PRÍRUČKA DEZINFORMAČNÝCH KAMPANÍ

TOMÁŠ BARANEC
KATARÍNA CSÉFALVAYOVÁ
FREDERICK HARDMAN LEA

INSTITUTE for CENTRAL EUROPE

Predhovor

Diskusia o problematike hybridných hrozieb a dezinformácií priniesla celú škálu pojmov, ktoré sme v slovenskom jazyku doposiaľ nemali, nepoužívali alebo používali v inom význame. Termíny ako dezinformácie, hoax, falošné správy alebo trol, bot či kyborg sa často medzi sebou voľne zamieňajú, používajú ako synonymá a len málokto, azda okrem odborníkov na túto problematiku, ich dokáže rozoznať a správne používať.

Dezinformácie dnes pritom predstavujú jednu z najväčších hrozieb, ktorej ako štát i spoločnosť čelíme a zároveň účinný boj proti dezinformáciám a budovanie odolnosti spoločnosti voči nim sú cieľmi, ktoré sa nám zatiaľ darí napĺňať len veľmi pomaly a čiastočne. Za krok smerom k napĺňaniu týchto cieľov pritom možno považovať i správne rozlišovanie a poznanie pojmov a vzťahov medzi nimi.

Táto publikácia stavia na predošlej práci Národného bezpečnostného analytického centra Slovenskej informačnej služby, Stratpolu, a iných organizácií, ktoré v slovenských podmienkach spracovali terminologické slovníky hybridných hrozieb, popisujúce a definujúce jednotlivé pojmy späté s dezinformačnými kampaňami.

Cieľom predkladanej publikácie je nielen definovanie kľúčových pojmov, ale aj vysvetlenie súvzťažností a rozdielov medzi nimi, zasadzujúc ich do kontextu a ilustrujúc na konkrétnych príkladoch z praxe dezinformačných kampaní.

Publikácia je určená predovšetkým pre pracovníkov štátnych inštitúcií, ktorí prichádzajú do styku s problematikou šírenia dezinformácií, ako aj pre širšiu verejnosť a kohokoľvek, kto si chce ujasniť často neprehľadnú terminológiu hybridných hrozieb. Je spracovaná s podporou Ministerstva obrany Slovenskej republiky, v rámci projektu „Posilnenie odolnosti SR voči hybridným hrozbám zo strany ruských aktérov – dezinformačné kampane na sociálnych sieťach". Nadväzuje na workshop „Propagandistické nástroje ruských aktérov na sociálnych sieťach – ako ich rozpoznať a ako sa im brániť?", ktorý Inštitút pre centrálnu Európu realizoval 7. 10. 2021 v Bratislave, ako aj na štúdiu „Ako čeliť riadeným dezinformáciám na sociálnych sieťach? Skúsenosti Ukrajiny, Gruzínska a Moldavska".

Obsah

Predhovor 2

Hybridné hrozby a Slovenská republika 4

Hlavné nástroje dezinformačných kampaní 5

Typy nepravdivých informácií 5

Nástroje tvorby a šírenia nepravdivých informácií 8

Nástroje posilnenia dosahu dezinformačných kampaní 12

Záver 17

Slovník iných často používaných termínov 18

Zoznam použitej literatúry 25

O nás 27

Hybridné hrozby a Slovenská republika

Podľa definície Hybrid CoE, medzinárodnej organizácie venujúcej sa skúmaniu budovania odolnosti voči hybridným hrozbám, ide v prípade hrozieb tohto typu o „kroky uskutočnené štátnymi aj neštátnymi aktérmi s cieľom oslabiť alebo poškodiť cieľ ovplyvnením jeho rozhodovacích procesov na miestnej, regionálnej, štátnej aj inštitucionálnej úrovni“[1].

Hybridnosť týchto krokov spočíva v tom, že ich aktér stiera tradičné hranice medzinárodnej politiky tým, že sa pohybuje na hrane vonkajšej a vnútornej politiky, legálnosti a nelegálnosti, ako aj mieru a vojny. Kombinuje pritom konvenčné a nekonvenčné metódy. Súčasťou hybridných operácií môže byť zároveň snaha o ovplyvnenie verejnej mienky a súdržnosti spoločnosti pomocou dezinformačných kampaní, kybernetických operácií, kriminálnych aktivít, ako aj asymetrického využívania vojenských prostriedkov a vojny. Všetky tieto stratégie sa pritom môžu v rámci hybridnej operácie vzájomne dopĺňať a posilňovať.

Hybridné operácie sa nevyhýbajú ani Slovenskej republike. Tá sa podľa Národného bezpečnostného úradu „najčastejšie stretáva s pokusmi o ovplyvňovanie verejnej mienky v kybernetickom priestore, ktorý má sám o sebe hybridnú povahu“[2]. Hlavným prostriedkom ovplyvňovania verejnej mienky v kybernetickom priestore sú dezinformačné kampane na sociálnych sieťach. Hoci sú dezinformačné kampane veľmi rôznorodým fenoménom, ktorý sa navyše vyvíja v čase, pri dosahovaní svojich cieľov sa väčšinou spoliehajú na účelové kombinovanie tých istých nástrojov. Jasné definovanie a pochopenie týchto nástrojov na tvorenie a šírenie dezinformácií, ako aj zvyšovanie ich efektivity je prvým krokom k úspešnej analýze dezinformačných kampaní.

[1] Hybrid CoE, “Hybrid threats as a concept”, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

[2] Národný bezpečnostný úrad, „Hybridné hrozby“, 2021, https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html

Hlavné nástroje dezinformačných kampaní

Typy nepravdivých informácií

S rozmachom informačných technológií a neustále sa zvyšujúcou dostupnosťou internetu pre široké masy dochádza aj k stále častejšiemu výskytu šírenia *nepravdivých informácií*. Súhrnne je zvykom ich označovať pojmom dezinformácie, falošné správy či hoaxy, pričom používatelia tieto pojmy často považujú za synonymá a voľne ich medzi sebou zamieňajú. Pravdou je, že všetky tieto pojmy súvisia s nepravdivými informáciami a majú podobný význam, nie sú však v skutočnosti synonymami v pravom zmysle slova.

Nie každá nepravdivá informácia je dezinformáciou

V prípade šírenia nepravdivých informácií je nevyhnutné rozlišovať medzi viacerými charakteristikami, ktorými sa vyznačujú. Prvým znakom, resp. kritériom ich klasifikácie je **veľkosť publika**, pre ktoré sú určené. Typickým znakom dezinformácií je v tomto prípade ich masovosť, teda šírenie zamerané na veľký počet užívateľov. To ju odlišuje od nepravdivej informácie, ktorú napríklad poskytne žiak svojmu učiteľovi, keď sa pokúša vysvetliť, prečo nemá vypracovanú domácu úlohu. V takom prípade nepravdivú informáciu označujeme ako *klamstvo, fabuláciu*, prípadne iným vhodným termínom, nejde však o dezinformáciu.

Druhým aspektom, ktorý pri nepravdivých informáciách treba brať do úvahy, je **úmyselnosť**. Z tohto pohľadu sa pojmom *dezinformácia* (po anglicky „disinformation") označuje úmyselne šírená nepravdivá informácia, pričom jej pôvodca, resp. šíriteľ, **úmyselne rozširuje nepravdivú informáciu s cieľom zmiasť, oklamať čo najväčšie publikum**. Neúmyselne šírená nepravdivá informácia sa v angličtine označuje pojmom „misinformation", ktorý do slovenského jazyka prekladáme ako *zlá informácia*, hoci tento termín presne nevystihuje podstatu neúmyselného vovedenia publika do omylu. Osobitnou kategóriou v tomto kontexte je pojem *Informácia so zlým úmyslom* (po anglicky „malinformation"), ktorý označuje šírenie pravdivej informácie s cieľom poškodiť určitú osobu, resp. subjekt. Ako príklad môže poslúžiť zverejnenie e-mailovej korešpondencie Hillary Clinton pred prezidentskými voľbami v USA v roku 2016 či zverejnenie komunikácie Emmanuela Macrona pred francúzskymi prezidentskými voľbami v roku 2017).

Z hľadiska dezinformačných kampaní je však kľúčovým pojmom, ako to sám názov naznačuje, **dezinformácia, teda nepravdivá informácia, ktorá je šírená masovo, resp. určená pre široké publikum** (napr. prostredníctvom médií či sociálnych sietí), **a zároveň úmyselne, s cieľom zavádzať ich prijímateľa**.

Nie každá dezinformácia je hoax

Hoci, ako sme uviedli vyššie, pojmy dezinformácia a hoax sa často v praxi voľne zamieňajú, nie sú synonymami. Skôr by sa dalo povedať, že hoax je špecifickou podkategóriou dezinformácií.

Slovo pochádza z angličtiny, pričom niektorí vedci sa domnievajú, že vznikol zo slovného spojenia „hocus pocus" a jeho používanie sa datuje približne od prelomu 18. a 19. storočia.

