

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE



AKADÉMIA
POLICAJNÉHO ZBORU
V BRATISLAVE



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond

Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy

Zborník príspevkov

Bratislava 2023

Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy

Zborník príspevkov z konferencie konanej v dňoch 5. – 6. 10. 2023 v Účelovom zariadení Kancelárie Národnej rady SR Časť – Papiernička

Akadémia Policajného zboru v Bratislave

Zborník vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Vzor citácie:

RUBISOVÁ, I. *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy*. Zborník príspevkov. Bratislava: Akadémia Policajného zboru v Bratislave, 327 s. ISBN

Zostavil: Mgr. Ivana Rubisová, PhD.

Recenzenti: prof. Ing Miroslav Lisoň, PhD.
plk.v.v. doc. JUDr. Robert Odler, PhD.

Za jazykovú úpravu, obsah a pôvodnosť príspevkov zodpovedajú autori.
Rukopis neprešiel jazykovou úpravou.

© Akadémia Policajného zboru v Bratislave

ISBN
EAN

OBSAH

SYSTÉM ROZŠIROVANIA HYBRIDNÝCH HROZIEB VO VEREJNEJ SPRÁVE

Jozef Balga5

AKTIVITY TAJNÝCH SLUŽIEB V SYSTÉME REALIZÁCIE HYBRIDNÝCH HROZIEB A V SYSTÉME IDENTIFIKÁCIE A MINIMALIZÁCIE ICH ŠÍRENIA

Jozef Balga, Monika Hullová22

UKAZOVATEĽ POUŽÍVANÝ NA MERANIE HYBRIDNÝCH HROZIEB V JEDNOTLIVÝCH DOMÉNACH HYBRIDNÝCH HROZIEB, JEHO ZBER A VYHODNOCOVANIE V RÁMCI SLOVENSKEJ REPUBLIKY

Daniel Blaško45

CHARAKTERISTIKA STRATEGICKEJ KORUPCIE VO VEREJNEJ SPRÁVE

Ondrej Blažek58

INFORMAČNÉ TECHNOLOGIE AKO HYBRIDNÉ HROZBY

Nataša Brabcová, Ervín Šimko65

HYBRIDNÉ HROZBY V SÚČASNOSTI

Martina Cíchová77

SEMI-AUTOMATED VULNERABILITY ASSESSMENT IN LORAWAN NETWORKS

Pavel Čičák, Katarína Kochanová, Patrik Sabol, Alexander Valach, Ladislav Zemko87

DEZINFORMÁCIE A PROPAGANDA

Juraj Drugda99

DIGITÁLNY PRENOS INFORMÁCIÍ A SYSTÉM KRYPTOAKTÍV AKO NÁSTROJE HYBRIDNÉHO KONFLIKTU

Daniela Gavurová, Andrej Lipták107

HOAX, JEHO PODSTATA A VNÍMANIE

Miroslav Gombár, Antonín Korauš, Šárka Mayerová, Alena Vagaská118

FUNKCE A VLASTNOSTI KOMPOZITNÍCH INDIKÁTORŮ VNÍMÁNÍ ZÁVAŽNOSTI HYBRIDNÍCH HROZEB

Miroslav Gombár, Antonín Korauš, Šárka Mayerová, Alena Vagaská, Pavlína Račková127

KYBERNETICKÁ BEZPEČNOSTĚ A JEJ PILIERE V ANALÝZE VNÍMANIA ZÁVAŽNOSTI OHROZENIA ŠTÁTU

Miroslav Gombár, Antonín Korauš, Šárka Mayerová, Alena Vagaská135

ONLINE PRIESTOR AKO PROSTRIEDOK NA OVPLYVNĚOVANIA VEREJNEJ MIENKY POČAS VOLEBNEJ KAMPANE V PARLAMENTNÝCH VOEBÁCH SLOVENSKEJ REPUBLIKY V ROKU 2023

Tatiana Hajdúková144

ŠÍŘENÍ DEZINFORMACÍ V KONTEXTU HYBRIDNÍHO PŮSOBNÍ

Lenka Jakubcová, Josef Dubský153

HYBRIDNÉ HROZBY VO FINANČNOM SYSTÉME A MOŽNOSTI NOVÝCH TECHNOLOGIÍ V BOJI PROTI TÝMTO HROZBÁM

Eva Jančíková, Stanislava Veselovská162

PRÁVNE ASPEKTY HYBRIDNÝCH HROZIEB

Sebastián Janko174

KULTÚRA ORGANIZÁCIE VEREJNEJ SPRÁVY A JEJ VÝZNAM PRE PROBLEMATIKU HYBRIDNÝCH HROZIEB	
Martin Kaščák	187
PRIPRAVENOSŤ KAPACÍT SLOVENSKEJ REPUBLIKY NA ZVÝŠENÝ NÁPOR ŽIADOSTÍ O UDELENIE AZYLU, V KONTEXTE HYBRIDNÝCH HROZIEB SÚVISIACICH S MIGRÁCIOU	
Juraj Klátik	193
PODPORA BEZPEČNÉHO TESTOVANIA V DISTRIBUOVANÝCH REAKTÍVNYCH SYSTÉMOCH ZALOŽENÁ NA IDENTIFIKÁCII DIAGRAMOV SEKVENCII	
Viktor Klíma, Ján Lang	198
MERANIE KORUPCIE V KRAJINÁCH EÚ	
Antonín Korauš, Beáta Stehlíková.....	205
POTREBA VNÍMANIA KONCEPTU HYBRIDNÝCH HROZIEB NA NÁRODNEJ ÚROVNI	
Patrícia Krásná.....	214
KRIZOVÉ ŘÍZENÍ PŘI OHROŽENÍ HYBRIDNÍMI HROZBAMI; RIZIKA PRO BEZPEČNOST STÁTU	
Karel Kubečka.....	228
VYUŽITIE TEÓRIE DIGITÁLNEJ STOPY PRI IDENTIFIKÁCII HYBRIDNÝCH HROZIEB	
Adam Kubelka.....	235
ON SEARCHING FOR NATURAL AND LEGAL PERSONS WITH AN UNFAVORABLE REPUTATION	
Richard Marko, Michal Ries, Antonín Korauš, Stanislav Šišulák.....	242
SLOVO AKO “ZBRAŇ” – NEHODNÉ OCHRANY GARANTOVANEJ SLOBODOU PREJAVU	
Vladislav Marko, Ivana Rubisová, Veronika Hegedúšová.....	251
ZVYŠOVANIE ÚROVNE VZDELÁVANIA V OBLASTI HYBRIDNÝCH HROZIEB	
Bohuslava Mihalčová.....	268
MIMORIADNE UDALOSTI A ICH ZNEUŽITIE PRE HYBRIDNÉ PÔSOBENIE NA VEREJNÚ SPRÁVU SR	
Michal Orinčák.....	276
DEZINFORMÁCIE V KRAJINÁCH EÚ	
Beáta Stehlíková, Antonín Korauš	285
ZPŮSOBY SPECIFICKÉHO ZKOUMÁNÍ PRAVICOVÉHO POLITICKÉHO EXTRÉMISMU JAKO MOŽNÉHO NÁSTROJE HYBRIDNÍHO PŮSOBENÍ	
Ivo Svoboda.....	294
KYBERNETICKÝ ROZMER HYBRIDNÝCH HROZIEB VO VZŤAHU K VEREJNEJ SPRÁVE	
Stanislav Šišulák.....	300
PROCESNÁ ANALÝZA V BOJI PROTI HYBRIDNÝM HROZBÁM	
Vladimír Špitalský, Ľubomír Török.	312
ÚLOHA BEZPEČNOSTNÍHO MANAGEMENTU PŘI IDENTIFIKACI A PREVENCI PROJEVŮ EXTRÉMISMU JAKO SPECIFICKÉ HYBRIDNÍ HROZBY	
Barbora Vegrachtová, Eduard Slad	318

SYSTÉM ROZŠIROVANIA HYBRIDNÝCH HROZIEB VO VEREJNEJ SPRÁVE

prof. Dr. Jozef Balga, PhD.

Katedra správneho práva Akadémie PZ v Bratislave, Sklabinská 1, 835 17 Bratislava, e-mail: jozef.balga@akademiapz.sk

Abstrakt: Existencia jednotlivca, spoločnosti a štátu je závislá na efektívnom a racionálnom riadení verejnej správy v súlade s najnovšími vedeckými poznatkami v oblasti manažovania štátnych orgánov a inštitúcií. Autor sa sústreďuje na identifikovanie systému rozširovania hybridných hrozieb s dôrazom na spôsoby prezentácie uvedenej formy hrozby. Šírenie jednotlivých metód hybridných hrozieb ovplyvňuje v plnej miere zamestnancov verejnej správy, ktorí vo svojej rozhodovacej činnosti negatívne alebo pozitívne rozhodnú na základe týchto metód v prospech štátnych alebo neštátnych subjektov tretích krajín realizujúcich systém hybridných hrozieb. Teleologickým zámerom vedeckej práce je načrtnúť teoretické a aplikačné problémy skúmania hybridných hrozieb vplyvujúcich na systém verejnej správy a ich skúmanie prostredníctvom bezpečnostných vied.

Kľúčové slová: verejná správa, metódy a formy verejnej správy, štátna správa, policajná správa, samospráva, hrozba, hybridné hrozby, pramene práva, systém rozširovania hybridných hrozieb, eliminácia hybridných hrozieb.

ÚVOD

Fungovanie spoločnosti a štátu je závislá od efektívnej úrovne riadenia správy za uplatňovania moderných foriem a metód manažovania štátnych orgánov a inštitúcií. Dôraz musí byť kladený na dôsledné plnenie úloh, ktoré stanovujú predovšetkým právne normy pre uvádzané subjekty podieľajúce sa na správe vecí verejných. Z uvádzaných dôvodov sa stáva verejná správa dôležitým prvkom pri zabezpečovaní funkcií štátu.

Pod funkciami štátu treba predovšetkým rozumieť hlavné, respektíve základné smery činnosti štátu. Štát prostredníctvom funkcií štátu, teda hlavných smerov svojej činnosti, rôznymi prostriedkami v rôznych oblastiach života spoločnosti smeruje k realizácii svojho poslania, t. j. k dosiahnutiu určitých cieľov a úloh, ktoré sa od neho očakávajú. Funkcie štátu prezentované ako hlavnú smery jeho činnosti odrážajú historické poslanie štátu ako základného nástroja regulácie spoločenských vzťahov v určitej etape historického vývoja spoločnosti.¹ Medzi základné funkcie štátu patrí funkcia reprodukčná, normatívna, ochranná, obranná, organizačno-správna, sociálno-ekonomická a bezpečnostná.

Organizačno-správna funkcia garantuje taxatívne stanovené činnosti, ktoré sa organizujú vo verejnom záujme, pričom sa sústreďuje na riadenie a správu oblastí, ktoré sú dôležité pre samotné fungovanie štátu a patrí sem napríklad oblasť finančná, zdravotná, hygienická, sociálna, vzdelávania, kultúry, vedeckého výskumu či kontrolná. Vedecký výskum sa v súčasnosti sústreďuje nie len na vedy technické ale aj vedy humánne, ktoré sa zaoberajú systematickou funkciou štátu či efektívnosťou verejnej správy. Patrí sem aj výskum štátovedný a správovedný v rámci, ktorého sa skúma vzťah správnej vedy, verejnej správy a správneho práva. Nesmieme zabudnúť taktiež na realizáciu funkcie bezpečnostnej, ktorá má dôležité miesto v rámci garantovania výkonu

¹ NESVADBA, A. 2022. Teória štátu. s. 20.

kompetencií orgánov a inštitúcií verejnej správy a zároveň vplyva na elimináciu metód hybridných hrozieb smerujúcich na činnosti uvedených subjektov.

1. SYSTÉM VEREJNEJ SPRÁVY

V súčasnej verejnej správe nejde len o vzrastajúcu rôznorodosť správnych činností, ktoré majú charakter verejnej služby, ale aj rozrôžňovanie štruktúry verejnej správy s nevyhnutným zasahovaním do organizačnej štruktúry tzv. verejného a súkromného sektoru. Z uvedeného vyplýva, že v pojme verejnej správy je potrebné akceptovať pluralitný charakter správnych subjektov, ako aj pluralitu vzťahov. Na pluralitu spôsobov uskutočňovania verejnej správy poukazovala právnická literatúra už aj v minulosti. Vychádzajúc z vyššie naznačeného chápania verejnej správy sa možno stotožniť s tým, že v rámci verejnej správy má iný charakter verejná správa uskutočňovaná ako štátna správa a iný verejná správa typu samosprávnej územnej a záujmovej.²

Z hľadiska skúmania verejnej správy v súčasnosti chápeme túto formu správy, ako *trichotomický* systém. Znamená to, že do systému verejnej správy patrí štátna správa (*systém správnych štátnych orgánov a inštitúcií - byrokratický prvok*), samospráva (*územná a záujmová*) a verejnoprávne korporácie.³

Nepochybne súčasťou a zároveň nástrojom, podieľajúcim sa na racionalizácii verejnej správy je identifikácia jej moderného systému, ktorý sa začal formovať v druhej polovici minulého storočia. Samotný vývoj systému nebol priamočiari a v súčasnosti môžeme o ňom hovoriť ako o zložitom systéme, ktorý obsahuje niekoľko zložitých prvkov. Systém verejnej správy nie je jednoliaty a v závislosti od svojho predmetu a objektu skúmania sa rozdeľuje z rôznych hľadísk a stránok.

V súčasnosti *systém verejnej správy* identifikujeme predovšetkým ako súbor prvkov, ktoré sa podieľajú na správe verejných záležitostí (vecí) a prejavujú sa pri realizácii funkcií štátu pričom obsahom sú taxatívne stanovené spoločenské vzťahy pri výkone štátnej moci, ktoré sú predmetom právnej úpravy. To znamená, že verejná správa je systémom, ktorý obsahuje *horizontálnu* a *vertikálnu* jednotu. Skúmaním systému verejnej správy sa zaoberá správna veda a jej neoddeliteľná súčasť teória verejnej správy.

Teória verejnej správy vystupuje vo forme logicky vybudovaného a skĺbeného celku t. j. *teoretického systému*, ktorý vysvetľuje skúmané procesy v oblasti správy. Samotná teória verejnej správy sa sústreďuje na skúmanie objektu, predmetu, subjektov a princípov teórie. Osobitne skúma metodológiu systému činností subjektov verejnej správy. Vo všeobecnosti objektom teórie verejnej správy je *konkrétna sociálna realita* ako produkt vedome vykonávajúcich činností vo verejnej správe. Zároveň predmetom sú jednotlivé procesy pri realizácii jednotlivých prvkov systému. Medzi základné subjekty ovplyvňujúce a tvoriace uvádzanú sociálnu realitu patria jednak občania a štátni príslušníci tretích krajín a ich aktivity, ako aj inštitúcie.

V súčasnosti vedeckým skúmaním systému boli identifikované teoretické východiská v súlade s charakterom uvádzanej sociálnej reality. Východisko personálne predstavuje *personálny substrát* zabezpečujúci realizáciu a aplikáciu verejnej správy, ako aj organizovanie vzdelávacích

² TÓTHOVÁ, K. a kol. 1993. Základy správneho práva hmotného. s. 7.

