2000. [online] [cit. 06.04.2022] Dostupné z: <https://www.hsdl.org/? abstract&did=446826>.
VARGO, C. J. – GUO, L. – AMAZEEN, M. A. 2017. The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. In *New Media & Society*, 2017, roč. 20, č. 5, s. 2028-2049. ISSN 1461-7315. [online] [cit. 09.04.2022] Dostupné z: <http://dx.doi.org/10.1177/1461444817712086>.
VOERZIO, M. 2021. *Hybrid War: Attack on the West*. Garden City: Babelcube, 2021. 96 s. ISBN 978-1-6674-1523-9.
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 v Bratislave, 2018, s. 217-224. ISBN 978-80-8054-773-8.
ZACHARIDESOVÁ, N. 2021. Moderné spôsoby vedenia vojny. In *Aktuálne bezpečnostné výzvy a medzinárodné právo - zborník príspevkov z medzinárodnej vedeckej konferencie*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021, s. 54-67. ISBN 978-80-7160-617-8.

Keywords: disinformation, social networks, hybrid threats, internet, technologies.

Summary

Disinformation today poses a considerable hybrid threat, the severity of which is exacerbated by the dynamic development and massive use of social networks. The origin of the Internet, connectivity, and information and communication technologies have caused that information is disseminated 24 hours a day, seven days a week. In the history of humankind, it has never been easier to receive, search and spread. However, this progress has many positives and many negatives. In the avalanche of information that comes to us daily, it is undoubtedly challenging to distinguish which information is genuine, objective, and based on real-life events, on the other hand, to identify the information which is misleading, distorted, or completely fabricated, created with the purpose to obtain economic, political or other profit. Many non-state actors, but, unfortunately, state actors as well, have begun to use this fact to disseminate false information to advance their financial, political, or power interests. Information, resp. disinformation has become a weapon. Therefore, the social networks, an excellent tool for spreading disinformation in today's modern information society, have become a battleground for hostile hybrid activities performed on the target audience in the so-called Grey zone between peace and war.

doc. Ing. Radoslav Ivančík, PhD. et PhD., MBA, MSc.
Katedra informatiky a manažmentu
Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava 35
e-mail: radoslav.ivancik@akademiapz.sk

prof. Ing. Jana Müllerová, PhD.
Katedra verejnej správy a krízového manažmentu
Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava 35
e-mail: jana.mullerova@akademiapz.sk

Recenzenti: doc. Ing. Vladimír Andrassy, PhD., mjr. JUDr. Matej Kostrec, PhD.