Charakteristickým znakom hoaxu je úmyselnosť, avšak bez zlého úmyslu. Cieľom býva skôr poukázať na určitý relevantný spoločenský problém. Jeho znakom býva často tiež humor a satira, hoci najmä v súčasnosti nie je jeho nevyhnutnou súčasťou. V každom prípade by však malo ísť o informáciu, ktorá zaujme na prvý pohľad a vyvolá senzáciu. Za jeden z prvých hoaxov je považovaný prípad z roku 1708, keď známy autor Jonathan Swift, píšuci pod pseudonymom Isaac Bickerstaff, prostredníctvom almanachu predpovedal smrť astrológa Johna Partridgea. Jeho cieľom bolo urobiť si žart z ľudí, ktorí veria predpovediam astrológov a skritizovať tak vieru v pseudovedu. Iným príkladom hoaxu je príhovor Benjamina Franklina z roku 1747, z údajného súdu s Polly Bakerovou. Súd i samotná postava Polly Bakerovej boli však vymyslené autorom, ktorý chcel takto poukázať na dvojité štandardy pri posudzovaní činov žien a mužov.

Hoax teda možno charakterizovať ako **formu úmyselného šírenia nepravdivej informácie, resp. dezinformácie, ktorej cieľom je vyvolať senzáciu za účelom poukázať na určitý problém alebo inak poučiť publikum**, často s využitím prvkov humoru. Hoax býva po čase vysvetlený a uvedený na pravú mieru.

Niektoré zdroje zároveň pridávajú ďalší typ hoaxu, ktorého cieľom má byť **peňažný zisk**. Tento typ hoaxu je ekonomicky motivovaný podobným spôsobom ako *clickbait* (viď nižšie.). Najčastejšie uvádzaným príkladom tohto typu hoaxu je prípad macedónskych tínedžerov, ktorí pred prezidentskými voľbami v USA v roku 2016 založili a prevádzkovali viac ako 100 webstránok podporujúcich prezidentského kandidáta Donalda Trumpa. Vytváraním senzačných (nepravdivých) titulkov a obsahu zabezpečili vysokú mieru návštevnosti a zdieľania týchto stránok, čo napokon viedlo k finančnému zisku[3].

Falošné správy, ktoré vyzerajú ako správy

Jedným z najznámejších a v angličtine zároveň najviac nadužívaných pojmov je *falošná správa* (po anglicky „fake news"). Tento termín sa spája najmä s bývalým americkým prezidentom Donaldom Trumpom. Ten ním označoval každú správu, ktorá mu nebola po vôli. V skutočnosti má tento pojem označovať **správy, ktoré sa vydávajú za skutočné a hodnoverné imitovaním skutočných médií**, resp. spravodajských webov. Šírené bývajú pomocou takzvaných *podvodných spravodajských webov* (po anglicky „fake news websites"). Takýto spôsob šírenia dezinformácií často pozorujeme v postsovietskom priestore, kde takéto podvodné weby, kopírujúce etablované zahraničné médiá (napr. BBC, Fox News či Euronews), prevádzkujú proruskí aktéri s cieľom získať si tak dôveru cieľového publika.

---

[3] Silverman Craig, Lawence Alander, Buzz Feed News, „How Teens In The Balkans Are Duping Trump Supporters With Fake News", 2016, https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo

Neškodná reklama či klamlivá manipulácia?

Ďalším často používaným termínom v súvislosti s riadenými dezinformačnými kampaňami je *propaganda*. Samotný výraz má pôvod v katolíckej Cirkvi a pochádza z latinského slova *propagare*, ktoré v pôvodnom význame malo označovať šírenie viery[4]. Po neblahých skúsenostiach z histórie, najmä (no nielen) z druhej svetovej vojny a komunistického režimu Východného bloku tento výraz nadobudol **hanlivú konotáciu** a vlády sa usilovali vyhnúť jeho používaniu. Napríklad v kontexte zahraničnej politiky, kde pôvodne označoval šírenie dobrého mena štátu smerom navonok, bol práve z tohto dôvodu nahradený termínom *verejná diplomacia (public diplomacy)*[5]. Samotný výraz má však neutrálny náboj, keďže propaganda môže byť využívaná na dobré i škodlivé účely. Pre správne použitie v kontexte dezinformačných kampaní je preto vhodné ho doplniť, resp. bližšie charakterizovať (napr. škodlivá propaganda).

Zákerné nepravdy aj nelichotivá realita

Hoci sú základom dezinformačných kampaní, ako to už názov naznačuje, dezinformácie, ich organizátori sa nespoliehajú len na ne. V snahe vytvoriť vlastný *naratív* (po anglicky „Narrative"), teda svoju verziu reality, miešajú dezinformácie s polopravdami, ako aj faktickými poukazmi na problémy cieľovej spoločnosti. Práve v tomto spočíva komplexnosť dezinformačných kampaní. Boj proti nim je komplikovaným procesom analyzovania naratívov a ich rozoberania na očividné dezinformácie, ako aj pravdivé informácie o problémoch cieľovej spoločnosti. Tie prvé musí štát v rámci budovania odolnosti aktívne vyvracať a tie druhé efektívne riešiť.

---

[4] Stengel Richard: Information Wars. New York: Atlantic Monthly Press, 2019, str. 290

[5] S týmto termínom ako prvý prišiel v 60. Rokoch 20. storočia Edmund Gullion, dekan Fletcherovej školy práva a diplomacie na Tufts University. Zdroj: Melissen Jan, Public Diplomacy, in: Kerr, P., Wiseman, G. (eds.), Diplomacy in a Globalizing World, New York: Oxford University Press, 2013

Nástroje tvorby a šírenia nepravdivých informácií

Pojmy ako *trol* (po anglicky „Troll") a *bot* sa v posledných rokoch v súvislosti s rozsiahlymi štátmi organizovanými dezinformačnými kampaňami stali pevnou súčasťou slovníka nielen bezpečnostných expertov, ale aj bežných používateľov internetu. Úspešná dezinformačná kampaň však v skutočnosti z hľadiska tvorby a šírenia dezinformácií zahŕňa omnoho väčšie množstvo rôznych aktérov a entít.

Trolovia: Rokmi overený prostriedok

V internetovej komunikácii je **trol definovaný ako človek, ktorý vyvoláva spory napr. nastoľovaním kontroverzných tém alebo napádaním iných účastníkov diskusií**. Z hľadiska dezinformačných kampaní však treba rozlišovať medzi bežnými trolmi a platenými organizovanými trolmi s jasne definovanou agendou. V prípade ruskými aktérmi organizovaných dezinformačných kampaní podliehajú trolovia neraz značnej centralizácii, pričom bývajú organizovaní v rámci takzvaných *trolých fariem*.

Takto organizovaní trolovia identifikujú citlivé témy v cieľových krajinách a následne sa zapájajú do relevantných diskusií na sociálnych sieťach s cieľom rozvíriť na predmetných témach vášne a ešte viac tak polarizovať miestnu spoločnosť. Podstatným prvkom ich stratégie je fakt, **že cieľom predmetných trolov nie je primárne presadzovanie konkrétnej ideológie alebo jedného špecifického naratívu, ale skôr polarizácia spoločnosti**.

„Nevymýšľajú si nič nové. Hľadajú sporné témy na Facebooku a Twitteri, pričom ich následne amplifikujú. Ide o bežný sociálny marketing, ktorý využíva sociálne siete mimoriadne úspešným spôsobom. Nie je to pritom veľmi drahé, v takejto podobe, ak zoberieme do úvahy koľko chaosu to spôsobuje," uviedla v tejto súvislosti americká diplomatka Sarah E. Mendelsonová[6].

Význam trolov pre dezinformačné kampane neohrozil ani nástup botov, ktorí dokážu dezinformácie pri správnej stratégii mimoriadne efektívne a lacno šíriť. Skutoční ľudia vrátane profesionálnych trolov totiž zostávajú hlavnými tvorcami a autormi dezinformácií a hoaxov[7].

Ako príklad môže poslúžiť Internetová prieskumná agentúra (Glavset)[8]. Ide o ruskú spoločnosť sídliacu v Petrohrade, ktorá sa zaoberá online vplyvovými a dezinformačnými kampaňami s cieľom presadzovať ruské obchodné a politické záujmy. Agentúra sídli v dvojposchodovej budove, pričom časť zamestnancov, ktorá pracuje na prízemí, vytvára falošné správy a dezinformácie,

---

[6] Barsotti Scottie, „Heinz College Experts Discuss Troll Farms, Fake News", Carnegie Mellon University, 2019, https://www.cmu.edu/news/stories/archives/2019/february/experts-discuss-fake-news.html

[7] Yiu Yuen, „Battling Online Bots, Trolls and People", Inside science, 2018, https://www.insidescience.org/news/battling-online-bots-trolls-and-people

[8] Dawson Andrew, Innes Martin, „How Russia's Internet Research Agency Built its Disinformation Campaign", The Political Quarterly, 2019, https://orca.cardiff.ac.uk/122489/1/Political%20Quarterly%20IRA%20Dawson%20&%20Innes.pdf

zatiaľ čo ich kolegovia na prvom poschodí vytvárajú hodnoverné falošné profily. S ich pomocou následne predmetné dezinformácie šíria na sociálnych sieťach. V roku 2015 údajne pre túto troliu farmu pracovalo až 1000 zamestnancov.