³ Pozri bližšie ŠKULTÉTY, P. 2008. Verejná správa a správne právo. s. 20-35.

a výskumných aktivít zo strany zamestnancov príslušných inštitúcií. Aplikácia systému vyžaduje, aby zamestnanci verejnoprávnych inštitúcií vykonávali určené funkcie a spĺňali kritériá v oblasti vzdelania, odbornej praxe, jazykových znalostí, mali vedomosti a zručnosti nadobudnuté praktickým výkonom. K výkonu niektorých funkcií sú stanovené špecifické oprávnenia ako prístup k utajovaným skutočnostiam. *Základným teoretickým východiskom je definícia kvalifikačných predpokladov pre zamestnancov verejnej správy, ktoré sú kompetentné realizovať a aplikovať systém.*

1.1 Subjekty verejnej správy

Medzi základné prvky systému teórie verejnej správy patria subjekty. Teória verejnej správy pristupuje k problematike subjektov komplexne a všíma si otázky, ktoré nie sú výslovne upravené v právnych normách a riadi sa nad rámec právnej regulácie i mimoprávnymi normami. *Subjektmi teórie verejnej správy* sú fyzické a právnické osoby, ktoré sú schopné stať sa nositeľom práv a povinností vyplývajúcich z právnych noriem, ktoré sú objektívne skúmané teóriou. To znamená, že majú právnú subjektivitu a taxatívne stanovené kompetencie (teritoriálnu, personálnu, vecnú, funkčnú a temporálnu). *Fyzické osoby* sú subjektom teórie v prípadoch, kedy majú svoju právnú subjektivitu, t. j. sú spôsobilí k subjektívnym právam a povinnostiam. Samotná právna subjektivita fyzických osôb v jednotlivých právnych odvetviach alebo v rámci právnych inštitútov je odstupňovaná väčšinou podľa veku a podľa schopnosti ovládať svoje konanie a posúdiť jeho dôsledky. Z fyzických osôb je subjektom teórie predovšetkým pracovník pôsobiaci vo verejnej správe a taktiež vedecko-pedagogickí pracovníci vedeckých a vysokoškolských ustanovizní. Ďalšími osobami sú občania a cudzí štátni príslušníci, ktorí svojimi konaniami aplikujú svoje práva, právom chránené záujmy a povinnosti vo vzťahu k orgánom verejnej správy.

Právnické osoby podľa platného práva majú právnú subjektivitu. V ich mene sú oprávnené konať stanoveným spôsobom ich štatutárne orgány. Za dôležité subjekty považujeme verejnoprávne korporácie, ktoré sú mocensky vybavené kompetenciami pre plnenie svojich úloh vyplývajúcich im z právnych noriem a postavenia v systéme verejnej správy. Štát je spolu s jeho štátnymi orgánmi a inštitúciami realizujúcimi štátnu (verejnú) moc, verejnoprávnu korporáciu.

Samospráva je organickou súčasťou verejnej správy, ktorej kompetencie sú teritoriálne stanovené v súlade s územnosprávnym členením Slovenskej republiky. Samostatná pôsobnosť samosprávy vyplýva z právnych noriem, ktoré aplikujú štatutárne orgány samosprávy alebo pracovníci samosprávnych úradov. Zahrňujú v sebe činnosti, ktoré sú vykonávané vlastnými silami a prostriedkami a sústreďujú sa predovšetkým do oblasti správy obcí a vyšších územných celkov.

Do samosprávy radíme *miestnu samosprávu*, ktorú vymedzujeme ako organizačnú formu verejnej správy, v ktorej spoločenstvo ako právnická osoba zabezpečuje riešenie úloh odlišných, ako zabezpečuje štát, ale realizácia týchto úloh sa rieši pod dozorom štátu. Zákonom stanovené úlohy rieši vo svojom mene a na svoju zodpovednosť a je viazaná len zákonmi, prípadne právnymi predpismi, ktoré sú vydané na ich realizáciu.⁴ Osobitná forma samosprávy je *samospráva záujmová*, ktorá sa zaoberá záležitosťami rôznych samosprávnych komôr, záujmových spoločenstiev a ďalších subjektov stavovského charakteru. Z hľadiska teórie uvádzané subjekty sa stávajú objektom skúmania v prípadoch kedy vykonávajú činnosti považujúce za *verejné*. Uvedené

⁴ ŠKULTÉTY, P. Verejná správa a správne právo. s. 33

delenie subjektov vyplýva zo základného zloženia verejnej správy a to na správu štátnu a samosprávu.

Ďalšie delenie subjektov je podľa špeciálnych činností a patria sem subjekty realizujúce, aplikujúce a skúmajúce. *Realizujúce subjekty* svoju činnosť zameriavajú na základe výsledkov výskumu a teoretických východísk do oblasti prijímania právnych noriem smerujúce k racionalizácii efektívnosti verejnej správy. *Aplikujúce subjekty* formou činností predovšetkým pracovníkov verejnej správy sa stávajú predmetom teórie a umožňujú skúmanie organizácie práce štátnych a samosprávnych orgánov. *Skúmajúce* (vedecko-výskumné) *subjekty* sú vedecké ústavy a vysoké školy, ktoré sa podieľajú na rozvoji správnej vedy a teórie verejnej správy.

Osobitne do systému subjektov teórie verejnej správy zaradíme *personálny substrát verejnej správy* t.j. fyzické osoby – pracovníci verejnej správy ktorých právne postavenie upravujú *lex specialis*. Výber pracovníkov z hľadiska spoločenských očakávaní, odborných znalostí, organizačných schopností, morálnych predpokladov, bezúhonnosti, osobnostných vlastností má primárny význam pri eliminácii šírenia hybridných hrozieb vo verejnej správe.

V súvislosti so systémom verejnej správy je dôležité upozorniť na činnosť verejnej správy. Každá organizovaná činnosť je činnosť dynamická vyznačujúca sa však súčasne poriadkom, ktorý túto činnosť činí usporiadanou v rámci určitých pravidiel. Platí to v plnej miere aj o verejnej správe, ktorej dynamika sa prejavuje predovšetkým v premenách a počte úloh, ktoré túto správu obsahovo vymedzuje, súčasne však existenciou záväzných procesných pravidiel a organizačnou štruktúrou vykonávateľov verejnej správy ako prvkami stabilizujúcimi.⁵

2. SYSTÉM PRAMEŇOV PRÁVA EURÓPSKEJ ÚNIE UPRAVUJÚCE BOJ PROTI HYBRIDNÝM HROZBÁM

Systém prameňov práva Európskej únie sa skladá z veľkého množstva materiálnych a formálnych prameňov a z uvedeného dôvodu uvedieme len kardinálne pramene, ktoré *expressis verbis* uvádzajú základné právne východiská pre boj proti hybridným hrozbám s osobitným dôrazom na subjekty verejnej správy.

V systéme prameňov práva Európskej únie (ďalej len EÚ) sa explicitne začali uvádzať hybridné hrozby až od roku 2016. Boj proti hybridným hrozbám, z hľadiska materiálnych prameňov práva EÚ, sa začal realizovať od uvedeného roku prijatím. Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ. V uvedenom dokumente bola vypracovaná aj charakteristika hybridných hrozieb. V zmysle spomenutého materiálneho prameňa práva EÚ, hybridné hrozby chápeme ako súbor rôznych nátlakových a podvrtných činností, konvenčných a nekonvenčných metód (*napríklad diplomatických, vojenských, ekonomických a technologických*), ktoré môžu rôzne štátne a neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu.⁶

⁵ HENDRYCH, D. a kol. Správni právo. Obecná časť. s. 119

⁶ Spoločné oznámenie Európskemu parlamentu a Rade – Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie – JOIN(2016) 18 final – 6. apríl 2016.

V tomto smere možno predmetný spoločný rámec vnímať ako základný koncepčný dokument, ktorý prvýkrát charakterizoval hybridné hrozby v materiálnych prameňoch práva EÚ a sústredil sa na ďalšie podstatné náležitosti riešenia tohto problému (*1. identifikáciu hybridných hrozieb; 2. zlepšovanie informovanosti a nastavenie vhodného inštitucionálneho rámca a mechanizmu pre strategickú komunikáciu; 3. budovanie odolnosti v jednotlivých oblastiach a boj proti financovaniu hybridných hrozieb; 4. prevenciu, reakciu na krízu spôsobenú hybridnými hrozbami a obnovu; 5. posilnenie spolupráce s NATO*). Z hľadiska primárnych prameňov práva EÚ, spoločný rámec uvádza článok 222 Zmluvy o fungovaní EÚ, ako možnosť pomoci členskému štátu v prípade, ak sa členský štát stane obeťou značných hybridných hrozieb. Zároveň zdôrazňuje skutočnosť, že pri eliminácii rozsiahlych a závažných prejavov hybridných hrozieb sa môže realizovať aj intenzívnejšia spolupráca a koordinácia s NATO. V tejto súvislosti nemožno opomenúť fakt, na ktorý spoločný rámec poukázal, a to že hybridné hrozby sú aj vzhľadom na ich charakter výsostnou národnou kompetenciou členských štátov (*primárne ohrozujú národné bezpečnostné a obranné záujmy*). Napriek tejto skutočnosti, EÚ ponúkla členským štátom komplexný návrh stratégie boja proti hybridným hrozbám, rozčlenený do už uvedených piatich základných oblastí.

V rámci boja proti hybridným hrozbám bola v nadväznosti na tieto kroky prijatá Spoločná správa Európskemu parlamentu a Rade o vykonávaní Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ.⁷ Spoločná správa reaguje na zvýšenú intenzitu činností v rámci hybridných hrozieb v takých oblastiach, ako je ovplyvňovanie volieb, dezinformačné kampane, negatívne aktivity v kybernetickom priestore a radikalizácia zraniteľných členov spoločnosti. Obsahom spoločnej správy je aj systém opatrení a určenie subjektov, ktoré tieto opatrenia majú realizovať. V závere správa opätovne upozorňuje členské štáty na primárnu zodpovednosť za boj proti hybridným hrozbám súvisiacich s národnou bezpečnosťou.⁸

V roku 2018 bolo následne vypracované a prijaté Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby.⁹ V rámci reakcie EÚ na silnejúce hybridné hrozby sa podnikli dôležité kroky na vybudovanie štruktúr potrebných na zlepšenie situačného povedomia a podporu rozhodovania. Spoločné oznámenie, taktiež, upozornilo na dôležitosť strategickej komunikácie šírením zrozumiteľných informácií prostredníctvom vzdelávania verejnosti, aby bežný občan dokázal rozlíšiť informácie od dezinformácií.

V nadväznosti na uvedené materiálne pramene práva EÚ zaoberajúce sa hybridnými hrozbami, bola v roku 2020 komisiou vypracovaná Stratégia EÚ pre bezpečnostnú úniu.¹⁰ Uvedená stratégia zdôraznila právnu skutočnosť, že členské štáty sú zodpovedné za bezpečnosť na strane druhej upozornila na zintenzívnenie snahy o zapojenie celej spoločnosti vrátane orgánov verejnej správy do realizácie bezpečnostnej politiky EÚ. Tento dokument zaradil hybridné hrozby do systému bezpečnostných hrozieb ohrozujúcich EÚ. Stratégia zdôraznila potenciál hybridných útokov zo

⁷ Annual progress reports on countering hybrid threats – JOIN(2017) 30 final.

⁸ Annual progress reports on countering hybrid threats – JOIN(2017) 30 final, 19. 7. 2017; JOIN(2018) 14 final, 13. 6. 2018; SWD(2019) 200 final, 29. 5. 2019; SWD(2020) 153 final, 24.7.2020; SWD (2021) 729, 22. 7. 2021; SWD(2022) 308, 16. 9. 2022.

⁹ Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby – JOIN(2018) 16 final.

¹⁰ Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – O stratégii EÚ pre bezpečnostnú úniu – COM(2020) 605 final.

strany štátnych a neštátnych subjektov, ktoré využívajú zraniteľnosť pomocou kombinácie kybernetických útokov, poškodzovania kritickej infraštruktúry, dezinformačných kampaní a radikalizácie politického jazyka. Vzhľadom na neustály vývoj v oblasti hybridných hrozieb sa má, okrem iného, intenzívnejšie klásť osobitný dôraz na začlenenie hybridných hrozieb do tvorby politik, aby sa naďalej udržal krok s dynamickým vývojom, a aby sa zabezpečilo, že sa neprehliadne žiadna potencionálna relevantná iniciatíva. Nové iniciatívy sa budú posudzovať optikou hybridných hrozieb aj v oblastiach, ktoré boli doposiaľ mimo rámca boja proti hybridným hrozbám, ako sú vzdelávanie, výskum a technológie. Pri tomto prístupe sa využije úsilie vyvinuté v oblasti konceptualizácie hybridných hrozieb zabezpečujúc komplexný pohľad na rôzne nástroje, ktoré môžu nepriatelia využívať.¹¹ Z hľadiska predchádzania hybridným hrozbám a ochrany pred nimi, bude aj naďalej kľúčové budovanie odolnosti. Znamená to, určenie odvetvových základných scenárov odolnosti proti hybridným hrozbám pre členské štáty a inštitúcie EÚ.

Ďalším dôležitým dokumentom je Strategický kompas EÚ pre bezpečnosť a obranu,¹² ktorý obsahuje konkrétne opatrenia nevyhnutné na efektívny boj proti hybridným hrozbám. Členské štáty sa v tejto stratégii zaviazali realizovať aktivity v štyroch základných oblastiach, a to aktivita, bezpečnosť, investície a partneri, pričom problematika boja proti hybridným hrozbám primárne spadá do oblasti bezpečnosti. Práve v poslednej spomenutej sfére si EÚ predsavzala, že zvýši svoje kapacity na analýzu spravodajských informácií, vytvorením súborov nástrojov a tímov rýchlej reakcie na hybridné hrozby. Okrem toho, si EÚ kládla za cieľ – vytvoriť súbor nástrojov kybernetickej diplomacie a v tomto ohľade aj politický rámec EÚ pre kybernetickú obranu a zároveň – vypracovať Stratégiu EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu a posilniť úlohu EÚ ako aktéra námornej bezpečnosti. Rok po schválení Strategického kompasu EÚ, zhodnotili ministri zahraničných vecí a ministri obrany členských štátov EÚ na spoločnom zasadnutí v marci 2023 pokrok, ktorý sa dosiahol pri jeho vykonávaní.¹³

Z hľadiska finančného zabezpečenia boja proti hybridným hrozbám bolo prijaté Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1149, ktorým sa zriaďuje Fond pre vnútornú bezpečnosť. Právna norma zdôrazňuje potrebu zaistenia vysokej úrovne bezpečnosti v priestore slobody, bezpečnosti a spravodlivosti. Na dosiahnutie cieľov súvisiacich s garantovaním bezpečnosti má EÚ okrem iného akcie podporujúce činnosti smerujúce k boju proti hybridným hrozbám ako výzvy pre vnútornú bezpečnosť EÚ. Fond má podporovať akcie zamerané na riešenie hlavných bezpečnostných hrozieb medzi ktoré sú zaradené aj hybridné hrozby. Fond má taktiež prispieť k plneniu zlepšenia a uľahčenia výmeny informácií medzi príslušnými orgánmi, úradmi a agentúrami EÚ. Ďalej je to podpora posilňovania spôsobilosti členských štátov v súvislosti s riadením udalostí, rizík a kríz súvisiacich s bezpečnosťou prostredníctvom intenzívnejšej spolupráce medzi orgánmi verejnej moci, občianskou spoločnosťou a súkromnými partnermi v rôznych členských štátoch. V prílohe III. explicitne v rámci cieľov fondu a z fondu sa môžu

¹¹ The Landscape of Hybrid Threats: A conceptual Model (prostredie hybridných hrozieb: koncepčný model), JRC117280, vypracované na základe spolupráce medzi Spoločným výskumným centrom a Európskym centrom excelentnosti pre boj proti hybridným hrozbám.