Existuje väčšie množstvo stratégií, ako oslabiť vplyv profesionálnych trolov. Viaceré sociálne siete vrátane Facebooku začali v tejto súvislosti označovať platené politické reklamy a vyžadovať overenie používateľov, ktorí prevádzkujú populárne stránky. Aj keď žiadny z týchto protokolov nedokáže úplne odstrániť dezinformácie na internete, podľa Robyn Caplanovej, expertky na sociálne médiá z Data and Society Research Institute v New Yorku, poskytujú určitú mieru ochrany. „Ak webová stránka vyžaduje telefónne číslo na overenie účtu, znamená to, že na vytvorenie falošného účtu si budete musieť kúpiť telefón na jedno použitie, čo predstavuje dodatočnú investíciu," uviedla Caplanová[9].

Experti však v tejto súvislosti varujú, že ide o potenciálne dvojsečnú stratégiu, keďže odstraňovanie anonymity z internetu môže prispieť k posilneniu jeho kontroly zo strany štátov.

Boti: Stávka na kvantitu

Zásadnú úlohu pri dezinformačných kampaniach zohrávajú aj už spomínaní boti. Na rozdiel od bežných používateľov, ktorí šíria falošné správy vedome alebo nevedome, nie sú boti fyzickými entitami. **Ide o počítačové algoritmy, existujúce na sociálnych sieťach, ktoré niekto naprogramoval tak, aby autonómne a opakovane vykonávali určité zadanie**. Dokážu pri tom stimulovať správanie bežných užívateľov sociálnych sietí.

Boti na Twitteri sú napríklad schopní veľkého množstva sociálnych interakcií, ktoré im umožňujú budiť dojem, že ide o bežných užívateľov. Sú naprogramovaní tak, aby dokázali odpovedať na otázky. Dokážu tiež vyhľadávať vplyvných užívateľov sociálnej siete a klásť im otázky tak, aby boli videní a naberali sledovateľov. Paralelne s tým stimulujú diskusiu tým, že zverejňujú príspevky o populárnych a sociálnou sieťou promovaných témach. Popri tom všetkom aktívne zdieľajú a šíria falošné správy medzi bežnými užívateľmi. Podľa výskumu uskutočneného Pew Research Center v roku 2018 boli za až dve tretiny interakcií pri populárnych témach na Twitteri zodpovední práve boti[10]. V porovnaní s trolmi sú boti ľahšie odhaliteľní a vo všeobecnosti menej vierohodní, pričom **sú najmä šíriteľmi dezinformácií a nie ich primárnymi tvorcami**. Využívanie botov je tak zamerané viac na kvantitu než na kvalitu.

Výskumníci tiež v poslednom čase zaznamenali, že boti sa v súčasnosti už neobmedzujú na jednoduché posielanie a zdieľanie tweetov, ale vývojári ich naprogramovali tak, že sa chovajú omnoho nenápadnejšie a podobnejšie bežným ľudským používateľom[11].

---

[9] Yiu Yuen, 2018

[10] Klepper David, „Cyborgs, Trolls and bots: Guide to online misinformation", Asociated Press, 2020, https://apnews.com/article/us-news-ap-top-news-elections-social-media-technology-4086949d878336f8ea6daa4dee725d94

[11] Yiu Yuen, 2018

Ako ukázala štúdia „Detecting Bots on Russian Political Twitter" zverejnená v žurnále Big Data[12], botov môžu pomocou ich špecifických charakteristík po zaškolení odhaliť aj bežní ľudia. Medzi takéto charakteristiky patrí absencia profilovej fotky alebo fotografia z fotobanky, používateľské meno s priveľa číslami, alebo neobvykle všeobecný popis profilu. Medzi jemnejšie detaily patrí napríklad priveľký nepomer medzi množstvom priateľov a sledovateľov, prípadne tweety obsahujúce výhradne text bez fotografií. V minulosti bolo možné botov odhaliť aj vďaka tomu, že sa vyznačovali abnormálne veľkým množstvom príspevkov, ktoré denne zverejňovali. V rámci rovnakého výskumu následne vedci skombinovali algoritmy strojového učenia s údajmi spravovanými ľudskými kódovačmi a vytrénovali tak počítače na analýzu takmer štvrť milióna účtov na Twitteri, ktoré v rokoch 2014 a 2015 tweetovali viac ako pätnásťmiliónovkrát. Zistili, že z 250 000 účtov bolo 97 000 aktívnych počas celého obdobia, z ktorých zhruba dve tretiny môžu byť boti.

Kyborgovia ako nový hybrid

Prostriedkom zvýšenia efektivity botov sa okrem mikrocielenia stalo aj vytvorenie tzv. *kyborgov*. V prípade kyborga ide o **hybridný účet, ktorý kombinuje neúnavnosť bota s ľudskou jemnosťou**. Za kyborgské sú považované **účty botov, nad ktorými kontrolu pravidelne preberá skutočný človek**, aby mohol reagovať na ostatných používateľov a uverejňovať pôvodný obsah[13]. Ich prevádzka je na jednej strane drahšia a časovo náročnejšia, no vo výsledku pôsobia takéto účty omnoho autentickejšie. Ide do určitej miery o kombináciu bota s trolom.

Falošné účty s tvárou aj bez nej

Ďalšími dvoma dôležitými nástrojmi z hľadiska tvorby a šírenia sú *falošné účty na jedno využitie* (po anglicky „Single use burner accounts") a *falošné osobnosti* (po anglicky „Fake personalities"). Oba nástroje sú vo svojej podstate protiklady s vlastnými špecifickými výhodami a slabinami.

V prípade **falošných účtov na jedno využite** ide o **účty, ktoré zdieľajú len jednu falošnú správu a následne zanikajú**. Ich najväčšou nevýhodou je veľmi malá virálnosť. Takýmito profilmi zdieľané posty sú len veľmi málo zdieľané reálnymi cieľovými užívateľmi. Ich výhodou však je praktická nemožnosť vystopovať pri ich použití pôvodný zdroj dezinformácií a zadávateľa dezinformačnej kampane[14].

Naopak **falošné osobnosti** predstavujú veľmi **starostlivo vypracované falošné profily v skutočnosti neexistujúcich blogerov, novinárov alebo analytikov s vlastnou biografiou a taktiež za pomoci umelej inteligencie vytvorenou profilovou fotografiou**. Tá môže byť vytvorená skombinovaním detailov fotiek skutočných ľudí. V porovnaní s falošnými účtami na jedno použitie majú podobné kampane väčšiu virálnosť a sú omnoho dôveryhodnejšie. Na druhej strane je však jednoduchšie odhaliť ich zdroj a eliminovať ich.

---

[12] Ibid.

[13] Klepper David, 2020

[14] Nimmo Ben, Francois Camille, et. al, „Secondary Infection", Graphica, 2020, https://secondaryinfektion.org/

Ako príklad môžu poslúžiť niektoré články v redakčnej rubrike stránky Sputnik.md, ktoré boli podpísané menami neexistujúcich osôb. Články v redakčnej rubrike podpísané Elenou Komolovou a Nikou Gončarovou propagujú proruské strany a bývalého proruského prezidenta Igora Dodona, kritizujú proeurópskych politikov, ako aj EÚ, MMF a USA, diskreditujú nezávislé médiá a mimovládne organizácie. Overovači faktov však dokázali[15], že autori s takýmito menami neexistujú, pričom fotografia jedného z „autorov" prezentovaných na stránke bola vytvorená počítačom skombinovaním fotografií dvoch známych osobností z Ruska. Podobné prípady boli v nedávnej minulosti zaznamenané aj v Gruzínsku.

Nie je Fox news ako Fox news

Dôležitým prostriedkom tvorby a šírenia dezinformácií sú tiež už *podvodné spravodajské weby*. Ide o **spravodajské stránky, ktoré sú vo svojej podstate úplne falošné, pričom však napodobňujú reálne etablované spravodajské kanály**. Často majú webové adresy, ktoré sú takmer totožné s adresami skutočných spravodajských webov. Ako príklad môže poslúžiť stránka Fox-news24.com, ktorá sa tvárila ako stránka spravodajskej stanice Fox News. Tá však mala skutočnú adresu foxnews.com[16]. Vďaka predmetnej stratégii má možnosť uvidieť dezinformácie na sociálnych médiách obrovské množstvo ľudí ešte predtým, než je podvod odhalený. Navyše môžu dezinformácie zverejnené podvodnými spravodajskými webmi zverejniť z nedbanlivosti aj skutočné spravodajské portály, čo dezinformácií výrazne pridá na dôveryhodnosti a vplyve.

Armáda nevedomých pešiakov

Hoci šesť vyššie uvedených príkladov nedokáže v plnej miere obsiahnuť všetky spôsoby tvorby a šírenia dezinformačných kampaní, ilustrujú rozmanitosť nástrojov, ktorými ich organizátori disponujú. Táto skutočnosť má priamy vplyv na množstvo stratégií, ktoré môžu tvorcovia dezinformačných kampaní zvoliť tak, aby dosiahli vo vzťahu k cieľovému štátu, prípadne skupine, čo najvyššiu mieru efektivity.

Podstatným faktorom v tomto smere však zostáva často prehliadaná skutočnosť, že najaktívnejšími šíriteľmi dezinformácií často nie sú trolovia ani boti. Tí zohrávajú kľúčovú úlohu najmä v prvotných fázach životného cyklu dezinformácie. Za najmasívnejšie šírenie dezinformácií sú neraz zodpovední takzvaní *nevedomí agenti* (po anglicky „unwitting agents"). **Ide o bežných užívateľov internetu, ktorí z rôznych príčin dezinformáciám veria a ďalej ich šíria, pričom sa tak nevedome stávajú nástrojom dezinformačnej kampane**[17].

---

[15] Stop Fals, „Editorialist cu identitate falsă pe site-ul Sputnik de la Chișinău", 2019, https://stopfals.md/ro/article/editorialist-cu-identitate-falsa-pe-site-ul-sputnik-de-la-chisinau-180194

[16] McElroy Damien, „Fox News 24 site is latest ploy in fake news", The National News, 2018, https://www.thenationalnews.com/world/europe/fox-news-24-site-is-latest-ploy-in-fake-news-1.696661

[17] Starbird Kate, „Disinformation's spread: bots, trolls and all of us", Nature, 2019, https://www.nature.com/articles/d41586-019-02235-x

Nástroje posilnenia dosahu dezinformačných kampaní

Štátnymi aktérmi organované dezinformačné kampane sa do značnej miery prelínajú s komerčným marketingom, podvodnou trestnou činnosťou, psychologickou vojnou a politickou vojnou, pričom v rôznych kombináciách obsahujú ich prvky. Ich základom je pritom sociálne inžinierstvo, ktoré manipuluje s jednotlivcami aj s celými skupinami.

Clickbait, sponzorovanie príspevkov (po anglicky „boosting") alebo profilu a *mikrocielenie* (po anglicky „microtargeting") využívajú firmy, ako aj celebrity na zvýšenie pozornosti zo strany cieľových skupín. *Klonovanie profilov* (po anglicky „profile cloning") a mikrocielenie používajú tiež zločinecké skupiny, ako prostriedky na krádež údajov. *Informačný šum* (po anglicky „information noise") je prirodzeným sprievodným javom činnosti, ako štandardných, tak aj falošných médií.

Aj vďaka tomu, že dezinformačné kampane využívajú existujúce problémy informačných zdrojov a platforiem, je pomerne náročné im efektívne vzdorovať. Uvedomenie si skutočnosti, že väčšina dezinformačných stratégií využíva vrodené chyby v komunikácii a distribúcii informácií, je zároveň prvým krokom k tomu, aby zodpovedné bezpečnostné organizácie a tretí sektor dokázali odlíšiť prirodzené dôsledky týchto chýb od dezinformačných kampaní.

Aby informáciu videl každý

Clickbait je termín, ktorý sa používa na **opis online obsahu navrhnutého tak, aby pritiahol čitateľov prostredníctvom sexuálne explicitných, emocionálne nabitých, násilných alebo politických ladených titulkov a obrázkov**. Hoci je clickbait eticky pochybný, je rozšírený a väčšina platforiem ho toleruje. Dá sa ľahko identifikovať podľa nasledujúcich charakteristík: **ide o sponzorovaný obsah**, ktorý používa **veľké množstvo zámen** (môj, jej, jeho atď.), ako aj **dramatický alebo emotívny jazyk**, ktorý je zámerne **jednoduchý**. Sprevádzajú ho tiež **pútavé snímky**, alebo ilustrácie. Clickbait sa zvyčajne objavuje v reklamných sekciách webových stránok, často vo forme sponzorovaného obsahu (t. j. vlastníkovi webových stránok bol zaplatený poplatok za jeho distribúciu). Taktiež mnohé médiá a reklamné organizácie používajú taktiky, ktoré spĺňajú definíciu clickbaitu s cieľom zvýšiť návštevnosť svojich webových stránok.

V dezinformačných kampaniach je využívaný tzv. **politický alebo spravodajský clickbait**. Témy aktuálneho spravodajstva z verejného života sú za pomoci clickbaitu pretkané nepravdivými informáciami navrhnutými tak, aby stimulovali predsudky čitateľov. Spravodajský clickbait pritom môže byť využívaný nie len médiami na zvýšenie čítanosti, ale aj štátnymi aktérmi ako prostriedok posilnenia dezinformačných kampaní[18].

Úlohou clickbaitu v štátom vedených dezinformačných kampaniach je cieľovú skupinu alebo

[18] Cvetkovska Saska, "Trump and COVID-19 fuel North Nacedonia's clickbait boom", Balkan Insight, 2020, https://balkaninsight.com/2020/11/02/trump-and-covid-19-fuel-north-macedonias-clickbait-boom/

spoločnosť polarizovať prostredníctvom šírenia strachu a nenávisti, zmiasť ju stimuláciou vzniku informačného šumu, prípadne poštvať voči inému štátu alebo organizácii.

Nepozornosť, prípadne senzáciechtivosť zo strany novinárov a mediálnych organizácií môže viesť k tomu, že dezinformácie obsiahnuté v clickbaitovom článku začlenia do svojho spravodajstva, čím ich nie len šíria ďalej, ale aj legitimizujú.

Sponzorovanie príspevkov vo význame boostingu je ďalšou morálne pochybnou, avšak legálnou možnosťou, ako môžu jednotlivci, organizácie, ale aj štátny aktéri zvýšiť svoju viditeľnosť a vplyv na sociálnych sieťach a internetových platformách. Dosiahnuť ho možno dvoma spôsobmi, **pomocou botov a pomocou platených prispievateľov**.

Využitie botov sa mierne líši v závislosti od cieľovej platformy. V prípade sponzorovania obsahu na internetovej databáze videí YouTube boti pridávajú pod videá klienta lajky, komentáre a podpisujú sa na jeho kanál. Na twitteri budú zas klientov obsah okrem podpisovania sa, lajkovania a komentovania aj ďalej zdieľať prostredníctvom retweetu. Boti sú väčšinou na tento účel prenajímaní jednotlivcami alebo organizáciami, ktoré predmetnú službu otvorene ponúkajú a reklamujú.

Vzhľadom na neraz neautentické správanie sa botov je tento spôsob sponzorovania možné pomerne jednoducho odhaliť. Podobne sponzorované profily charakterizuje tiež skutočnosť, že sledovatelia im nepribudli postupne, ale náhle a v nezvyčajne vysokom množstve.

V druhom prípade organizácie s cieľom podporiť nevypúšťajú armádu botov, ale platia skutočným ľuďom, aby zvyšovali mieru interakcie na cieľových stránkach a profiloch podobným spôsobom, ako to robia boti. Na túto úlohu sú často najímaní ľudia s potrebnou jazykovou výbavou, ktorí žijú v chudobnejších štátoch s vysokou mierou nezamestnanosti.

Hoci skutoční ľudia nedokážu vytvoriť také množstvo interakcií ako boti, **ich interakcie sú omnoho autentickejšie, a teda kvalitatívne na omnoho vyššej úrovni**. Taktiež sa pohybujú pod radarmi algoritmov, ktoré využívajú sociálne siete na odhaľovanie botov.

Okrem komerčných účelov je takéto sponzorovanie často využívané aj organizátormi dezinformačných kampaní na zvyšovanie viditeľnosti ich naratívov ako aj ich efektívnejšie šírenie smerom od nimi zriadených skutočných, falošných a klonovaných profilov[19].

Aby informáciu videl ten, kto má

Kľúčovým nástrojom pre zvýšenie efektivity dezinformačných kampaní je využitie takzvaných „big data" a analýzy v rámci *mikrocielenia* (po anglicky „microtargeting").

[19] Thomas Elise, Zhang Albert, & Wallis Jake "COVID-19 disinformation and social media manipulation: automating influence on COVID-19", International Cyber Policy Centre, 2020.,

Tvorcovia falošných správ dokážu prostredníctvom mikrocielenia zasiahnuť konkrétnou správou tých užívateľov, ktorí sú najnáchylnejší jej uveriť, prípadne ktorých správanie a postoje môže najviac ovplyvniť. Umožňujú to najmä **súbory cookies**.