¹² Rada EÚ. 2022. Strategický kompas pre silnejšiu bezpečnosť a obranu EÚ v nasledujúcom desaťročí: Tlačová správa z 21. 3. 2022. [online]. [cit. 2023-9-3]. Dostupné na internete: <https://www.consilium.europa.eu/sk/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>.

¹³ EEAS, 2023. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.

podporiť okrem iného aj akcie, ktorými sa zlepšuje odolnosť, pokiaľ ide o vznikajúce hybridné hrozby. Finančné krytie na vykonanie fondu na obdobie od 1. januára 2021 do 31. decembra 2027 sa stanovil na 1 931 000 000 EUR v bežných cenách.¹⁴

Z formálnych prameňov práva na úseku boja proti hybridným hrozbám v súčasnosti je najdôležitejším Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/144/ES.¹⁵ Smernica zdôrazňuje, že opatrenia členských štátov zamerané na identifikáciu kritických subjektov a pomoc pri zabezpečovaní ich odolnosti by sa mali riadiť prístupom založeným na riziku, ktorý sa zameriava na subjekty, ktoré sú najdôležitejšie z hľadiska dôležitých spoločenských funkcií alebo hospodárskych činností. Takýto cielený prístup členských štátov v harmonizovanom rámci má smerovať k posúdeniu relevantných prírodných a ľudskou činnosťou spôsobených rizík vrátane rizík medziodvetvovej a cezhraničnej povahy, ktoré by mohli ovplyvniť poskytovanie základných služieb, vrátane nehôd, prírodných katastrof, hybridných hrozieb alebo iných antagonistických hrozieb. Uvedená právna norma by sa mala vzťahovať aj na subjekty vykonávajúce činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane vyšetrovania, odhaľovania a stíhania trestných činov alebo poskytujú služby výlučne subjektom verejnej správy, ktoré vykonávajú činnosti prevažne v uvedených oblastiach. Vzhľadom na zodpovednosť členských štátov za ochranu národnej bezpečnosti a obrany, by členské štáty mali mať možnosť rozhodnúť, že povinnosti kritických subjektov, taxatívne vymedzených v smernici, sa na tieto subjekty úplne alebo čiastočne neuplatňujú. Do rozsahu pôsobnosti tejto smernice by však mali patriť subjekty, ktorých služby alebo činnosti súvisia s uvedenými oblastami len okrajovo. Osobitne sa uvádza subjekt verejnej správy, ktorý je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani obchodný charakter. Tento subjekt má právnu subjektivitu, je z väčšej časti financovaný štátnymi orgánmi alebo inými ústrednými orgánmi, ktoré sa riadia verejným právom, jeho riadenie podlieha dohľadu týchto orgánov. Zároveň má právomoc vydávať správne alebo regulačné rozhodnutia určené fyzickým alebo právnickým osobám, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovaru, služieb alebo kapitálu. V zmysle prílohy smernice sem patria subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom. Transpozičná lehota smernice je určená do 17. októbra 2024. Uvedená smernica sa bude týkať aj činnosti špeciálnych orgánov štátnej správy pri realizácii previerok zamestnancov kritických subjektov v riadne odôvodnených prípadoch a pri zohľadnení posúdenia rizika členským štátom. Musíme ďalej upozorniť na skutočnosť, že incident, ktorý môže významne narušiť poskytovanie základnej služby charakterizovanej smernicou, môže byť udalosť spôsobená prostredníctvom hybridných útokov. Z uvedených dôvodov, táto smernica je jedným z právnych nástrojov EÚ aj v boji proti hybridným hrozbám.

Systém boja proti hybridným hrozbám z pohľadu EÚ prioritne tvoria nasledujúce prvky – pramene práva *EÚ (materiálne a formálne, primárne a sekundárne)*, subjekty *(právnické osoby, fyzické osoby, štátne a neštátne subjekty)*, metódy *(analýza, komparácia atď.)*, prostriedky *(technické, informačné, evidenčné a iné)*, prvky spolupráce, vzdelávacie prvky, strategická komunikácia, teritoriálne, časové a teleologické prvky. Osobitný subsystém subjektov v rámci hybridných

¹⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1149 zo 7. júla 2021, ktorým sa zriaďuje Fond pre vnútornú bezpečnosť – L 251, 15.7.2021, s.94-131.

¹⁵ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/144/ES – L 333, 27.12.2022, s.164.

hrozieb tvoria subjekty realizujúce hybridné útoky proti štátom s demokratickým politickým systémom a subjekty, ktoré identifikujú a eliminujú tieto útoky v rámci boja proti hybridným hrozbám, napríklad spravodajské služby, polícia, ozbrojené sily a podobne.

3. SYSTÉM BOJA PROTI HYBRIDNÝM HROZBÁM V SLOVENSKEJ REPUBLIKE

Pre pochopenie stavu boja proti hybridným hrozbám je nutné uviesť niekoľko koncepčných a strategických dokumentov politického a odborného významu, ktoré boli prijaté za posledné roky. Patrí sem Koncepcia pre boj SR proti hybridným hrozbám, Bezpečnostná stratégia SR, Obranná stratégia SR, Akčný plán koordinácie boja proti hybridným hrozbám,¹⁶ Koncepcia bezpečnostného systému SR a Koncepcia strategickej komunikácie. Všetky uvedené dokumenty reagujú na úniové záväzky SR v tejto oblasti a obsahujú taxatívne stanovené opatrenia na posilnenie postavenia subjektov podieľajúcich sa na posilnení kapacít štátu pre boj proti hybridným hrozbám. Na strane druhej je nutné podotknúť skutočnosť, že pre systém verejnej správy nie sú adekvátne uvedené úlohy v boji proti hybridným hrozbám a dokumenty sa sústreďujú len na štátnu správu opomínajúc samosprávu a verejnoprávne korporácie.

Skôr než sa sústredíme na pertraktovanú problematiku, uvedieme a charakterizujeme postavenie niektorých subjektov v SR, ktoré sa zaoberajú identifikáciou a elimináciou hybridných hrozieb.

Primárnym subjektom je Bezpečnostná rada SR (*d'alej len BR SR*),¹⁷ ktorá má okrem iného zriadený výbor pre zahraničnú politiku, výbor pre kybernetickú bezpečnosť, výbor pre koordináciu spravodajských služieb a od mája 2023 aj výbor pre hybridné hrozby. Z hľadiska skúmaného vedeckého problému sa budeme zaoberať len výborom pre hybridné hrozby.

Výbor pre hybridné hrozby, pri koordinácii plánovania opatrení zameraných na zachovanie bezpečnosti a budovania odolnosti SR voči pôsobeniu hybridných hrozieb, vyhodnocuje bezpečnostnú situáciu v SR a vo svete v oblasti hybridných hrozieb s dôrazom na hodnotenie hybridného pôsobenia na odolnosť štátu a odolnosť spoločnosti. Pripravuje pre BR SR návrhy opatrení na zvýšenie odolnosti štátu a spoločnosti voči rizikám hybridného pôsobenia. Podieľa sa na formovaní politiky SR, ako aj na vypracúvaní koncepčných dokumentov v oblasti hybridných hrozieb a na koordinácii medzirezortnej a medzinárodnej spolupráce v oblasti hybridných hrozieb. Predkladá BR SR návrhy opatrení na zvyšovanie celospoločenského povedomia o hybridných hrozbách a prerokúva návrhy predkladané BR SR, ktoré súvisia s plnením úloh v oblasti hybridných hrozieb. Vypracúva odborné stanoviská vzťahujúce sa na hybridné hrozby a predkladá ich BR SR. Posudzuje právne predpisy a medzinárodné zmluvy vzťahujúce sa na hybridné hrozby, ktoré sú predložené na prerokovanie BR SR.

Ďalším subjektom, ktorý v bezpečnostnom prostredí SR operuje v pozícii národného kontaktného miesta pre hybridné hrozby, je Situačné centrum SR.¹⁸ Situačné centrum SR alias SITCEN je súčasťou Kancelárie BR SR (*d'alej len KBR*) a formálne existuje od januára 2016. Úlohou

¹⁶ NBÚ. 2022. Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf>.

¹⁷ Čl. 8 Ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

¹⁸ Uznesenie vlády Slovenskej republiky č. 486/2018 zo dňa 17. októbra 2018.

SITCEN-u, ako vládneho informačného analytického pracoviska s celoštátnou pôsobnosťou, je zabezpečovať nepretržitý tok informácií a koordináciu tohto toku medzi Strediskom EÚ pre hybridné hrozby (*formálne označované ako „EU Hybrid Fusion Cell“, resp. „EU HFC“*), a SR, a to oboma smermi. Okrem toho sa podieľa na monitorovaní, analýze a prognóze vývoja bezpečnostnej situácie a v prípade potreby, napr. krízovej situácie, má za úlohu kontaktovať relevantné orgány SR alebo v zahraničí. V tejto súvislosti treba podotknúť, že BR SR, často práve na základe informácií od SITCEN-u predkladá vláde návrhy opatrení na zníženie alebo odstránenie rizík ohrozenia bezpečnosti SR, ktoré môžu viesť ku krízovej situácii. Je zrejmé, že podstatou činnosti tohto vládneho pracoviska je príprava výstupných analytických materiálov a ich predkladanie kompetentným adresátom decíznej sféry pre ďalšie využitie, napríklad pre voľbu strategických rozhodnutí v rámci smerovania bezpečnostnej politiky SR, príp. v neskorších etapách aj na operačno-taktickej úrovni.

Dôležitú funkciu na tomto úseku plní aj Národné bezpečnostné analytické centrum (*d'alej len NBAC*), zastávajúce úlohu národného kooperačného centra pre hybridné hrozby, ktorého poslaním je sústreďovať informácie o hybridných hrozbách na základe prijatých hlásení od orgánov štátnej správy, prípadne od iných subjektov (*fyzických a právnických osôb*) a následne ich vyhodnocovať a distribuovať určeným adresátom pre ďalšie využitie (*najčastejšie práve SITCEN-u*).¹⁹ NBAC je definované ako analytické, komunikačné a kooperačné pracovisko Slovenskej informačnej služby (*d'alej len SIS*), s celoštátnou pôsobnosťou v oblasti bezpečnostných hrozieb. Napriek tomu, že centrum vzniklo v januári 2013 na základe projektu, ktorého iniciátorom a zároveň aj gestorom bola SIS, NBAC vo svojej podstate reprezentuje novú formu medzirezortnej organizačnej štruktúry. Na jeho platforme spolupracujú vyslaní zástupcovia SIS, Vojenského spravodajstva (*d'alej len VS*), Policajného zboru, Kriminálneho úradu finančnej správy, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, Generálneho štábu Ozbrojených síl SR a Úradu vlády SR. Medzi jeho hlavné úlohy patrí príprava komplexných analytických hodnotení bezpečnostných incidentov na základe hlásení prijatých od štátnych orgánov SR, monitorovanie bezpečnostnej situácie v SR z odkrytých zdrojov a poskytovanie analytických produktov o bezpečnostných hrozbách v SR určeným príjemcom. NBAC funguje ako analytické pracovisko založené na aktívnej participácii rozhodujúcich štátnych orgánov SR, ktoré pôsobia v bezpečnostnej oblasti. Ďalšie participujúce štátne subjekty poskytujú NBAC informačnú podporu formou hlásení o zaznamenaných bezpečnostných incidentoch. Informačné produkty spracované analytickým pracoviskom NBAC sú poskytované všetkým zúčastneným štátnym orgánom a inštitúciám a prípadne aj ďalším subjektom v zriaďovateľskej pôsobnosti štátnych orgánov za účelom rozhodovania a prijímania bezpečnostných opatrení.

Osobitnú pozornosť si v tomto ohľade zasluhuje vojenské spravodajstvo, ktoré patrí medzi spravodajské služby legitímne operujúce v bezpečnostnom a obrannom prostredí SR. Vojenské spravodajstvo na účely planenia úloh stanovených v zákone o Vojenskom spravodajstve získava, sústreďuje a vyhodnocuje informácie dôležité na zabezpečenie obrany, obranyschopnosti a bezpečnosti SR na území SR a mimo územia SR zamerané aj na hybridné hrozby a dezinformácie, ak ohrozujú obranu alebo obranyschopnosť SR.²⁰ Na uvedenom úseku plní úlohu spravidla utajeným spôsobom a vykonávajú také činnosti ako je sledovanie osôb a vecí, používanie

¹⁹ Slovenská informačná služba. 2020. O nás: Národné bezpečnostné analytické centrum (NBAC). [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/o-nas/nbac.html>.

²⁰ § 5 zákona č. 500/2022 Z. z. o Vojenskom spravodajstve

krycích dokladov a využívanie osôb konajúcich v prospech Vojenského spravodajstva. Taktiež na plnenie uvedenej úlohy je Vojenské spravodajstvo oprávnené používať informačno-technické prostriedky za podmienok stanovených zákonom o ochrane pred odpočúvaním.²¹

4. SYSTÉM ROZŠIROVANIA HYBRIDNÝCH HROZIEB V RÁMCI SUBJEKTOV VEREJNEJ SPRÁVY

V súvislosti so skúmaním systému rozširovania hybridných hrozieb je nutné stanoviť charakteristiku pojmu hrozba a hybridné hrozby v zmysle materiálnych prameňov práva zaoberajúcich sa bezpečnosťou SR. Samotný pojem *hrozba* charakterizujeme ako jasný, zrozumiteľný a identifikovateľný systém možných okolností, udalostí, skutočností, procesov a javov, ktoré majú negatívny vplyv na realizáciu práv a povinností subjektov súvisiacich s poskytovaním služieb stanovených v právnych normách. Hrozba vplýva na správanie osôb a skupín obyvateľstva, správanie profesijných skupín (napríklad zamestnanci verejnej správy), procesy prebiehajúce vo vnútri spoločnosti, správanie záujmových skupín a lobistov. *Hrozba pre verejnú správu* je primerane rozpoznateľná okolnosť, udalosť, skutočnosť, proces, jav či stav smerujúci proti systému verejnej správy, ktoré majú nepriaznivý vplyv na plnenie funkcií, úloh a kompetencií vo verejnom záujme a poskytovaní služieb administratívno-právneho charakteru

Pri charakteristike hybridných hrozieb vychádzame zo základných indikátorov týchto hrozieb. Patrí sem okrem iného externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie, ekonomický alebo energetický nátlak, rozsiahle sabotáže proti kľúčovej infraštruktúre ale aj informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie a tým vyvolať spoločenské nepokoje. Ďalej sú to kybernetické útoky, ovplyvňovanie etnických, náboženských a kultúrnych menšín, ich politická manipulácia a hrozba použitia vojenskej sily. Následne hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku.²² Akčný plán koordinácie boja proti hybridným hrozbám (2022 – 2024) za hybridné hrozby označuje aktivity štátnych alebo neštátnych aktérov, ktoré majú otvoreným alebo skrytým pôsobením vojenských alebo nevojenských metód, oslabiť alebo inak poškodiť vybraný cieľ.²³ V súčasnosti bude nutné prehodnotiť uvedené charakteristiky a vypracovať definíciu za účasti odbornej a vedeckej komunity, ktorá by spĺňala požiadavky teórie definícií. V definícii hybridných hrozieb musí byť stanovený objekt, subjekty, ciele a prostriedky realizované v rámci hybridných hrozieb.

V súvislosti s hybridnými hrozbami sa nekoná nič nového a prevratného. Nový je len veľký rozsah, škála koordinovaných prostriedkov pre dosiahnutie cieľa. Realizovaná hybridná hrozba (bezpečnostná udalosť) sa nazýva v odbornej bezpečnostnej komunite hybridná kampaň. Jej cieľom je vyvolať určitý nátlak, podvratnú činnosť, pričom sa používajú štátne a neštátne inštitúcie

²¹ zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním)

²² Národný bezpečnostný úrad. Konceptia boja SR proti hybridným hrozbám. . [online]. [cit. 2023-10-11]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Konceptia-boja-SR-proti-hybridnym-hrozbam.pdf>

²³ Ministerstvo obrany SR. Akčný plán koordinácie boja proti hybridným hrozbám (2022 – 2024). [online]. [cit. 2023-10-11]. Dostupné na internete <https://www.mosr.sk/51291-sk/akcny-plan-koordinacie-boja-proti-hybridnym-hrozbam-posilni-odolnost-statu-a-spolocnosti-voci-hybridnemu-posobeniu/>

z vojenskej, polovojenskej a civilnej sféry, takým spôsobom, aby ich protivník nemohol napadnúť či ovplyvniť vo svoj prospech. Hybridné hrozby sú veľmi sofistikované, používajú aj rôzne krytia, tzv. legendy, takže pre napadnutého nie je jednoduché, aby skrytú hybridnú kampaň vôbec objavil, na to aby ju efektívne ovplyvnil. Hybridné hrozby využívajú klasické nástroje, často ich kombináciu a integráciu, ktoré zahŕňajú diplomáciu, informácie, ozbrojené sily ekonomiku, finančníctvo, spravodajstvo, verejný poriadok a právny štát.²⁴

Skúmanie hybridných hrozieb má svoju časť teoretickú a aplikačnú. *Teoretická časť* objasňuje procesy prebiehajúce v rámci činností subjektov realizujúcich hybridné hrozby k dosiahnutiu cieľov predovšetkým v oblasti realizácie princípov právneho štátu a jeho fungovania a samozrejme ohrozenia bezpečnosti jednotlivca, skupín obyvateľstva, spoločnosti a štátu. Kým *aplikačná časť* má za úlohu vypracovať predovšetkým metodiku činností, ktorých cieľom je eliminácia hybridných hrozieb smerujúcich k ohrozeniu alebo narušeniu bezpečnosti jednotlivca, spoločnosti a štátu. V súvislosti so skúmaním vplyvu hybridných hrozieb na činnosť verejnej správy a šírenie týchto hrozieb je potrebné uviesť charakteristiku systému šírenia hybridných hrozieb vo verejnej správe a pojem eliminácia šírenia hybridných hrozieb vo verejnej správe.

Systémom rozširovania hybridných hrozieb vo verejnej správe rozumieme špecifické činnosti realizované subjektami štátneho a neštátneho charakteru cudzieho štátu s cieľom pôsobiť destabilizačne na subjekty verejnej správy realizujúce funkcie právneho štátu predovšetkým organizačno-správnú a reprodukčnú a tým negatívne pôsobiť na bezpečnosť jednotlivca, spoločnosti a štátu. Zároveň môže smerovať k zmene politického režimu, štátneho a policajného mechanizmu. Pri rozširovaní hybridných hrozieb subjekty štátneho alebo neštátneho charakteru využívajú vysokú mieru plánovania, organizovania a riadenia činností, akčnosť a bezohľadnosť. Z hľadiska personálnej štruktúry realizátorov hybridných hrozieb ich môžeme deliť na riadiacich, navrhovateľov, posudzovateľov, šíriteľov, príslušníkov spravodajských služieb, pracovníkov organizácií (vládných, mimovládnych) a predstaviteľov finančných skupín.

Na strane druhej *eliminácia šírenia hybridných hrozieb vo verejnej správe* je systém opatrení legislatívneho, organizačného, inštitucionálneho, personálneho, finančného a informačno-evidenčného charakteru smerujúceho k posilneniu subjektov vykonávajúcich činnosti cielené k zamedzeniu negatívnych vplyvov hybridných hrozieb na charakter právneho štátu a garantovať bezpečnosť jednotlivca, spoločnosti a štátu v danej sociálnej realite. Kvalitatívne ovplyvňuje uvádzanú elimináciu šírenia hybridných hrozieb vo verejnej správe aplikácia zásad eliminácie medzi ktoré patrí zásada legality a legitimacy, zásada objektívnosti, zásada prezentovania relatívnej pravdy, zásada odbornosti, zásada primeranosti, zásada spolupráce, zásada hodnovernosti, zásada evidenčná a zásada kontroly. V súčasnej dobe za jednu z primárnych nástrojov eliminácie hybridných hrozieb pokladáme využitie umelej inteligencie. Ďalším nástrojom eliminácie sa stáva *ohlasovanie hybridných hrozieb* kompetentným subjektom majúcim adekvátne vedomosti a znalosti o identifikácii hybridných hrozieb. Eliminácia šírenia hybridných hrozieb má svoju aktívnu a pasívnu stránku. *Aktívna stránka* obsahuje koordinovaný súbor aktivít kompetentných štátnych orgánov a inštitúcií, ktoré zahŕňajú identifikovanie a analýzu jednotlivých metód hybridných hrozieb a následnú reakciu vo forme koordinovaných činností s cieľom narušiť dôvernosť alebo integritu hybridných hrozieb, ktoré ohrozujú fungovanie verejnej správy. *Pasívna stránka* predstavuje koordinovaný súbor aktivít realizovaných v oblasti bezpečnosti subjektov

²⁴ PORADA, V. a kol. 2019. Bezpečnostní vědy. s. 644

verejnej správy, zaznamenávania metód hybridných hrozieb, monitoring hybridných hrozieb a prijímanie opatrení na elimináciu hybridných hrozieb. V neposlednej rade *eliminácia vplyvu hybridných hrozieb* na činnosť orgánov verejnej správy obsahuje identifikáciu foriem hybridných hrozieb, identifikáciu metód využívaných v rámci hybridných hrozieb, identifikáciu vplyvu hybridných hrozieb na formy a metódy činnosti verejnej správy, identifikáciu cieľov a subjektov realizácie hybridných hrozieb a identifikáciu legislatívnej ochrany subjektov verejnej správy voči hybridným hrozbám. Zároveň si musíme uvedomiť, že subjektmi realizácie hybridných hrozieb sa stávajú predovšetkým štátne organizácie a inštitúcie, neštátne inštitúcie, polovojenské organizácie, iné právnické osoby (súkromný sektor) a fyzické osoby.

Nezabúdajme na *bezpečnostné opatrenia* smerujúce k eliminácii hybridných hrozieb vo verejnej správe ktorých obsahom sú úlohy v legislatívnej, organizačnej, personálnej, finančnej, evidenčnej a technickej oblasti, ktorých cieľom je garantovanie bezpečnosti subjektov verejnej správy. Prijímanie bezpečnostných opatrení sa realizuje s cieľom predchádzať ohrozeniu subjektov verejnej správy a minimalizovanie vplyvu hybridných hrozieb na činnosť a organizačnú štruktúru verejnej správy.

Z hľadiska fungovania právneho štátu a realizácie jeho základných princípov ako princíp legality, princíp legitimacy a princíp humanizmu je dôležité uviesť právny rámec eliminácie hybridných hrozieb. Tento právny rámec tvorí systém prameňov práva, ktoré rozdeľujeme na materiálne pramene, formálne pramene, epistemologické pramene a teleologické pramene. Ďalej sa právny rámec v súvislosti s členstvom Slovenskej republiky v EÚ delí na európsku právnu úpravu (materiálne a formálne pramene, primárne a sekundárne).

Dôležité pre elimináciu hybridných hrozieb a boj proti šíreniu týchto hrozieb vo verejnej správe je identifikovanie jednotlivých oblastí v ktorých sa realizujú hybridné hrozby. V súčasnosti sem zaradíme kritickú infraštruktúru, dezinformácie, kybernetickú bezpečnosť, energetickú bezpečnosť, ovplyvňovanie volieb, ovplyvňovanie činnosti politických strán a hnutí, extrémizmus, nelegálnu medzinárodnú migráciu, šírenie nenávisťi a intolerancie, potravinovú bezpečnosť, organizovanú trestnú činnosť, korupciu, vlastníctvo zdrojov vody, výskum a inovácie, vzdelávanie, životné prostredie, terorizmus, separatizmus a iredentizmus, získavanie utajovaných skutočností, priemyselná špionáž, nelegálne obchodovanie so zbraňami. Vymenované oblasti sa môžu dopĺňať s ohľadom na ďalší vývoj spoločnosti a medzinárodných vzťahov.

Z hľadiska eliminácie systému rozširovania hybridných hrozieb vo verejnej správe je dôležité uplatňovanie transparentnosti, otvorenosti, účinnosti a súdržnosti v rámci dobrej správy vecí verejných. Znamená to taktiež zaviesť právne záruky, aby sa zabránilo svojvoľnému rozhodovaniu. Postupy v rámci zamestnávania a menovania do funkčných pozícií predovšetkým v štátnych orgánoch a inštitúciách by mali byť založené na jasne vymedzených a verejne dostupných kritériách policajných a bezpečnostných štruktúr nevynímajúc. Klasifikácia a sprístupňovanie dokumentov v oblasti bezpečnostnej správy majú podliehať oficiálne schváleným a predvídateľným postupom. Informácie majú byť verejné pokiaľ neobsahujú utajované skutočnosti s cieľom zvýšiť transparentnosť a porozumenie. Účinný systém vnútornej kontroly by mali byť zavedené v rámci jednotlivých štátnych orgánov a inštitúcií. Mechanizmy preverovania, dodržiavania etického kódexu, kontrola zo strany občianskej spoločnosti takisto prispievajú k zodpovednosti za vykonávanie činností zamestnancov.

Dôležitou výzvou v súvislosti so šírením hybridných hrozieb je zvyšovanie informovanosti a vzdelávanie zamestnancov verejnej správy, aby dokázali rozlíšiť informácie od dezinformácií. Primárnou formou v tejto oblasti je strategická komunikácia. Zlepšenie spolupráce v oblasti strategickej komunikácie v systéme štátnych orgánov a inštitúcií má zásadný význam a vyžaduje si prípravu a nácvik napríklad na krízové situácie v reálnom čase a priestore. Rozšírenie odborných znalostí a vedomostí zvyšuje možnosť adekvátnej reakcie na elimináciu metód využívaných pri rozširovaní hybridných hrozieb.

Hybridné hrozby majú vplyv na racionalitu, efektívnosť, hospodárnosť a praxeologickú časť fungovania verejnej správy. Vplýva na objektívne rozhodovanie orgánov verejnej správy v rámci realizácie princípov právneho štátu. Idey prezentované prostredníctvom hybridných hrozieb negatívne pôsobia na správno-bezpečnostné prostredie a smerujú k ovplyvňovaniu konaní v rámci identifikovania právnych skutočností dôležitých pre rozhodovanie orgánov verejnej správy. Z hľadiska činnosti orgánov verejnej správy majú hybridné hrozby vplyv na administratívno-právnu činnosť a bezpečnostno-právnu činnosť. Znamená to ovplyvňovanie jednotlivých etáp činností vykonávaných vo verejnom záujme a službe obyvateľom, ovplyvňovanie aplikácie právnych noriem smerujúce k rozhodovaniu a samotnému rozhodnutiu a špeciálne v rámci správneho konania, priestupkového konania, správno-súdneho konania, konania v rámci lex specialis. Rozhodovanie môže byť následne pozitívne alebo negatívne v prospech subjektu alebo účastníka konania. Ovpľyvňovanie myslenia, konania personálneho substrátu orgánov verejnej správy môže mať vplyv na verejnú mienku smerujúcu k zmene postojov k vybraným subjektom verejnej správy ako sú štátne orgány a inštitúcie. Medzi faktory ovplyvňujúce realizáciu hybridných hrozieb ovplyvňujúce subjekty verejnej správy patrí teritorialita, temporalita, personalita a funkcionalita.

Formy hybridných hrozieb s jasným obsahom sú prezentované v elektronickej, printovej, zvukovo-obrazovej, zvukovej forme a iných formách za využitia moderných informačných technológií. Tento obsah má svoju informačnú hodnotu, ktorá spravidla negatívne ovplyvňuje systém rozhodovania a samotné rozhodnutie a zásadným spôsobom môže ovplyvniť činnosť orgánov verejnej správy pri mimoriadnych udalostiach, krízových situáciách či organizované činnosti subjektov kritickej infraštruktúry. Obsah zasahuje do bezpečnostného systému štátu to znamená aj do verejnej správy, organizačnej štruktúry nevynímajúc. Znamená to aj vplyv na samotnú činnosť štátnych orgánov a inštitúcií tvoriacich systém verejnej správy z hľadiska organizačného. Spôsoby realizácie hybridných hrozieb môžu byť skryté alebo verejne dostupné. Základnou formou realizácie hybridných hrozieb je dezinformácia. Primárnymi metódami realizácie hybridných hrozieb sú presvedčovanie, pozorovanie, analytická činnosť, komparácia a ďalšie vedecké metódy. Medzi prostriedky realizácie hybridných hrozieb radíme finančné, technické, informačné, evidenčné a iné prostriedky.