Ide o malé súbory, ktoré sa uložia na počítač alebo mobilné zariadenie v prípade, že tak určí webová stránka, ktorú používateľ navštívi. Tieto súbory obsahujú informácie o tom, z ktorej webovej stránky pochádzajú, ako dlho majú byť uložené na vašom zariadení a taktiež uchovávajú nejakú hodnotu, napríklad zvolený jazyk stránky.

Internetové stránky väčšinou používajú cookies na identifikáciu používateľa. Keď ten príde na stránku prvýkrát, vytvorí sa cookie s hodnotou X, ktorá je unikátna práve pre jeho zariadenie (samozrejme v praxi sa používa hodnota s viacerými znakmi, aby ju nebolo možné uhádnuť). Táto cookie sa nazýva **relačná**. Ak túto stránku navštívi používateľ znova, jeho prehliadač odošle relačnú cookie s hodnotou X a server s danou stránkou bude vedieť, že je to práve on, pretože iba jeho relačná cookie má hodnotu X. Pomocou cookies dokážu sociálne siete a analytické spoločnosti sledovať a vyhodnocovať preferencie užívateľov a zisťovať tak s pomerne veľkou presnosťou akú reklamu alebo informácie na nich cieliť[20].

Stránky, ktoré zhromažďujú najviac osobných údajov, sú bezplatné služby, ako je Facebook, Twitter, YouTube a TikTok, kde používatelia dobrovoľne poskytujú množstvo osobných informácií od mien a veku až po ich jedinečné črty tváre a ich politické presvedčenie. Ako príklad efektivity tohto nástroja môže poslúžiť muž, ktorému Facebook ponúkal literatúru o tom, ako sa okoliu priznať k homosexuálnej orientácii v čase, keď takýto krok ešte len zvažoval[21].

Prípad spoločnosti Cambridge Analytica, ktorá údajne pomocou botov a mikrocielenia dokázala ovplyvniť Brexit aj americké prezidentské voľby v roku 2016, ukázal, že ide o potenciálne silný nástroj ovplyvňovania verejnej mienky. O to viac, že mikrocielenie býva využívané aj na efektívnejšie šírenie falošných správ[22].

Operáciám mikrocielenia je veľmi ťažké brániť sa, pričom jediným realistickým prostriedkom je prepracovanie zákonov o ochrane údajov. Avšak vzhľadom na komerčný záujem o používanie mikrocielenia na reklamu to bude ťažké dosiahnuť.

Zdanie dôveryhodnosti

Sponzorovanie príspevkov nie je jediným nástrojom zvyšovania zdanlivej dôveryhodnosti informácie a jej šíriteľa. Jedným z najdôležitejších je vyššie spomínané **klonovanie profilov**. Ide

[20] Citadelo.sk, „ČO SÚ COOKIES, NA ČO SLÚŽIA A MÁME SA ICH BÁŤ?“, 2018, https://citadelo.com/sk/blog/co-su-cookies-na-co-sluzia-a-mame-sa-ich-bat/

[21] Gaymoli, Chris, “How Facebook knew a man was gay before he came out”, The Week, 2015, https://theweek.com/articles/466504/how-facebook-knew-man-gay-before-came

[22] Dawson, J., “Microtargeting as Information Warfare”. The Cyber Defense Review, 6(1), 63–80., 2021, https://www.jstor.org/stable/26994113

o podvodný krok, pri ktorom útočník vytvorí falošný profil existujúcej osoby, organizácie alebo skupiny. Takto vytvorený profil následne využíva legitimitu a vzťahy pôvodného profilu.

Klonovanie účtu môže mať dve formy. V prvom prípade je účet **klonovaný na tej istej platforme**, kde sa nachádza aj pôvodný účet. Cieľom je väčšinou získať od kontaktov pôvodného účtu podvodný spôsobom finančné prostriedky alebo informácie. Táto metóda však môže byť použitá aj pri dezinformačných kampaniach, keď dodáva dezinformáciám šíreným z klonovaného účtu legitimitu pôvodného profilu. Profily klonované na tej istej platforme, kde sa nachádza aj pôvodný profil sú väčšinou odhalené v pomerne krátkom čase.

Pri druhom type je postup v prvej etape rovnaký s tým, že klon vytvorený na rovnakej platforme ako pôvodný profil nie je využívaný na získanie finančných prostriedkov, prípadne legitimáciu dezinformácií. Jeho jediným cieľom je získať maximálne množstvo informácií o pôvodnom profile. **Takto získané informácie sú následne využité pri vytvorení ďalšieho klonovaného profilu, avšak na inej platforme, kde pôvodný profil neexistuje**. Prepracovaný klonovaný profil sa tak následne stane jediným reprezentantom cieľovej osoby, organizácie alebo skupiny na danej platforme, čím už od začiatku pôsobí omnoho dôveryhodnejšie[23]. Profil môže byť následne využívaný na šírenie dezinformácií, pričom v danom prípade je pomerne náročné ho včas odhaliť. Druhý typ klonovaného profilu sa oproti prvému typu tiež omnoho lepšie hodí na poškodenie reputácie pôvodného profilu. Často preto býva využívaný pri útokoch na rešpektované osobnosti a organizácie.

Informačný šum

Takmer všetky taktiky dezinformačných kampaní prispievajú v rôznej miere ku vzniku informačného šumu, teda **nepotrebných údajov a informácií, ktoré znečisťujú informačný priestor** a platformy. Informačný šum sám o sebe je prirodzeným fenoménom, ktorý vzniká, hoci v menšej intenzite, aj v dôsledku bežného spravodajstva.

Informačný šum má z hľadiska dezinformačných kampaní **dve využitia**. Tvorcovia takýchto kampaní ho využívajú ako formu intelektuálnej dymovej clony, v ktorej sa strácajú reálne fakty. Dezinformačné kampane sa tak často snažia umelo posilňovať informačný šum vytváraním veľkého množstva kontranaratívov[24].

V prvom prípade môže **posilnenie informačného šumu vytvoriť priestor pre iné útočné vplyvové operácie**. Informačný šum môže v takom prípade napomôcť nanovo interpretovať inak nepriateľské aktivity útočiaceho štátu ako „mierotvornú misiu" alebo „spontánnu aktivitu miestnych povstalcov". Túto taktiku použilo Rusko pri vytváraní naratívu okolo prítomnosti jeho ozbrojených síl na východnej Ukrajine.

---

[24] Gregor Miloš, Mlejnková, Petra, "Challenging online propaganda and disinformation in the 21st century" Palgrave Macmillan, 2021.

V druhom prípade je **vytvorenie intenzívneho informačného šumu samo o sebe hlavným cieľom**. Mnohí prijímatelia informácií totiž v záplave protichodných naratívov často rezignujú na hľadanie pravdy. Príkladom môže byť informačný šum vytvorený po zostrelení letu MH-17 na východe Ukrajiny v roku 2014, pričom Rusko o tejto udalosti šíri hneď niekoľko protichodných dezinformácií. Cieľom je, aby sa čitateľ stratil vo veľkom množstve rôznych verzií a rezignoval na hľadanie pravdivej verzie udalostí. Verdikt medzinárodnej vyšetrovacej komisie o tom, že za útokom stálo Rusko, sa tak pre mnohých konzumentov stáva len jednou z možných verzií udalosti.

Dezinformácie a štrukturálne problémy sociálnych sietí

Tento stručný popis nástrojov využívaných na posilnenie vplyvu dezinformácií na cieľovú spoločnosť nám načrtáva hlavnú slabinu budovania odolnosti voči nim. Sú ňou do značnej miery štrukturálne problémy sociálnych sietí. Úlohou štátov by v tomto smere preto mala byť užšia spolupráca so sociálnymi sieťami na odstraňovaní medzier v systémoch, ktoré sú zneužívané nielen organizátormi dezinformačných kampaní, ale aj kriminálnymi živlami. Štáty by tiež mali zamerať svoju pozornosť na otázku zberu ohromného množstva údajov o používateľoch sociálnych sietí.

Záver

Pochopenie anatómie dezinformačných kampaní vrátane hlavných stratégií a nástrojov, ktoré využívajú, je len prvým krokom na ceste k budovaniu väčšej odolnosti voči tomuto typu hybridných hrozieb. Nemenej dôležitá je identifikácia efektívnych stratégií a nástrojov, ako jednotlivé kampane neutralizovať čo najskôr a pri využití čo najmenšieho množstva ľudských aj finančných zdrojov. Hoci ich identifikácia, analýza a hodnotenie presahujú možnosti a ambície tejto štúdie, analýza vyššie popísaných nástrojov dezinformačných kampaní nám umožňuje definovať aspoň **tri priority** v boji proti nim.