V neposlednej rade je nutné uviesť formy a metódy činnosti verejnej správy a taktiež rozhodovacie procesy vo verejnej správe, ktoré sú cieľom realizácie hybridných hrozieb. Základnými metódami verejnej správy na ktoré vplývajú hybridné hrozby sú presvedčovanie a donucovanie. Ďalším cieľom realizácie hybridných hrozieb sú formy verejnej správy ako normotvorné formy, jednostranné právno-realizačné formy, správne dohody, spoločenskoorganizačné opatrenia a materiálno-technické operácie.²⁵ Do systém rozhodovacích procesov, ktoré ovplyvňujú hybridné

²⁵ ŠKULTÉTY, P. a kol. 1997. Správne právo hmotné. Všeobecná a osobitná časť. s.70 a 82-95.

hrozby patria rozhodovacie procesy v oblasti realizácie práva, rozhodovacie procesy v oblasti riadiacej a organizátorskej činnosti a rozhodovacie procesy v oblasti aplikácie práva.²⁶

Orgány verejnej správy sú cieľom rozširovania hybridných hrozieb za účelom pozitívneho alebo negatívneho rozhodovania v prospech subjektov realizujúcich hybridné hrozby. Systém verejnej správy existuje predovšetkým na realizáciu a aplikáciu právnych noriem, ktoré majú garantovať dobrú správu vecí verejných. Hoci je tento koncept teoreticky jasný, v praxi môžu nastať určité ťažkosti predovšetkým s aplikáciou právnych noriem. Tieto ťažkosti okrem iného môžu zapríčiniť aj metódy a formy realizácie hybridných hrozieb či využívané prostriedky na ovplyvňovanie rozhodovacích procesov orgánov verejnej správy. Z uvedeného dôvodu je dôležité realizovať bezpečnostné opatrenia, ktoré eliminujú rozširovanie hybridných hrozieb vo verejnej správe.

5. VÝSKUM DOSAHU REALIZÁCIE HYBRIDNÝCH HROZIEB V BEZPEČNOSTNOM SYSTÉME SLOVENSKEJ REPUBLIKY

Z dôvodu teleologického posúdenia charakteru a úrovne dosahu realizácie hybridných hrozieb pôsobiacich na bezpečnostný systém SR s osobitným zreteľom na činnosti subjektov verejnej správy, výskumný tím zastrešovaný Akadémiou Policajného zboru v Bratislave, ktorého členom je aj spracovateľ vedeckej štúdie, realizoval prieskum verejnej mienky dotazníkovou technikou. Zber dát prebiehal od 17. 2. do 18. 5. 2023 elektronickou cestou. Výskumnú vzorku tvorilo 60 respondentov – pedagógov, pracovne alebo služobne zaradených na Akadémii Policajného zboru v Bratislave na pracovných pozíciách, ktoré vyžadujú ukončené vysokoškolské vzdelanie minimálne 2. stupňa, z toho 37 mužov a 23 žien.

Úlohou respondentov, okrem iného, bolo posúdiť stupeň závažnosti hybridných hrozieb vo vzťahu k ohrozeniu SR. V rámci vyhodnocovania odpovedí respondentov sme sa zamerali len na pôsobenie hybridných hrozieb na verejnú správu. V oblasti vedenia nepriateľských kampaní v súvislosti s nedostatočným preverovaním zamestnancov verejnej správy, ktorí môžu pracovať v prospech tretích strán 18 % respondentov hodnotilo ako kritické riziko, 38 % pokladá uvedený problém za vysoko rizikový, 30 % si myslí že uvedený problém je stredne rizikový, kým ale 14 % sa vyjadrilo že je riziko nízke. V oblasti narušenia alebo zníženia bezpečnosti eGovernmentu v časti podceňovania kybernetických hrozieb v štátnej/verejnej správe 42 % opýtaných pokladá túto skutočnosť za vysoké riziko, 35 % opýtaných pokladá tento problém za stredne rizikový, 9 % za kritické riziko a len 8 % percent za riziko nízke. Len 10 % percent respondentov nedostatočné zabezpečenie informačných a kybernetických systémov štátnej/verejnej správy, ktoré slúžia na komunikáciu občanov so štátom považuje za rizikovo nízke. Naopak až 66 % uvedenú skutočnosť vníma ako stredne alebo vysoké riziko z hľadiska zabezpečenia uvedených systémov, ktoré majú byť v prospech občanov. Z celkového počtu opýtaných len 24 % toto nedostatočné zabezpečenie považuje za kritické riziko. V rámci nedostatočného vzdelávania zamestnancov štátnej/verejnej správy ohľadom kybernetickej bezpečnosti 67 % respondentov sa vyjadrilo že je to stredné až vysoké riziko, 30 % označilo tento problém za kritické riziko a len 6 % opýtaných v tom nevidí žiadne alebo len nízke riziko pre činnosť subjektov verejnej správy. V oblasti strategickej korupcie v časti nedostatočnej odolnosti zamestnancov štátnej správy a politických predstaviteľov voči korupčnému správaniu až 56 % respondentov sa vyjadrilo že korupčné správanie je riziko vysoké

²⁶ VRABKO, M. a kol. 2009. Správne právo. Procesná časť. s. 20-23.

až kritické pre fungovanie štátneho mechanizmu, 33 % vníma tento problém ako stredne rizikový a len 11 % opýtaných považuje túto nedostatočnú odolnosť za žiadne alebo nízke riziko.

V súvislosti s problematikou strategickej korupcie je nutné uviesť, že patrí k citlivým témam v SR, ktorým je predovšetkým v informačnom priestore prikladaná patričná váha, dôkazom čoho je celý rad mediálne sledovaných prípadov korupcie. Z uvedeného dôvodu je možné konštatovať, že táto oblasť bola respondentmi hodnotená ako najrizikovejšia pre fungovanie štátnej správy. Zároveň je nutné upozorniť na skutočnosť, že je potrebné hľadať nové, inovatívne, systémové, koncepčné, efektívne, racionálne a technické riešenia, ktoré prispievajú k posilneniu spôsobilostí orgánov verejnej správy včas identifikovať a eliminovať hybridné hrozby.

ZÁVER

Súčasný poznávanie procesov, javov a dejov v systéme verejnej správy dáva predpoklad k vedeckému skúmaniu spoločenskej reality – správy vecí verejných ako samostatnej vednej disciplíny ktorá je relatívne nezávislá na systéme správneho práva a súčasťou správnej vedy s vlastným predmetom a systematickou. Skúmanie činností subjektov verejnej správy a predovšetkým orgánov verejnej správy pri eliminácii rozširovania hybridných hrozieb sa stáva realitou. Priamy vzťah medzi činnosťami orgánov verejnej správy a vplyvu hybridných hrozieb na systém verejnej správy je v spoločnom subjekte. Systém rozširovania hybridných hrozieb vo verejnej správe sa skladá z jednotlivých prvkov medzi ktoré radíme objekt, predmet, subjekty, ciele, formy, metódy a prostriedky. Zároveň podotýkame, že medzi základné subjekty ovplyvňujúce a tvoriace uvádzanú sociálnu realitu patria jednak právnické a fyzické osoby, predovšetkým cudzinci ako aj štátne a neštátne orgány a inštitúcie tretích krajín. V budúcnosti bude dôležité sústrediť pozornosť nie len na elimináciu rozširovania hybridných hrozieb v štátnej správe ale taktiež v samosprávne, vo verejnoprávných korporáciách a subjektoch osobitnej správy. Skúmanie systému realizácie hybridných hrozieb bude dôležitou súčasťou ochrany bezpečnosti jednotlivca, spoločnosti a štátu z pohľadu bezpečnostných vied. Dôvodom je skutočnosť, že hybridné hrozby priamo ovplyvňujú predovšetkým negatívne systém ochrany vnútornej bezpečnosti štátu. Hybridné hrozby smerujú do tých oblastí činnosti štátnych orgánov a inštitúcií samosprávy nevynímajúc, ktoré sú životne dôležité pre fungovanie štátu, V neposlednej rade ovplyvňovanie rozhodovacích procesov orgánov verejnej správy môže mať katastrofálne následky pri riešení krízových situácií.

Všetky aktivity v rámci realizácie hybridných hrozieb smerujú k prehodnoteniu tradícií a hodnôt preferovaných spoločnosťou a jednotlivcami, k destabilizácii štátu a spoločnosti, k prevzatíu moci v štáte alebo k jeho zániku. Realizácia hybridných hrozieb v konečnom dôsledku vplýva na štátny, politický a policajný systém dôsledkom čoho je oslabenie pôsobenia štátneho, štátno-administratívneho a policajného mechanizmu. Z uvedeného dôvodu SR musí mať vytvorený systém štátnych orgánov a inštitúcií, ktoré sú kompetentné koordinovať prípravné, plánovacie, riadiace, realizačné a kontrolné opatrenia v oblasti eliminácie rozširovania hybridných hrozieb aj vo verejnej správe. Primárnym subjektom v uvedenom systéme musí byť vláda SR a Bezpečnostná rada SR..

Zdroje

1. Annual progress reports on countering hybrid threats – JOIN(2017) 30 final, 19. 7. 2017.

2. Annual progress reports on countering hybrid threats – JOIN(2018) 14 final, 13. 6. 2018.
3. Annual progress reports on countering hybrid threats – SWD(2019) 200 final, 29. 5. 2019.
4. Annual progress reports on countering hybrid threats – SWD(2020) 153 final, 24.7.2020.
5. Annual progress reports on countering hybrid threats – SWD (2021) 729, 22. 7. 2021.
6. Annual progress reports on countering hybrid threats – SWD(2022) 308, 16. 9. 2022.
7. Council conclusions on CSDP – Consilium 8971/15, 18. 5. 2015, European Council meeting (25 and 26 June 2015) – Conclusions – EUCO 22/15, 26. 6. 2015.
8. EEAS, 2023. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.
9. HENDRYCH, D. a kol. 2016. Správni právo. Obecná časť. Praha: C.H. Beck, 2016. 599 s. ISBN 978-80-7400-624-1
10. NBÚ. 2022. Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNYPPLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf>.
11. NESVADBA, A. 2022. Teória štátu. Bratislava: Akadémia Policajného zboru v Bratislave, 2022. 167 s. ISBN 978-80-8054-930-5
12. Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – O stratégii EÚ pre bezpečnostnú úniu – COM(2020) 605 final.
13. PORADA, V. a kolektív. 2019. Bezpečnostní vědy. Plzeň: Aleš Čeněk, 2019, 784 s. ISBN 9788073807580.
14. Slovenská informačná služba. 2020. O nás: Národné bezpečnostné analytické centrum (NBAC). [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/o-nas/nbac.html>.
15. Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES – L 333, 27.12.2022, s.164.
16. Spoločné oznámenie Európskemu parlamentu a Rade – Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie – JOIN(2016) 18 final – 6. apríl 2016.
17. Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby – JOIN(2018) 16 final.
18. ŠKULTÉTY, P. a kolektív. 1997. Správne právo hmotné. Všeobecná a osobitná časť. Bratislava: Vydavateľské oddelenie Právnickej fakulty UK. 1997. 248 s. ISBN 80-7160-026-1.
19. ŠKULTÉTY, P. 2008. Verejná správa a správne právo. Bratislava: VEDA, 2008. 204 s. ISBN 978-80-224-1023-4..
20. The Lanscape of Hybrid Threats: A conceptual Model (prostredie hybridných hrozieb: koncepčný model), JRC117280, vypracované na základe spolupráce medzi Spoločným výskumným centrom a Európskym centrom excelentnosti pre boj proti hybridným hrozbám.
21. TÓTHOVÁ, K. a kolektív. 1993. Základy správneho práva hmotného. Bratislava: Vydavateľské oddelenie Právnickej fakulty UK. 1993. 172 s. ISBN 80-7160-059-8
22. VRABKO, M. a kolektív. 2009. Správne právo. Procesná časť. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, Oddelenie edičnej a vydavateľskej činnosti, 2009. 230 s. ISBN 978-80-7160-234-7.
23. Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

24. Uznesenie vlády Slovenskej republiky č. 486/2018 zo dňa 17. októbra 2018.
25. Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.
26. Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.
27. Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy [online] : Projekt podporený z Európskeho sociálneho fondu. Operačný program Efektívna verejná správa. Prijímateľ MV SR. Kód projektu ITMS2014+: 314011CDW7.

AKTIVITY TAJNÝCH SLUŽIEB V SYSTÉME REALIZÁCIE HYBRIDNÝCH HROZIEB A V SYSTÉME IDENTIFIKÁCIE A MINIMALIZÁCIE ICH ŠÍRENIA

prof. Dr. Jozef Balga, PhD., doc. JUDr. Monika Hullová, PhD.

Katedra správneho práva Akadémie PZ v Bratislave, jozef.balga@akademiapz.sk, Katedra kriminálnej polície
Akadémie PZ v Bratislave, monika.hullova@akademiapz.sk

Abstrakt: Autori v predkladanom príspevku vo forme vedeckej štúdie prezentujú výsledky vedeckého bádania, ktoré dosiahli v súlade s projektom podporeným z Európskeho sociálneho fondu, v rámci Operačného programu Efektívna verejná správa na tému Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy. Cieľom príspevku je analýza postavenia a funkcie tajných (*spravodajských*) služieb, rešpektujúc pritom systémový náhľad riešenia formulovaného vedeckého problému, ktorý v sebe bezo sporu nesie prvky kontradikcie, aj vzhľadom na to, že tieto špecifické služby môžu na jednej strane pôsobiť v systéme identifikácie a eliminácie (*minimalizácie*) hybridných hrozieb a zároveň aj v systéme ich realizácie (*šírenia*), t. j. v ich pozitívnom aj negatívnom zmysle slova. V závere tejto vedeckej práce prezentujú výsledky prieskumu verejnej mienky v oblasti percepcie hybridných hrozieb na Slovensku, ktoré získali s použitím techniky dotazníka.

Kľúčové slová: hybridné hrozby, systém identifikácie a eliminácie hybridných hrozieb, systém realizácie hybridných hrozieb, pramene práva, materiálne pramene práva, formálne pramene práva, primárne pramene práva, sekundárne pramene práva, tajná služba, spravodajská služba, spravodajská činnosť, metódy a prostriedky spravodajskej činnosti.

ÚVOD

Medzi základné funkcie štátu patrí reprodukčná funkcia, ochranná funkcia, administratívnoprávna funkcia a bezpečnostná funkcia. Subjekty realizujúce štátnu moc sa sústreďujú na zabezpečenie predovšetkým funkcie bezpečnostnej, ktorá zároveň medzi uvedenými funkciami je *primus inter pares*. Na plnenie uvedenej funkcie vplyvajú také prvky, ako je personálny substrát štátu, štátne územie, policajno-bezpečnostný mechanizmus a realizátori štátnej moci. Pre spoločnosť, skupiny a jednotlivcov je dôležité, aby v reprodukčnom prostredí boli vytvorené zodpovedajúce pravidlá pre aplikáciu kompetencií subjektov, ktoré garantujú bezpečnosť. Vo veľkej miere, bezpečnosť ovplyvňuje funkčnosť spoločnosti a jej ďalší vývoj. Správne nastavený systém ochrany bezpečnosti z dlhodobého hľadiska pozitívne pôsobí na štátne orgány a inštitúcie plniace úlohy v bezpečnostnom systéme štátu. Zároveň upozorňujeme na skutočnosť, že subjekty ochrany bezpečnosti v rámci plnenia svojich kompetencií sú viazané princípom legality, princípom legitimacy a princípom humanizmu. Znamená to, v plnej miere dodržiavať právne normy, ktoré upravujú činnosti zamestnancov týchto subjektov a dodržiavať katalóg základných ľudských práv a slobôd. Na strane druhej, v bezpečnostnom prostredí sa vytvoril systém subjektov, ktoré ohrozujú bezpečnosť rôznymi otvorenými alebo utajenými formami, metódami a prostriedkami. Cieľom takýchto aktivít je ohrozenie fungovania štátu, ovplyvňovanie subjektov politického systému a pôsobenie na prvky bezpečnostno-administratívneho mechanizmu v rozhodovacom procese. Medzi uvedené aktivity v súčasnosti radíme aj hybridné hrozby, ktoré priamo ohrozujú základné demokratické hodnoty právneho štátu a slobody jednotlivcov. Súčasťou subjektov vykonávajúcich aktivity v uvedenej oblasti patria tajné (*spravodajské*) služby, ktoré vykonávajú nátlakové a podvrtné činnosti a spravodajské služby, ktorých úlohou je eliminovať resp. minimalizovať tieto činnosti, zohľadňujúc pritom fakt, že úplná eliminácia tohto nežiadúceho javu je aj napriek enormne vynaloženému úsiliu a priori nereálna.