Prvou by malo byť **jasné zadefinovanie jednotlivých pojmov súvisiacich s hybridnými hrozbami** na štátnej, prípadne celoeurópskej úrovni. Slovensko v tomto smere podniklo už viaceré úspešné kroky. Spomenúť možno napríklad Krátky slovník hybridných hrozieb , ktorý vznikol z iniciatívy Národného bezpečnostného analytického centra - analytického, komunikačného a kooperačného pracoviska Slovenskej informačnej služby. Ustálené zadefinovanie pojmov na úrovni dokumentov a slovníkov je však len jedným z krokov. Po ňom by v tomto smere malo nasledovať vzdelávanie širšej odbornej, ale aj laickej verejnosti, s cieľom zabrániť nejasnostiam, nedorozumeniam, ktoré v diskurze o dezinformáciách spôsobuje nedostatočné pochopenie základných pojmov.

V rámci druhej priority by sa štát mal zamerať na **vzdelávanie obyvateľstva s cieľom zvýšiť jeho odolnosť voči dezinformačným kampaniam a iným vplyvovým operáciám cudzích mocností**. To by sa primárne nemalo zakladať na produkovaní a šírení vlastných naratívov, ale na zvyšovaní schopnosti obyvateľstva kriticky myslieť a overovať informácie bez ohľadu na ich zdroj. Práve armáda bežných užívateľov internetu, šíriaca dezinformácie nevedome, je základom úspechu mnohých dezinformačných kampaní.

V neposlednom rade sa ako nevyhnutnosť ukazuje už spomínaná **užšia spolupráca so sociálnymi sieťami** pri snahe identifikovať a napraviť systémové chyby, ktoré úspešné dezinformačné kampane, ale aj trestné činy umožňujú v takej miere, v akej sme svedkami v súčasnosti. Motivácia technologických gigantov pristúpiť k takýmto krokom však nie je samozrejmosťou. Preto je v tomto smere nevyhnutná koordinácia úsilia jednotlivých štátov, ktoré sú hybridným útokom vrátane dezinformačných kampaní najviac vystavené.

Slovník iných často používaných termínov

A.

Ačohentizmus (po anglicky: „Whataboutism“)
Klamný argument pri ktorom dochádza namiesto odpovede na otázku ku zmene témy. V tomto príklade ide konkrétne o obrátenie obvinenia, pri ktorom rečník tvrdí, že druhá strana je zodpovedná za rovnakú, prípadne ešte vážnejšiu chybu alebo zločin, než z akej bol pôvodne obvinený on. Vyhne sa pritom akémukoľvek vyjadreniu k pôvodnej téme diskusie.

Argument ad hominem
Falošná argumentácia, pri ktorej sa osoba namiesto reakcie na argumenty protivníka zameria na osobný útok voči nemu, resp. skupine alebo inštitúcii, ktorú reprezentuje.

Argument šikmou plochou (po anglicky: „Slippery slope argument“)
Falošná argumentácia, pri ktorej dochádza k zamietnutiu určitého aktu alebo procesu nepodložene tvrdiac, že by automaticky viedol k sledu nežiaducich udalostí s nežiaducim výsledkom.

Astroturfing
Ide o fenomén vytvárania umelej verejnej podpory. V súčasnej dobe je využívaný najmä na internete, pričom jeho cieľom je imitovať širokú podporu verejnosti pre určitých ľudí, organizácie alebo ich aktivity. Pojem Astroturfing má pôvod v názve americkej spoločnosti AstroTurf, ktorá vyrábala umelé trávniky pre štadióny. Tak ako ona napodobňovala trávu, rovnako je vykonštruovaná verejná iniciatíva napodobňujúca tú skutočnú.

Asymetrická hrozba (po anglicky: „Asymmetric threat“)
Hrozba, ktorá sa uskutočňuje neobyčajným alebo obskúrnym spôsobom, zvyčajne prichádzajúca od zdroja, ktorý je značne slabší ako jej cieľ.

Atribúcia (po anglicky: „Attribution“)
Pripisovanie významu objektu alebo situácii, napr. priradenie skutku konkrétnemu aktérovi.

D.

Dôveryhodnosť (po anglicky: „Reliability“)
Dôveryhodnosť informácie nám určuje, do akej miery môžeme informácii dôverovať, že je pravdivá. Indikátorom miery dôveryhodnosti môže byť to, či sa pod článok ako autor podpísala reálna osoba, či je možné dopátrať sa k pôvodnému zdroju, alebo to, či správu zdieľajú viaceré médiá.

Dôkaz slobodou (po anglicky: „Probans libertate“)
Chybné argumentovanie slobodou slova k obhájeniu svojich postojov alebo k diskreditácii postojov oponenta.

E.

Efekt rozbehnutého vlaku (po anglicky: „Bandwagon effect“)
tendencia osvojiť si určitý štýl, názor, postoj, z dôvodu, že ho má aj okolie.

Elf
Osoba odhaľujúca dezinformácie, ich pôvodcov a trolov. Opak trola.

F.

Falošná dilema (po anglicky: „False choice“)
Argumentačná technika, pri ktorej sú na výber ponúknuté len dve možnosti bez prihliadnutia na ostatné relevantné alternatívy (napr. New York buď miluješ, alebo nenávidíš).

Falošný kompromis, klam strednej cesty
(po anglicky: „False compromise, Middle ground fallacy“)
Nepresné zjednodušené tvrdenie, podľa ktorého je tvrdenie nachádzajúce sa v strede medzi dvoma extrémami pravdivé a priori preto, že sa nachádza v strede.

Falošný rozhodca (po anglicky: „Fallacy-Fallacy“)
Predpoklad, že výrok, ktorý bol nesprávne vyargumentovaný protivníkom, musí byť nevyhnutne nesprávny. Účastník diskusie sa pri tejto technike stavia do roly rozhodcu, pričom poukazom na jeden nesprávny argument svojho oponenta spochybní celý jeho výrok ako taký.

I.

Ilúzia zhlukovania (po anglicky: „Clustering illusion“)
Tendencia ľudí vidieť súvislosti a trendy v udalostiach a javoch, ktoré spolu nesúvisia, len nasledujú za sebou alebo sa udejú naraz.

Inbetweeners
Osoby, ktoré nemajú v množstve spoločensky dôležitých otázok žiaden názor a riadia sa tézou, že pravda je niekde v strede.

Informačné operácie (po anglicky: „Information operations“)
Tiež vplyvové operácie, spočívajú v zhromažďovaní taktických informácií o protivníkovi, ako aj rozširovanie propagandy s cieľom nadobudnúť konkurenčnú výhodu oproti protivníkovi.

Informačné preťaženie (po anglicky: „Information overload“): Ide o stav, keď je človek zahltený priveľkým množstvom informácií, z ktorých je veľká časť nepotrebná. Daný stav vedie často k neschopnosti uskutočniť rýchle a racionálne rozhodnutie a spracovávať ďalšie informácie.

K.

Klam neúplných dôkazov (po anglicky: „Cherry picking“)
Manipulačná metóda pri ktorej sa manipulátor snaží cieľovú skupinu presvedčiť o svojich tvrdeniach tým, že vyberá výhradne tie fakty, ktoré týmto tvrdeniam zodpovedajú. Paralelne s tým vedome zamlčiava fakty, ktoré jeho naratívu odporujú.

Konšpiračná teória (po anglicky: „Conspiracy theory“)
Teória, ktorá vysvetľuje určitú udalosť alebo okolnosti ako dôsledok tajného sprisahania mocných osôb alebo organizácií. Prípadne môže ísť o teóriu, podľa ktorej je pred verejnosťou skrývaná nejaká dôležitá skutočnosť.

Kontext (po anglicky: „Context“):
Kontext je vytváraný okolnosťami alebo dodatočnými udalosťami sprevádzajúcimi pre nás zaujímavú udalosť, prípadne fenomén. Zamlčanie, prípadne pokrivenie kontextu umožňuje autorovi zásadne ovplyvniť spôsob, akým bude čitateľ udalosť interpretovať.

Kotvenie (po anglicky: „Anchoring“)
Ide o prirodzenú tendenciu ľudí spoliehať sa pri rozhodovaní primárne na prvú časť ponúknutej informácie („kotvu“). Kotvenie nastáva, ak jednotlivci použijú úvodnú časť informácie pre svoje ďalšie úsudky. Hneď ako je kotva nastavená, následné úsudky sú vykonávané úpravou smerom od kotvy, pričom v okolí kotvy dochádza k skresleniu informácie. Napríklad: Úvodná cena požadovaná za ojazdený automobil nastavuje štandard pre zvyšok rokovania. Ceny nižšie ako pôvodne požadovaná cena následne pôsobia rozumne, hoci môžu byť v skutočnosti omnoho vyššie než je reálna trhová cena.