Samotný pojem „*tajné služby*“ sa často používa na označenie štátnych bezpečnostných organizácií pracujúcich utajeným spôsobom. Patria k nim predovšetkým neuniformované policajné zložky (*kriminálna polícia, útvary proti organizovanému zločinu, ekonomická a finančná polícia*), ale tiež protiteroristické komandá, no predovšetkým spravodajské služby (*civilné a vojenské rozvedky a kontrarozvedky*).²⁷ Napriek tomu, že nejde o všeobecne akceptovanú definíciu, považujeme za potrebné uviesť, že s analogickým vymedzením týchto špeciálnych štátnych orgánov, pracujúcich utajeným spôsobom, sa možno stretnúť vo viacerých publikáciách určených pre odbornú či laickú verejnosť. V každom prípade, tajné služby ako subjekty štátneho bezpečnostného sektora resp. štátneho bezpečnostného systému,²⁸ reprezentujú určitý organizačný celok (*organizáciu, inštitúciu*), ktorého základnou funkciou je plnenie cieľov a záujmov štátu, vrátane zaistenia jeho vnútornej a vonkajšej bezpečnosti (*služba štátu, nevyhnutný servis pre najvýznamnejšie subjekty decíznej, t. j. štátno-mocenskej sféry*). Z tohto (*inštitucionálneho, statického*) uhla pohľadu, sa pojem tajné služby významovo prekrýva s pojmami „*spravodajské služby, špeciálne služby, bezpečnostné služby, informačné služby, či výzvedné služby*“²⁹, prípadne rôzne významové kolokácie, ktoré niekedy úplne očividne naznačujú poslanie takejto organizácie a inokedy len veľmi nejasne alebo vôbec („*tajná spravodajská služba, bezpečnostná informačná služba, bezpečnostná agentúra, úrad na ochranu bezpečnosti a obranu, úrad pre zahraničné styky a informácie*“). Skutočnosť, že v kontexte týchto služieb sa často používa gramatický tvar v pluráli, poukazuje na to, že v spoločnosti obvykle operuje viacero takýchto služieb, ktoré analogicky ako pri výraze „*ozbrojené sily*“ symbolizujú spektrum vnútorne diferencovaných a špecificky profilovaných organizácií synergicky a oficiálne operujúcich v bezpečnostnom priestore (*obvykle dva a viac takýchto subjektov*). V súčasnosti má tento pojem skôr archaický, publicistický, než odborný ráz. V minulosti poukazoval na fakt, že nielen činnosť týchto služieb, ale aj ich samotná existencia mali utajený charakter. Nemožno však poprieť, že zásada utajenosti (*konšpirácie*) je jednou z dominantných a univerzálne platných zásad spravodajskej profesionality, ktorá zohľadňuje dynamickú stránku týchto služieb. V tomto zmysle slova pod spravodajskou činnosťou rozumieme aktívny, systematický a cieľavedomý proces získavania, zhromažďovania, spracovávaní a využívania informácií z rôznych (*často aj utajených*) zdrojov a spravidla utajeným spôsobom, t. j. za použitia osobitných metód, prostriedkov a foriem činnosti. Práve z tohto (*procesuálneho, dynamického*) hľadiska, sa pojem tajné služby prelína s pojmami „*vyzvedačstvo, špionáž, rozvedka, prieskum, špehovanie a i.*“.³⁰ V tejto súvislosti považujeme za potrebné zdôrazniť, že subjektom spravodajskej činnosti sú aj spravodajské agentúry (*verejné alebo súkromné*), ktorými sa na tomto mieste a v kontexte riešeného problému nebudeme bližšie zaoberať.³¹

²⁷ CHURAN, M. a kol. 2000. Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti, s. 359.

²⁸ Týmto konštatovaním nenegujeme existenciu iných (*neštátnych, privátnych*) subjektov, ktoré operujú v spoločnosti a nezriedka aj priamo v bezpečnostnom prostredí (*napr. súkromné bezpečnostné služby, súkromné armády, žoldnieri*), ani existenciu iných tajných zoskupení (*tajných spoločností, spoločenstiev*), ktoré vznikali už od nepamäti a často fungovali na princípe exkluzivity členstva či ilegality, pričom mali rôzny charakter (*napr. mysticko-náboženský, kriminálny, politicko-sociálny*).

²⁹ ŠKVRNDA, F. 2007. Spravodajské služby a bezpečnosť sveta, s. 75-76.

³⁰ ŠKVRNDA, F. 2007. Spravodajské služby a bezpečnosť sveta, s. 76.

³¹ Objektom záujmu spravodajských agentúr, na rozdiel od tajných spravodajských služieb, sú všetky mediálne známe udalosti; cieľom ich činnosti je kumulácia zisku prostredníctvom predaja a šírenia správ širokej verejnosti; výstupným produktom ich činnosti je spravidla neutajovaná informácia poskytovaná širokému okruhu adresátov (*t. j. komukoľvek*) a spôsoby získavania informácií (*napr. metódy, prostriedky, formy*) nie sú striktné vymedzené zákonom (*t. j. informácie môžu získavať akýmkoľvek spôsobom, ktorý zákon vyslovene nezakazuje*).

V ďalšej časti štúdie sa bližšie sústreďíme na analýzu systému identifikácie a minimalizácie šírenia hybridných hrozieb z rôznych aspektov, ale aj na analýzu systému realizácie (*šírenia*) hybridných hrozieb tajnými službami. Ako sme už vyššie naznačili, prezentovaná ambícia (*účelová analýza pro et contra*) je súčasťou širšej vedeckej stratégie obsiahnutej v schválenom projekte tematicky orientovanom na problematiku budovania odolnosti spoločnosti voči hybridným hrozbám.³²

1. SYSTÉM IDENTIFIKÁCIE A MINIMALIZÁCIE ŠÍRENIA HYBRIDNÝCH HROZIEB Z HĽADISKA EURÓPSKEJ ÚNIE

V novembri 2010 prijala Komisia Stratégiu vnútornej bezpečnosti Európskej únie: päť krokov k bezpečnejšej Európe, ktorá určuje strategické piliere vnútornej bezpečnosti EÚ. Ich štruktúra bola postavená na sérii opatrení, ktorých účel spočíval v rozložení medzinárodných zločineckých sietí; zabráňovaní terorizmu, radikalizácii a náboru iných členov; zvýšení úrovne bezpečnosti občanov a podnikateľskej verejnosti v kybernetickom priestore a na zvýšení bezpečnosti prostredníctvom riadenia hraníc. Členské štáty boli v tejto stratégii okrem iného vyzvané, aby do roku 2012 vypracovali vlastné metódy posudzovania hrozieb a od roku 2013 spoločne s Komisiou a koordinátorom Európskej únie (*d'alej len EÚ*) pre boj proti terorizmu pripravovali pravidelný prehľad aktuálnych hrozieb.³³

Z uvedeného je zrejmé, že hrozby, ktorým EÚ čelila na začiatku 21. storočia, mali jasne vymedzené kontúry, hoci s explicitným formulovaním potreby reagovať na hrozby s prívlastkom „hybridné“ sme sa v euro priestore na oficiálnej úrovni prvýkrát stretli až v roku 2014 (*išlo napr. o politické usmernenia predsedu Komisie Jean-Claude Junckera z roku 2014, Závery Rady o spoločnej bezpečnostnej a obrannej politike z mája 2015, Závery Európskej rady z júna 2015*).³⁴

Následne, Európsky program v oblasti bezpečnosti, prijatý v roku 2015, uvádzal ambíciu EÚ vytvoriť priestor vnútornej bezpečnosti, v rámci ktorého sú jednotlivci chránení v plnom súlade so základnými právami. V tejto súvislosti možno poznamenať, že program sa zameriaval na príbuzné priority, ktoré boli prezentované v stratégii EÚ z roku 2010.³⁵ Z uvedeného vyplýva niekoľko čiastkových záverov. V prvom rade, hybridné hrozby boli už registrované nielen ako potenciálny, ale jednoznačne ako reálny bezpečnostný problém, ktorému je potrebné venovať pozornosť zo strany tvorcov politik. V druhom rade, otvorený boj proti hybridným hrozbám, v kontexte tematicky orientovaných dokumentov, či cielených aktivít a krokov na pôde EÚ, sa formálne začal realizovať až o čosi neskôr, konkrétne od roku 2016, v súvislosti s prijatím tzv. Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ.

³² Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy [online] : Projekt podporený z Európskeho sociálneho fondu. Operačný program Efektívna verejná správa. Prijímateľ MV SR. Kód projektu ITMS2014+: 314011CDW7.

³³ Oznámenie Komisie Európskemu parlamentu a Rade: Stratégia vnútornej bezpečnosti EÚ: päť krokov k bezpečnejšej Európe – COM(2010) 673 v konečnom znení, 22. 11. 2010.

³⁴ Council conclusions on CSDP – Consilium 8971/15, 18. 5. 2015, European Council meeting (25 and 26 June 2015) – Conclusions – EUCO 22/15, 26. 6. 2015.

³⁵ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Európsky program v oblasti bezpečnosti – COM(2015) 185 final.

Pokiaľ budeme skúmať systém boja proti hybridným hrozbám zo strany EÚ, je nutné uviesť samotnú charakteristiku hybridných hrozieb, ktoré ohrozujú bezpečnostnú situáciu v EÚ. V zmysle materiálnych prameňov práva EÚ, hybridné hrozby chápeme ako súbor rôznych nátlakových a podvratných činností, konvenčných a nekonvenčných metód (*napríklad diplomatických, vojenských, ekonomických a technologických*), ktoré môžu rôzne štátne a neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu.³⁶

V tomto smere možno predmetný spoločný rámec vnímať ako kľúčový koncepčný dokument, ktorý nielenže prvýkrát zakotvil definíciu hybridných hrozieb v materiálnych prameňoch práva EÚ, ale sústredil sa aj na ďalšie podstatné náležitosti riešenia tohto problému (*1. identifikáciu hybridných hrozieb; 2. zlepšovanie informovanosti a nastavenie vhodného inštitucionálneho rámca a mechanizmu pre strategickú komunikáciu; 3. budovanie odolnosti v jednotlivých oblastiach a boj proti financovaniu hybridných hrozieb; 4. prevenciu, reakciu na krízu spôsobenú hybridnými hrozbami a obnovu; 5. posilnenie spolupráce s NATO*). Z hľadiska primárnych prameňov práva EÚ, spoločný rámec uvádza článok 222 Zmluvy o fungovaní EÚ, ako možnosť pomoci členskému štátu v prípade, ak sa členský štát stane obeťou značných hybridných hrozieb. Zároveň zdôrazňuje skutočnosť, že pri eliminácii rozsiahlych a závažných prejavov hybridných hrozieb sa môže realizovať aj intenzívnejšia spolupráca a koordinácia s NATO. V tejto súvislosti nemožno opomenúť fakt, na ktorý spoločný rámec poukázal, a to že hybridné hrozby sú aj vzhľadom na ich charakter výsoťou národnou kompetenciou členských štátov (*primárne ohrozujú národné bezpečnostné a obranné záujmy*). Napriek tejto skutočnosti, EÚ sa od riešenia tohto závažného bezpečnostného problému úplne nedištancovala, ale ponúkla členským štátom komplexný návrh stratégie boja proti hybridným hrozbám, rozčlenený do piatich základných oblastí, resp. v užšom zmysle slova do 22 konkrétnych opatrení.

V rámci boja proti hybridným hrozbám bola v nadväznosti na tieto kroky prijatá Spoločná správa Európskemu parlamentu a Rade o vykonávaní Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ.³⁷ Spoločná správa reaguje na zvýšenú intenzitu činností v rámci hybridných hrozieb v takých oblastiach, ako je ovplyvňovanie volieb, dezinformačné kampane, negatívne aktivity v kybernetickom priestore a radikalizácia zraniteľných členov spoločnosti. Obsahom spoločnej správy je aj systém opatrení a určenie subjektov, ktoré tieto opatrenia majú realizovať. V závere správa opätovne upozorňuje členské štáty na primárnu zodpovednosť za boj proti hybridným hrozbám súvisiacich s národnou bezpečnosťou. Okrem toho považujeme za potrebné zdôrazniť, že implementácia opatrení stanovených v spoločnom rámci sa monitoruje pravidelne, pričom Európska komisia, prostredníctvom svojho útvaru – Generálneho riaditeľstva pre obranný priemysel a vesmír (*angl. Directorate-General for Defence Industry and Space – DEFIS*) v spolupráci s ESVČ (*angl. European External Action Service – Európska služba pre vonkajšiu činnosť*), každoročne (*teda od roku 2017 do roku 2022*) predkladá správu o úrovni pokroku v tejto oblasti, pričom aj do budúcnosti možno s veľkou pravdepodobnosťou očakávať kontinuálne pokračovanie v nastavenom trende.³⁸

³⁶ Spoločné oznámenie Európskemu parlamentu a Rade – Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie – JOIN(2016) 18 final – 6. apríl 2016.

³⁷ Annual progress reports on countering hybrid threats – JOIN(2017) 30 final.

³⁸ Annual progress reports on countering hybrid threats – JOIN(2017) 30 final, 19. 7. 2017; JOIN(2018) 14 final, 13. 6. 2018; SWD(2019) 200 final, 29. 5. 2019; SWD(2020) 153 final, 24.7.2020; SWD (2021) 729, 22. 7. 2021; SWD(2022) 308, 16. 9. 2022.