M.

Mém (po anglicky: „Meme“)
V širšom zmysle ide o „jednotku kultúrneho prenosu“. Môže ísť o nápad, správanie, alebo štýl, ktorý sa šíri od osoby k osobe v rámci určitej kultúry. V kontexte internetu a sociálnych médií sú mémami neraz populárne a virálne obrázky alebo videá s krátkym textom.

Argument pomocou monokauzality (po anglicky: „Single cause argument“)
S monokauzalitou sa stretávame vtedy, ak má jav alebo fenomén len jednu príčinu. Pri dezinformačných kampaniach a manipulovaní argumentovanie pomocou monokauzality znamená, že osoba využívajúca túto techniku zdôrazňuje len jednu príčinu javu a ignoruje ďalšie, ktoré nezodpovedajú jej záverom.

N.

Nabitá otázka (po anglicky: „Loaded question“)
Ide o otázku, ktorá v sebe obsahuje nepotvrdené a často negatívne ladené tvrdenie, na ktoré je možné odpovedať len áno alebo nie. Príklad: „Mali ste vždy problém s hazardnými hrami?“

Nelichotivá asociácia (po anglicky: „Guilt by association“)
Ide o techniku útočenia na argumenty ideového oponenta prostredníctvom poukazovania na jeho príslušnosť k určitej konkrétnej skupine. Je to typ útoku ad hominem, pri ktorom nie je dôraz kladený primárne na individuálnu osobu oponenta, ale jednu zo skupín, ktorej je súčasťou.

Nevyvrátiteľnosť (po anglicky: „Unfalsifiability“)
Ide o techniku podpory vlastného tvrdenia pomocou dôkazu, ktorý nie je možné ani vyvrátiť a ani potvrdiť.

O.

Odpútanie pozornosti (po anglicky: „Red Herring“)
Vedomá snaha o preorientovanie diskusie z témy, ktorá rečníkovi nevyhovuje k téme, pri ktorej dokáže lepšie obhájiť svoje stanoviská.

Overovanie faktov (po anglicky: „Fact-checking“)
V širšom kontexte ide o investigatívnu činnosť s cieľom overiť pravdivosť tvrdení. V kontexte dezinformačných kampaní znamená overovanie faktov cielené odhaľovanie a vyvracanie falošných informácií.

U.

Účet ponožkovej bábky (po anglicky: „Sock puppet account“)
Ide o falošný účet, ktorý si osoba vytvorí na vychvaľovanie seba samého, útok na svojich protivníkov, prípadne vytvorenie sporu na sociálnych sieťach so svojím skutočným profilom s cieľom argumentačne ho vyhrať.

P.

Paródia a satira (po anglicky: „Parody and Satire“)
Ide o staré a dobre etablované žánre, ktorých autori sa nechcú podieľať na šírení dezinformácií. V ére sociálnych sietí sa však bez dostatočnej verifikácie stávajú aj parodické a satirické stránky neraz nástrojom dezinformačných kampaní. Dochádza k tomu vtedy, ak ich používatelia či už vedome, alebo nevedome zdieľajú ako skutočné zdroje.

Psychologická operácia (po anglicky: „Psychological operation, PSYOP“)
Psychologické operácie sú aktivity uskutočňované s cieľom manipulovať cieľovú populáciu, aby sa správala, myslela a konala tak, ako si želá útočník. Ich súčasťou býva propaganda a dezinformácie, avšak využívajú aj pravdivé informácie, umenie a iné aktivity. Psychologické operácie sa často zameriavajú na využívanie polarizácie, kultúrnych, rasových a etnických rozdielov už existujúcich v spoločnosti.

Propaganda
Idey alebo tvrdenia, ktoré sú často nepravdivé alebo prehnané, pričom šírené sú s cieľom pomôcť nejakej kampani, politikovi alebo vláde.

Proxy a štátom sponzorované médiá (po anglicky: „Proxy and state-controlled media“)
Zvyčajne sú založené, financované a otvorene spojené s agresorským štátom. Proxy spravodajské kanály sú zvyčajne menej viditeľne spojené s agresorským štátom a sú založené v štáte, ktorý je cieľom dezinformačných kampaní. Obe sú zdanlivo spravodajské siete, ktoré majú inú perspektívu ako „západné“ médiá. Zapájajú sa však do dezinformačných kampaní využívaním selektívneho spravodajstva, propagáciou konšpiračných teórií, prekrývaním rozdeľujúcich príbehov a hosťovaním okrajových alebo kontroverzných osobností. Štátom sponzorované siete sa zriedka zameriavajú na domáce publikum svojho sponzora, čo dokazujú jazyky, v ktorých sa rozhodnú vysielať. Často sa líšia od ostatných štátom sponzorovaných správ v kvalite spravodajstva aj objektivite.

R.

Rámcovanie (po anglicky: „Framing“)
Rámcovanie je kognitívna chyba, pri ktorej si prijímateľ vyberá medzi viacerými informáciami viac na základe toho, akým spôsobom mu boli podané, než na základe ich faktickosti a logickosti.

S.

Slamený panák (po anglicky: „Straw man“)
Ide o formu argumentu, ktorý vyvoláva dojem vyvrátenia argumentu oponenta, zatiaľ čo skutočný

predmet argumentu nebol adresovaný alebo vyvrátený, ale bol nahradený falošným. Môže sa tak stať napríklad, ak je argument oponenta prevzatý, prehnaný a následne vyvrátený vo svojej prehnanej podobe.

Spolucestujúci (po anglicky: „Fellow traveller")
Na rozdiel od nevedomých agentov, „spolucestujúci" sa na dezinformačnej kampani cudzieho štátu podieľajú dobrovoľne a plne vedome. Užitoční idioti a spolucestujúci najmä v podobe dobre organizovaných skupín dokážu posilniť už existujúci informačný šum.

Stereotypizácia (po anglicky: „Stereotyping")
Generalizácia charakteristík veľkej skupiny ľudí. Súčasťou stereotypov môžu byť fyzické, povahové, emocionálne, intelektuálne a iné charakteristiky, ktoré môžu mať pozitívny aj negatívny charakter. Často ide o zjednodušenie alebo pokrivenie kultúrnych charakteritík.

Strategická komunikácia (po anglicky: „Strategic communication, STRATCOM")
Komunikácia, ktorá cielene podporuje strategický zámer, alebo požiadavky misie.

Stred pozornosti (po anglicky Spotlight fallacy)
Ide o chybu úsudku, pri ktorom človek automaticky predpokladá, že udalosti, ktoré dostávajú viac priestoru v médiách, sú častejšie než tie, ktoré dostávaj priestoru menej. Táto chyba úsudku môže zásadne ovplyvniť požiadavky obyvateľstva voči vláde. V praxi tak niektoré vlády vyčleňujú viac finančných rozpočtov na boj proti terorizmu, než na prevenciu voči záplavám a efektívnu reakciu na ne. A to aj napriek tomu, že záplavy sa dejú častejšie než teroristické útoky a spôsobujú omnoho väčšie škody.

V.

Verifikácia (po anglicky: „Verification")
Jedným z hlavných cieľov verifikácie na sociálnych sieťach je overenie si, či zdroj je tým, za koho alebo za čo sa vydáva. Týka sa to najmä verejne známych osôb ako sú politici, novinári a experti. Viaceré sociálne siete, ako napríklad Twitter, potvrdzujú pravosť oficiálnych profilov takýchto osôb, aby daný profil odlíšili od profilov parodických a falošných.

Vplyvová operácia (po anglicky: „Influence operation")
Ide o operácie, pri ktorých útočník zbiera o svojom cieli taktické informácie a následne voči nemu smeruje propagandu a dezinformácie s cieľom získať nad ním výhodu.

Vysoko falošný obsah (po anglicky: „Deepfake")
Za pomoci vyspelého softvéru vytvorené video alebo zvuková stopa, pri ktorých sú tvár alebo hlas určitej osoby nahradené tvárou alebo hlasom inej osoby. Môže poslúžiť na diskreditáciu oponenta.

Vytrhávanie z kontextu (po anglicky: „Quote mining“)
Akt, pri ktorom je citát oponenta prezentovaný bez pôvodného kontextu s cieľom podporiť vlastný argument falošnými dôkazmi alebo diskreditovať oponenta.

Z.

Zaujatosť (po anglicky „Bias“):
Zaujatosť sa prejavuje vtedy, ak autor podporuje konkrétny argument alebo názor, prípadne nedáva priestor druhej strane. V argumentácii sa v takomto prípade nemusia priamo nachádzať nepravdivé informácie alebo dezinformácie. Stačí, ak jedna strana, prípadne argument dostáva neprimerane viac priestoru.