V roku 2018 bolo následne vypracované a prijaté Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby.³⁹ V rámci reakcie EÚ na silnejšie hybridné hrozby sa podnikli dôležité kroky na vybudovanie štruktúr potrebných na zlepšenie situačného povedomia a podporu rozhodovania. Strategickú úlohu tu zohrávalo práve Stredisko EÚ pre hybridné hrozby (*formálne označované ako „EU Hybrid Fusion Cell“, resp. „EU HFC“*), ktoré bolo, v nadväznosti na spomínaný spoločný rámec, zriadené v roku 2016. EU HFC je organizačne začlenené pod Spravodajské analytické centrum EÚ (*angl. Intelligence Analysis Centre – EU INTCEN*) v rámci ESVČ, čo sa logicky odzrkadľuje aj v rozsahu pôsobnosti tejto integrovanej spravodajskej jednotky pre boj proti hybridným hrozbám. Pre doplnenie uvádzame, že oficiálnym predchodcom tohto centra bolo Spravodajské a situačné centrum EÚ (*angl. The EU Intelligence and Situation Centre – EU SITCEN, príp. SITCEN EÚ*), ktoré bolo zriadené v roku 2002, teda rok po nešťastných udalostiach súvisiacich s teroristickými útokmi v New Yorku. K hlavným úlohám centra/vrátane strediska patrí poskytovanie spravodajských a analytických produktov určeným adresátom, napr. ESVČ, rozhodovacím orgánom EÚ a členským štátom. Zároveň vystupujú ako jednotné kontaktné miesta v EÚ pre utajované informácie pochádzajúce z civilných spravodajských a bezpečnostných služieb členských štátov, čo vnímame ako veľmi podstatný fakt vo vzťahu ku koordinácii spravodajskej činnosti. Nemalú zásluhu na tom má aj ich kvalitný a vysoko erudovaný personálny aparát, čo do istej miery súvisí s tým, že pod záštitou centra/strediska pracujú národní experti a zamestnanci spravodajských služieb členských štátov. V týchto intenciách považujeme za potrebné zdôrazniť, že centrum/stredisko nemajú povahu spravodajskej služby v pravom zmysle slova, tzn. že nedisponujú vlastnými operatívnymi a spravodajskými kapacitami, ale sú len (*tak ako sme to už naznačili vyššie*) miestom kumulácie, analýzy a distribúcie informácií, ktoré boli získané od iných subjektov (*spravodajských a bezpečnostných služieb členských štátov*), prípadne z tzv. otvorených zdrojov (*realizujú tzv. Open Source Intelligence – OSINT*). Napriek uvedenému zastávame názor, že práve týmito krokmi sa podarilo nastaviť optimálne podmienky nielen pre koordináciu spravodajskej činnosti, ale v konečnom dôsledku aj na získavanie strategických informácií o rôznych druhoch bezpečnostných hrozieb, čo vytvára platformu pre proces rozhodovania nielen na strategickej, ale aj na operačno-taktickej úrovni. Okrem toho, z pohľadu koordinácie spravodajskej činnosti a následných prijatých opatrení, nemožno opomenúť skutočnosť, že kontaktný bod (*angl. Point of Contact alebo PoC*) pre EU HFC a pre EU INTCEN na Slovensku je náš národný SITCEN, ktorého úlohou je zabezpečovať nepretržitý tok informácií a koordináciu tohto toku medzi HFC a Slovenskom, a to oboma smermi. V konkrétnych reáliách, úlohou SITCEN-u, ako národného kontaktného miesta pre hybridné hrozby, je podieľať sa na monitorovaní, analýze a prognóze vývoja bezpečnostnej situácie a v prípade potreby, napr. krízovej situácie, zabezpečiť adekvátnu reakciu zo strany kompetentných orgánov na Slovensku alebo v zahraničí.

EU HFC má intenzívne pracovné vzťahy s Európskym centrom výnimočnosti pre boj proti hybridným hrozbám (*angl. The European Centre of Excellence for Countering Hybrid Threats – ďalej len „Hybrid CoE“*), ktoré má sídlo v Helsinkách. Európske centrum bolo zriadené v apríli 2017 na posilnenie strategického dialógu a vykonávanie výskumu a analýzy hybridných hrozieb. Pre doplnenie uvádzame, že Slovensko je členom Hybrid CoE od augusta 2020, pričom národným

³⁹ Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby – JOIN(2018) 16 final.

PoC sa, rovnako ako pri EU HFC a EU INTCEN, stal náš SITCEN, ktorý pracuje ako sprostredkovateľ rôznych webinárov, workshopov, vzdelávacích a tréningových aktivít. V tejto súvislosti sa môžeme pochváliť, že v júni 2023 bola realizovaná prvá simulácia hybridného pôsobenia na Slovensku práve na základe spolupráce Ministerstva vnútra Slovenskej republiky (*d'alej len SR*) a Hybrid CoE, pričom slovenská strana v tejto simulácii uspela veľmi dobre.

Spoločné oznámenie, ako sme už poznamenali vyššie, upozornilo na dôležitosť strategickú komunikácie šírením zrozumiteľných informácií prostredníctvom vzdelávania verejnosti, aby bežný občan dokázal rozlíšiť informácie od dezinformácií. Aj v nadväznosti na tieto ciele a v súlade so spoločným rámcom, boli v rámci ESVČ zriadené tzv. Task Forces, ako osobitné útvary pre strategickú komunikáciu. V súčasnosti existujú tri takéto útvary (*pre východ – hlavne Arménsko, Azerbajdžan, Bielorusko, Gruzínsko, Moldavsko a Ukrajinu; západný Balkán; juh – pre arabský svet, t. j. pre Blízky východ, severnú Afriku a Perzský záliv*). V blízkej budúcnosti sa pripravuje aj zriadenie nového útvaru (tzv. *Task Force Afrika*). Hlavnou náplňou práce týchto útvarov je identifikovať a vysvetľovať dezinformačné naratívy a analyzovať dezinformačné trendy, ktoré sú šírené v informačnom priestore. Ich vlajkovým projektom je aj webová stránka, na ktorej je umiestnená databáza článkov a médií, ktoré prezentujú nepravdivé, skreslené alebo neúplné informácie (*EUvsDisinfo*), ako aj tematický týždenník *Disinformation Review*, ktorého poslaním je zvyšovanie povedomia o dezinformáciách. K úspechom tohto tímu expertov na dezinformácie patrí, že sa im podarilo vyvrátiť viac ako 15 000 dezinformačných článkov/príspevkov. Zjednodušene možno povedať, že pridanou hodnotou tohto vysoko odborného tímu (*výstupným produktom činnosti*) sú predovšetkým rôzne odborné analýzy, informácie, správy a podklady určené pre strategickú komunikáciu vládnych a politických špičiek, tlačové služby, ale aj pre širokú verejnosť.

Okrem toho, v predmetnom spoločnom oznámení bola osobitná pozornosť venovaná aj budovaniu odolnosti proti nepriateľskej spravodajskej činnosti. Boj proti nepriateľskej spravodajskej činnosti v súlade s príslušnými pravidlami a opatreniami EÚ a vnútroštátnymi pravidlami a opatreniami členských štátov vyžaduje zvýšenú a účinnú koordináciu medzi členskými štátmi. Nevyhnutné malo byť zvýšenie spôsobilosti inštitúcií EÚ čeliť rastúcej hrozbe takýchto aktivít zameraných výslovne na inštitúcie a vybudovať kultúru informovanosti o bezpečnosti.

Inštitúcie mali takisto spolupracovať s členskými štátmi na budovaní odolnejšieho akreditačného systému EÚ. Takýto systém by bol založený na aktívnom podávaní správ, ktoré by umožnilo lepšiu informovanosť medzi členskými štátmi a inštitúciami o možných nepriateľských subjektoch, najmä tých, ktoré už členské štáty identifikovali. Budúce kroky mali smerovať na udržanie a rozvoj schopnosti EÚ spolupracovať s členskými štátmi v boji proti nepriateľskej spravodajskej činnosti zameranej konkrétne na inštitúcie. Ďalej zdokonaľiť EU HFC doplnením expertíz v oblasti kontrarozviednej činnosti, s cieľom poskytnúť podrobné analýzy a brífingy o povahe nepriateľskej spravodajskej činnosti pravdepodobne vyvíjanej proti jednotlivcom a inštitúciám. Pre predmet nášho výskumu sa spoločné oznámenie stáva dôležitým prameňom pre stanovenie postavenia spravodajských služieb v systéme hybridných hrozieb a aktivít vykonávaných subjektami – štátnymi orgánmi a inštitúciami.

Za účelom rýchleho varovania medzi inštitúciami EÚ a členskými štátmi bol v rámci ESVČ, na základe Akčného plánu proti dezinformáciám z roku 2018,⁴⁰ vytvorený aj špecifický nástroj, tzv. Rapid Alert System (*EU RAS*). RAS ako sieť 28 národných PoC predstavuje nielen digitálnu platformu pre členské štáty a európske inštitúcie, na ktorej môžu zdieľať informácie o dezinformačných kampaniach, analýzach, trendoch a diskutovať o osvedčených postupoch v boji proti dezinformáciám, ale zároveň sa stáva aj nástrojom ich koordinovanej reakcie. RAS pracuje s informáciami z otvorených zdrojov, pričom spolupracuje s akademickým sektorom, overovateľmi faktov (tzv. *fact-checkers*), online platformami, európskymi štruktúrami zaoberajúcimi sa krízovou reakciou, kyberkriminalitou a hybridnými hrozbami, ako aj medzinárodnými partnermi, napr. NATO a G7. Zmyslom takého postupu je v konečnom dôsledku dosiahnuť koordinovanú odpoveď EÚ v boji proti dezinformáciám, a to zvyšovaním informovanosti a povedomia, ktorú vo svojej podstate zabezpečuje ESVČ v spolupráci s Komisiou. V týchto súvislostiach nemožno opomenúť dôležitú úlohu, ktorú zohrával RAS v čase volieb do europarlamentu v máji 2019 a počas pandémie koronavírusu, a ktoré sa stali ozajstnou živnou pôdou pre šírenie dezinformačných kampaní. Pri zabezpečovaní koordinovanej reakcie na tieto incidenty bola, ale aj v súčasnosti je, nevyhnutná rýchla a efektívna spolupráca orgánov a inštitúcií EÚ s členskými štátmi, pričom za SR sa národným PoC pre RAS, analogicky ako pri vyššie uvedených európskych subjektoch operujúcich na tomto úseku, stal náš SITCEN (*spolu s niektorými ďalšími národnými útvarmi pre boj proti hybridným hrozbám a strategickú komunikáciu*).

Pokiaľ hovoríme o inštitucionálnom rámci v rámci systému boja hybridným hrozbám v EÚ, nemožno v tomto kontexte opomenúť *horizontálnu pracovnú skupinu pre zvyšovanie odolnosti a boj proti hybridným hrozbám* (angl. *The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats*), ktorá vznikla v júli 2019 v rámci prípravných orgánov Rady. Pracovná skupina uľahčuje koordináciu činností Rady v oblasti boja proti hybridným hrozbám a podľa potreby spolupracuje s inými prípravnými orgánmi (napr. *horizontálnou pracovnou skupinou pre kybernetické otázky* – angl. *The Horizontal Working Party on Cyber Issues – CYBER*, *Koordinačným výborom pre komunikačné a informačné systémy* – angl. *Coordination Committee for Communication and Information Systems – CCCIS*, *Politickým a bezpečnostným výborom – PBV* – angl. *Political and Security Committee – PSC*), inými inštitúciami, útvarmi a agentúrami EÚ.⁴¹

V nadväznosti na uvedené materiálne pramene práva EÚ zaoberajúce sa hybridnými hrozbami, bola v roku 2020 komisiou vypracovaná Stratégia EÚ pre bezpečnostnú úniu.⁴² Tento dokument zaradil hybridné hrozby do systému bezpečnostných hrozieb ohrozujúcich EÚ. Stratégia zdôraznila potenciál hybridných útokov zo strany štátnych a neštátnych subjektov, ktoré využívajú zraniteľnosť pomocou kombinácie kybernetických útokov, poškodzovania kritickej infraštruktúry, dezinformačných kampaní a radikalizácie politického jazyka. Vzhľadom na neustály vývoj v oblasti hybridných hrozieb sa má, okrem iného, intenzívnejšie klásť osobitný dôraz na začlenenie hybridných hrozieb do tvorby politik, aby sa naďalej udržal krok s dynamickým vývojom, a aby sa

⁴⁰ Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov – Boj proti dezinformáciám na internete: európsky prístup – COM(2018) 236 final, 26. 4. 2018.

⁴¹ Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats: Establishment and adoption of its Terms of Reference – 10027/19, 8. 7. 2019.

⁴² Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – O stratégii EÚ pre bezpečnostnú úniu – COM(2020) 605 final.

zabezpečilo, že sa neprehliadne žiadna potencionálna relevantná iniciatíva. Nové iniciatívy sa budú posudzovať optikou hybridných hrozieb aj v oblastiach, ktoré boli doposiaľ mimo rámca boja proti hybridným hrozbám, ako sú vzdelávanie, výskum a technológie. Pri tomto prístupe sa využije úsilie vyvinuté v oblasti konceptualizácie hybridných hrozieb zabezpečujúc komplexný pohľad na rôzne nástroje, ktoré môžu nepriatelia využívať.⁴³ Z hľadiska predchádzania hybridným hrozbám a ochrany pred nimi, bude aj naďalej kľúčové budovanie odolnosti. Znamená to, určenie odvetvových základných scenárov odolnosti proti hybridným hrozbám pre členské štáty a inštitúcie EÚ.

Neobyčajným vývojom v súvislosti s hybridnými útokmi na EÚ v lete 2021 bol pokus o destabilizáciu EÚ prostredníctvom zneužívania migrantov na vonkajších hraniciach EÚ. Bielorusko v lete 2012 čelilo sankciám po vynútenom pristátí osobného lietadla v máji 2012. Režim reagoval uľahčením príchodu nelegálnych migrantov na hranice Litvy, Lotyšska a Poľska, ktorý svedčil o rozhodnom pokuse o vytvorenie pretrvávajúcej krízy v rámci širšieho sústredeného úsilia o destabilizáciu EÚ. Okrem toho, že migranti boli vystavení značnému osobnému riziku, bolo dôležitou súčasťou činnosti Bieloruska pri zneužívaní migrantov manipulácia s informáciami. EÚ monitorovala, analyzovala a odhalila zahraničnú manipuláciu s informáciami a zasahovanie zo zahraničia a svoje zistenia zdieľala s členskými štátmi a medzinárodnými partnermi prostredníctvom systému rýchleho varovania. Zo strany Bieloruska to bolo štátom podporované zneužívanie migrantov na vonkajších hraniciach EÚ.⁴⁴

Reagujúc na vzniknutú a vznikajúcu bezpečnostnú situáciu v kontexte registrácie a eskalácie hybridných hrozieb, bola spracovaná piata správa o pokroku pri vykonávaní Stratégie EÚ pre bezpečnostnú úniu.⁴⁵ V správe sa konštatovalo, že v poslednom desaťročí sa zaviedlo viac ako 200 opatrení na posilnenie odolnosti proti hybridným hrozbám na úrovni EÚ. V kontexte hodnotenia dosiahnutého progresu na tomto úseku, možno opätovne vyzdvihnúť význam EU HFC, ktorý prispieva k rozhodovaciemu procesu EÚ a je ústredným orgánom, zabezpečuje komplexné situačné povedomie a strategický výhľad, zhromažďuje informácie zo všetkých zdrojov a vykonáva posudzovanie spravodajských informácií týkajúcich sa hybridných hrozieb. K úspechom možno zaradiť aj skutočnosť, že sa začalo pracovať na tvorbe tímov rýchlej reakcie EÚ na hybridné hrozby (*angl. EU Hybrid Rapid Response Teams*), s cieľom podporiť členské štáty, misie a operácie v rámci spoločnej bezpečnostnej a obrannej politiky, hoci tieto tímy ešte doteraz formálne vytvorené neboli. Inšpiráciou v tomto sú v mnohých ohľadoch práve podporné tímy boja proti hybridným hrozbám v rámci NATO (*angl. NATO Counter Hybrid Support Teams*), ktoré boli v roku 2021 nasadené v Litve, či v roku 2019 v Čiernej Hore. Pomernou novinkou je aj tzv. súbor hybridných nástrojov EÚ (*angl. EU Hybrid Toolbox – EUHT*), ktorým sa poskytuje rámec pre koordinovanú reakciu na hybridné kampane, ktoré ovplyvňujú EÚ a členské štáty. Manipulácia s informáciami a zasahovanie do zahraničia, ktorých cieľom je narúšať dôveru v EÚ sa stávajú čoraz dôležitejším prvkom pri hybridných útokoch. Z uvedeného dôvodu bol vypracovaný súbor nástrojov EÚ na boj proti manipulácii s informáciami a zasahovaniu zo zahraničia s cieľom

⁴³ The Landscape of Hybrid Threats: A conceptual Model (*prostredie hybridných hrozieb: koncepcný model*), JRC117280, vypracované na základe spolupráce medzi Spoločným výskumným centrom a Európskym centrom excelentnosti pre boj proti hybridným hrozbám.