Zavádzajúca dramatizácia (po anglicky „Misleading vividness“)
Nepravdivý predpoklad, že určitá udalosť alebo fenomén sú bežné s poukazom na niekoľko dramatických prípadov. Ako príklad môže poslúžiť aj súčasná diskusia o vakcínach voči ochoreniu COVID-19. Hoci množstvo prípadov vážnych vedľajších účinkov je štatisticky pomerne malé, niekoľko fatálnych prípadov vyvolalo v dôsledku veľkého mediálneho pokrytia u časti spoločnosti dojem, že vakcíny sú omnoho nebezpečnejšie než ukazujú štatistiky. Ide o podobný klamný argument ako v prípade argumentu stredom pozornosti.

Zdroj (po anglicky: „Source“):
Zdroj je prvým pôvodcom informácie. Jej prvý autor alebo prvý portál, na ktorom bola zverejnená. Vedomosť o pôvodom zdroji je pre čitateľa dôležitým nástrojom, pomocou ktorého môže vyhodnotiť dôveryhodnosť informácie.

Zoznam použitej literatúry

Barsotti Scottie, „Heinz College Experts Discuss Troll Farms, Fake News", Carnegie Mellon University, 2019,
https://www.cmu.edu/news/stories/archives/2019/february/experts-discuss-fake-news.html

Citadelo.sk, „ČO SÚ COOKIES, NA ČO SLÚŽIA A MÁME SA ICH BÁŤ?", 2018,
https://citadelo.com/sk/blog/co-su-cookies-na-co-sluzia-a-mame-sa-ich-bat/

Cvetkovska Saska, "Trump and COVID-19 fuel North Nacedonia's clickbait boom", Balkan Insight, 2020, https://balkaninsight.com/2020/11/02/trump-and-covid-19-fuel-north-macedonias-clickbait-boom/

Dawson Andrew, Innes Martin, „How Russia's Internet Research Agency Built its Disinformation Campaign", The Political Quarterly, 2019, https://orca.cardiff.ac.uk/122489/1/Political%20Quarterly%20IRA%20Dawson%20&%20Innes.pdf

Dawson, Jessica, "Microtargeting as Information Warfare". The Cyber Defense Review, 6(1), 63–80., 2021, https://www.jstor.org/stable/26994113

Finneman, Teri, Thomas, Ryan J., "A Family of Falsehoods: Deception, Media Hoaxes and Fake News". Newspaper Research Journal, 39(3), 350-361, September 2018
https://journals.sagepub.com/doi/abs/10.1177/0739532918796228

Gaymoli, Chris, "How Facebook knew a man was gay before he came out", The Week, 2015,
https://theweek.com/articles/466504/how-facebook-knew-man-gay-before-came

Gregor Miloš, Mlejnková, Petra, "Challenging online propaganda and disinformation in the 21st century" Palgrave Macmillan, 2021.

Hybrid CoE, "Hybrid threats as a concept",
https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Kharaji, Morteza Yousefi, Rizi, Fatemeh Salehy, "An IAC Approach for Detecting Profile Cloning in Online Social Networks", International Journal of Network Security & Its Applications (IJNSA),.6(1)., 2014,

Klepper David, „Cyborgs, Trolls and bots: Guide to online misinformation", Asociated Press, 2020, https://apnews.com/article/us-news-ap-top-news-elections-social-media-technology-4086949d878336f8ea6daa4dee725d94

McElroy Damien, „Fox News 24 site is latest ploy in fake news", The National News, 2018,
https://www.thenationalnews.com/world/europe/fox-news-24-site-is-latest-ploy-in-fake-news-1.696661

Melissen Jan, Public Diplomacy, in: Kerr, P., Wiseman, G. (eds.), Diplomacy in a Globalizing World, New York: Oxford University Press, 2013

Národný bezpečnostný úrad, "Hybridné hrozby", 2021, https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html

Národný bezpečnostný úrad, „Krátky slovník hybridných hrozieb", 2021, https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html

Nimmo Ben, Francois Camille, et. al, „Secondary Infection", Graphica, 2020, https://secondaryinfektion.org/

Silverman Craig, Lawence Alander, Buzz Feed News, „How Teens In The Balkans Are Duping Trump Supporters With Fake News", 2016, https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo

Slovenská informačná služba, Národné bezpečnostné analytické centrum: Krátky terminologický slovník HYBRIDNÉ HROZBY, 2020, https://www.sis.gov.sk/o-nas/nbac-slovnik-hh.html

Starbird Kate, „Disinformation's spread: bots, trolls and all of us", Nature, 2019, https://www.nature.com/articles/d41586-019-02235-x

Stengel Richard: Information Wars. New York: Atlantic Monthly Press, 2019

Stop Fals, „Editorialist cu identitate falsă pe site-ul Sputnik de la Chișinău", 2019, https://stopfals.md/ro/article/editorialist-cu-identitate-falsa-pe-site-ul-sputnik-de-la-chisinau-180194

Thomas Elise, Zhang Albert, & Wallis Jake "COVID-19 disinformation and social media manipulation: automating influence on COVID-19", International Cyber Policy Centre, 2020., https://apo.org.au/node/307264

Yiu Yuen, „Battling Online Bots, Trolls and People", Inside science, 2018, https://www.insidescience.org/news/battling-online-bots-trolls-and-people

O nás

Inštitút pre Centrálnu Európu (ICE) spája ľudí, ktorí sú presvedčení, že pre dobré rozhodnutia vo verejnom sektore je potrebná správne vedená odborná diskusia relevantných stakeholderov. ICE vytvára platformu pre diskusiu predstaviteľov verejného života, akadémie a hospodárstva. Prepája výsledky vlastného výskumu s expertízou domácich i zahraničných odborníkov v jednotlivých oblastiach a predostiera návrhy na zlepšenie sektorových politík štátu. Vo svojej činnosti sa inštitút zameriava na rozšírenie tradičného vnútroštátneho prístupu, zohľadňujúc európsky a regionálny kontext. ICE sa sústreďuje na široké spektrum tém, ktoré formujú kvalitu života obyvateľov na Slovensku, v stredoeurópskom regióne a v Európe. ICE v súčasnosti realizuje, okrem iného, aj projekty s podporou Severoatlantickej aliancie, Ministerstva zahraničných vecí a európskych záležitostí SR a Ministerstva obrany SR. Viac na www.iceoz.eu.

Autori

Tomáš Baranec sa vo svojej analytickej práci venuje vývoju v tzv. post-sovietskom priestore, predovšetkým s ohľadom na politicko - historický kontext, možné zdroje napätia a otvorených konfliktov. Vyštudoval Karlovu univerzitu v Prahe, odbor zameraný na Stredoerópske, Balkánske a Stredoázijské štúdiá. Svoje vedomosti si ďalej rozširoval na Univerzite I. Džvachišviliho v Tbilisi. Viac ako rok strávil na Kaukaze ako terénny výskumník venujúci sa prebiehajúcim konfliktom v regióne. Na Slovensku o.i. pracoval ako novinár, výskumný pracovník na ministerstve obrany a tiež ako expert pre niektoré mimovládne organizácie.

Katarína Cséfalvayová je spoluzakladateľkou a riaditeľkou Inštitútu pre Centrálnu Európu. Pôsobila ako predsedníčka Zahraničného výboru a podpredsedníčka Výboru pre európske záležitosti Národnej rady Slovenskej republiky. Ako silná obhajkyňa proatlantickej a proeurópskej zahraničnej politiky na Slovensku sa často kriticky vyjadrovala na adresu populistických a extrémistických politikov a hnutí, spochybňujúcich členstvo Slovenska v EÚ a NATO. Pred svojím zvolením do Národnej rady Slovenskej republiky pôsobila ako prodekanka pre zahraničné vzťahy na Fakulte medzinárodných vzťahov na Ekonomickej univerzite v Bratislave. Je držiteľkou inžinierskeho titulu v odbore ekonomická diplomacia, ako i doktorátu v odbore medzinárodné vzťahy. Francúzsky prezident Emmanuel Macron jej v roku 2020 udelil Národný rád za zásluhy.

Frederick Hardman Lea je študentom krízového a bezpečnostného manažmentu na Justice Institute of British Columbia. Študoval históriu a verejnú bezpečnosť v Kanade so špecializáciou na fyzickú bezpečnosť, núdzový manažment a techniky prevencie kriminality. Vykonával výskum a analýzy súvisiace s politickým násilím v Ázii, Európe a Severnej Amerike so zameraním na terorizmus, etnické konflikty, rasové násilie, nepokoje a revolúcie. Frederickovou špecializáciou je vytváranie kaskádových modelov a vypracovávanie bezpečnostných hodnotení – najmä pokiaľ ide o fyzickú bezpečnosť a environmentálny dizajn.

MINISTERSTVO
OBRANY
SLOVENSKEJ REPUBLIKY

Realizované s finančnou podporou Ministerstva obrany Slovenskej republiky v rámci dotačného programu. Za obsah tohto dokumentu je výlučne zodpovedný Inštitút pre Centrálnu Európu.