⁴⁴ Oznámenie Komisie Európskemu parlamentu a Rade o tretej správe o pokroku v plnení Stratégie EÚ pre bezpečnostnú úniu – COM(2021) 799 final.

⁴⁵ Oznámenie Komisie Európskemu parlamentu a Rade o piatej správe o pokroku pre vykonávaní Stratégie EÚ pre bezpečnostnú úniu – COM(2022) 745 final.

podporiť koordinovanú reakciu na manipulatívne správanie zahraničných subjektov, spravodajských služieb nevynímajúc, tzv. súbor nástrojov FIMI (*angl. Toolbox Foreign Information Manipulation and Interference*).

Ďalším dôležitým dokumentom je Strategický kompas EÚ pre bezpečnosť a obranu,⁴⁶ ktorý obsahuje konkrétne opatrenia nevyhnutné na efektívny boj proti hybridným hrozbám. Členské štáty sa v tejto stratégii zaviazali realizovať aktivity v štyroch základných oblastiach, a to aktivita, bezpečnosť, investície a partneri, pričom problematika boja proti hybridným hrozbám primárne spadá do oblasti bezpečnosti. Práve v poslednej spomenutej sfére si EÚ predsavzala, že zvýši svoje kapacity na analýzu spravodajských informácií, vytvorením (*už vyššie uvádzaných*) súborov nástrojov a tímov rýchlej reakcie na hybridné hrozby. Okrem toho, si EÚ kládla za cieľ – vytvoriť súbor nástrojov kybernetickej diplomacie a v tomto ohľade aj politický rámec EÚ pre kybernetickú obranu a zároveň – vypracovať Stratégiu EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu a posilniť úlohu EÚ ako aktéra námornej bezpečnosti. Rok po schválení Strategického kompasu EÚ, zhodnotili ministri zahraničných vecí a ministri obrany členských štátov EÚ na spoločnom zasadnutí v marci 2023 **pokrok, ktorý sa dosiahol pri jeho vykonávaní.**⁴⁷ Dospeli k záveru, že vo všetkých štyroch pilieroch bol zaznamenaný progres a zároveň určili oblasti, ktoré si vyžadujú ďalšie úsilie. Aktuálne sa vykonáva revízia Protokolu EÚ v boji proti hybridným hrozbám, zároveň sa priebežne testujú a precvičujú aj naše možnosti reakcie na základe rôznych scenárov, aby sme mohli pokračovať vo vývoji nášho koncepčného prístupu k odolnosti a hybridným hrozbám.

Z formálnych prameňov práva na úseku boja proti hybridným hrozbám v súčasnosti je najdôležitejším Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/144/ES.⁴⁸ Uvedená právna norma by sa mala vzťahovať aj na subjekty vykonávajúce činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane vyšetrovania, odhaľovania a stíhania trestných činov alebo poskytujú služby výlučne subjektom verejnej správy, ktoré vykonávajú činnosti prevažne v uvedených oblastiach. Vzhľadom na zodpovednosť členských štátov za ochranu národnej bezpečnosti a obrany, by členské štáty mali mať možnosť rozhodnúť, že povinnosti kritických subjektov, taxatívne vymedzených v smernici, sa na tieto subjekty úplne alebo čiastočne neuplatňujú. Do rozsahu pôsobnosti tejto smernice by však mali patriť subjekty, ktorých služby alebo činnosti súvisia s uvedenými oblasťami len okrajovo. Osobitne sa uvádza subjekt verejnej správy, ktorý je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani obchodný charakter. Tento subjekt má právnu subjektivitu, je z väčšej časti financovaný štátnymi orgánmi alebo inými ústrednými orgánmi, ktoré sa riadia verejným právom, jeho riadenie podlieha dohľadu týchto orgánov. Zároveň má právomoc vydávať správne alebo regulačné rozhodnutia určené fyzickým alebo právnickým osobám, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovaru, služieb alebo kapitálu. V zmysle prílohy smernice sem patria subjekty

⁴⁶Rada EÚ. 2022. Strategický kompas pre silnejšiu bezpečnosť a obranu EÚ v nasledujúcom desaťročí: Tlačová správa z 21. 3. 2022. [online]. [cit. 2023-9-3]. Dostupné na internete: <https://www.consilium.europa.eu/sk/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>.

⁴⁷EEAS, 2023. Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.

⁴⁸ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/144/ES – L 333, 27.12.2022, s.164.

verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom. Transpozičná lehota smernice je určená do 17. októbra 2024. Podotýkame, že uvedená smernica sa bude týkať aj činnosti spravodajských služieb, napríklad pri realizácii previerok zamestnancov kritických subjektov v riadne odôvodnených prípadoch a pri zohľadnení posúdenia rizika členským štátom. A v neposlednom rade musíme upozorniť na skutočnosť, že incident, ktorý môže významne narušiť poskytovanie základnej služby charakterizovanej smernicou, môže byť udalosť spôsobená prostredníctvom hybridných útokov. Z uvedených dôvodov, táto smernica je jedným z právnych nástrojov EÚ aj v boji proti hybridným hrozbám. V súlade s touto smernicou bola na tomto úseku vytvorená skupina pre odolnosť kritických subjektov (*angl. The Critical Entities Resilience Group – CERG*), zriadená sieť ERNCIP (*angl. The European Reference Network for Critical Infrastructure Protection*) a zároveň bolo prijaté odporúčanie Rady o celoúniijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.⁴⁹

Na základe nášho poznania, úplne posledným dôležitým dokumentom, ktorý dotvára systém právnych základov boja proti hybridným hrozbám v EÚ, je nariadenie Európskeho parlamentu a Rady EÚ z októbra 2022 o jednotnom trhu s digitálnymi službami, tzv. Akt o digitálnych službách (*angl. Digital Services Act, resp. DSA*).⁵⁰ Termín DSA sa používa na označenie európskej legislatívy komplexne upravujúcej pravidlá v digitálnom priestore EÚ. Cieľom DSA je prispieť k riadnemu fungovaniu vnútorného trhu so sprostredkovateľskými službami, stanovením harmonizovaných pravidiel pre bezpečné, predvídateľné a dôveryhodné online prostredie a v neposlednom rade riešiť šírenie nezákonného obsahu na internete a spoločenské riziká, ktoré môžu vyplynúť zo šírenia dezinformácií alebo iného obsahu, a v rámci ktorého sú účinne chránené základné práva zakotvené v charte a uľahčujú sa inovácie. V súvislosti s hybridnými hrozbami, toto nariadenie nastavuje pravidlá a povinnosti pre veľké online platformy vo vzťahu k šíreniu dezinformácií na ich službách, t. j. formálne zabezpečuje prevzatie kódexu postupov proti šíreniu dezinformácií⁵¹ do DSA. Poskytovatelia veľmi veľkých online platforiem a veľmi veľkých internetových vyhľadávačov by sa napriek tomu, že nemajú všeobecnú povinnosť monitorovať informácie, ktoré prenášajú (*tzv. kešing*) alebo uchovávajú (*tzv. hosting*), mali zamerať na systémové riziká, vrátane všetkých algoritmických systémov, odporúčaní a reklamných systémov, ale aj na postupy zberu a používania údajov. V kontexte nami riešeného problému možno v stručnosti konštatovať, že úlohou týchto sprostredkovateľských služieb je úzka spolupráca s príslušnými vnútroštátnymi justičnými alebo správnymi orgánmi na úseku identifikácie a minimalizácie negatívnych dôsledkov šírenia hybridných hrozieb.

Sumarizáciou doposiaľ uvedeného a na základe získaných vedeckých poznatkov, systém boja proti hybridným hrozbám z pohľadu EÚ prioritne tvoria nasledujúce prvky – pramene práva EÚ (*materiálne a formálne, primárne a sekundárne*), subjekty (*právnické osoby, fyzické osoby, štátne a neštátne subjekty*), metódy (*analýza, komparácia atď.*), prostriedky (*technické, informačné*,

⁴⁹ Odporúčanie Rady z 8. decembra 2022 o celoúniijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry 2023/C 20/01 – C 20/1, 20. 1. 2023.

⁵⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) – L 277/1, 27. 10. 2022.

⁵¹ Kódex postupov proti šíreniu dezinformácií bol prijatý v roku 2018 a revidovaný v roku 2022. In EURÓPSKA KOMISIA, 2018. EU Code of Practice on Disinformation. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://digital-strategy.ec.europa.eu/sk/library/2018-code-practice-disinformation>; L 95/1, 15. 4. 2010.

evidenčné a iné), prvky spolupráce, vzdelávacie prvky, strategická komunikácia, teritoriálne, časové a teleologické prvky.

Osobitný subsystém subjektov v rámci hybridných hrozieb tvoria subjekty realizujúce hybridné útoky proti štátom s demokratickým politickým systémom a subjekty, ktoré identifikujú a eliminujú tieto útoky v rámci boja proti hybridným hrozbám, napríklad spravodajské služby, polícia, ozbrojené sily a podobne. Našou ambíciou v predkladanej vedeckej štúdii je, okrem iného, bližšie identifikovať a analyzovať systém realizácie hybridných hrozieb tajnými resp. spravodajskými službami.

2. SYSTÉM REALIZÁCIE HYBRIDNÝCH HROZIEB TAJNÝMI SLUŽBAMI

Hybridné hrozby sú dlhodobé, premyslené, v utajení pripravované špecializovanými tímami veľmi vzdelaných, skúsených odborníkov z rôznych oblastí, podporovaných zázemím všetkých štátnych zložiek a ďalšími spolupracujúcimi inštitúciami, ktoré nemusia ani poznať skutočné ciele, poslanie zverených úloh. Rôzne hybridné hrozby môžu byť pripravované tak, aby pôsobili súbežne, vzájomne sa dopĺňovali, harmonicky sa podporovali. Hybridné hrozby sú prekvapivé, náhle a veľmi dobre medializované rôznymi komunikačnými kanálmi. Propaganda jednak ovplyvňuje obyvateľov cieľovej krajiny útoku, zároveň má za úlohu presvedčiť vlastné obyvateľstvo o správnosti a nevyhnutnosti aktivít útočiacej krajiny.⁵²

Činnosti realizované spravodajskými službami v rámci šírenia hybridných hrozieb predstavujú špeciálne úkony a opatrenia týchto služieb smerujúce proti základom právneho štátu. Sú charakteristické rozmanitosťou spôsobov a foriem, a to nie len z hľadiska právneho, ale aj inštitucionálneho, organizačného a personálneho. Relatívne veľké množstvo hybridných útokov sa vykonáva prostredníctvom cudzích komunikačných a iných spravodajských prostriedkov využívajúc neschopnosť mnohých osôb sa správne orientovať v zložitej vnútropolitickej a medzinárodnop politickej situácii. Príprava hybridných útokov býva spojovaná aj s poradnými stretnutiami pracovníkov nepriateľských spravodajských služieb s vytypovanými osobami a vytváraním vhodných podmienok na šírenie napríklad dezinformácií medzi obyvateľmi štátu. Na strane druhej, ide o získavanie dôverných informácií o možných reakciách štátnych orgánov a inštitúcií na hybridné útoky.

V tomto kontexte je možné zdôrazniť, že pre získanie subjektov z radov obyvateľstva SR pre spoluprácu, nepriateľské spravodajské služby môžu vytvárať také situácie, ktorými sú subjekty kompromitovaní alebo ideologicky ovplyvňovaní a postupne získavaní pre spoluprácu. V prevažnej väčšine prípadov si kladú za cieľ získať subjekty k spolupráci predovšetkým z prostredia verejnej správy. Nepriateľské spravodajské služby môžu taktiež vyťažovať subjekty o skutočnostiach predstavujúcich utajované skutočnosti. Zložité a premyslené akcie pre získanie subjektov k spolupráci môžu byť realizované aj v dlhšom časovom horizonte. Príslušníci slovenských spravodajských služieb musia prijímať preventívne opatrenia k paralyzovaniu možných akcií nepriateľských spravodajských služieb v oblasti eliminácie hybridných hrozieb konštruktívnym uplatňovaním svojich kompetencií. Dôležitou súčasťou boja proti hybridným hrozbám bude využívanie osôb konajúcich v prospech spravodajských služieb s cieľom získať

⁵² PORADA, V. a kolektív. 2019. Bezpečnostní vědy, s.666.

informácie súvisiace s pripravovanými hybridnými útokmi na konkrétne kritické subjekty a oblasti.

3. SYSTÉM IDENTIFIKÁCIE A MINIMALIZÁCIE ŠÍRENIA HYBRIDNÝCH HROZIEB TAJNÝMI SLUŽBAMI V PODMIENKACH SLOVENSKEJ REPUBLIKY

Pre pochopenie stavu boja proti hybridným hrozbám je nutné uviesť niekoľko materiálov politického a odborného významu, ktoré boli prijaté za posledné roky. Patrí sem Koncepcia pre boj SR proti hybridným hrozbám, Bezpečnostná stratégia SR, Obranná stratégia SR, Akčný plán koordinácie boja proti hybridným hrozbám,⁵³ Koncepcia bezpečnostného systému SR a Koncepcia strategickej komunikácie. Všetky uvedené dokumenty reagujú na úniové záväzky SR v tejto oblasti a obsahujú taxatívne stanovené opatrenia na posilnenie postavenia subjektov podieľajúcich sa na posilnení kapacít štátu pre boj proti hybridným hrozbám.

Skôr než sa sústredíme na pertraktovanú problematiku, uvedieme a charakterizujeme postavenie niektorých subjektov v SR, ktoré sa zaoberajú identifikáciou a elimináciou hybridných hrozieb realizovaných nepriateľskými tajnými službami.

Primárnym subjektom je Bezpečnostná rada SR (*dalej len BR SR*),⁵⁴ ktorá má okrem iného zriadený výbor pre zahraničnú politiku, výbor pre kybernetickú bezpečnosť, výbor pre koordináciu spravodajských služieb a od mája 2023 aj výbor pre hybridné hrozby. Z hľadiska skúmaného vedeckého problému sa budeme zaoberať len výborom pre koordináciu spravodajských služieb a výborom pre hybridné hrozby.

Pri koordinácii plánovania opatrení na zabezpečenie činnosti spravodajských služieb sa výbor pre koordináciu spravodajských služieb podieľa na koordinácii činnosti spravodajských služieb, vypracováva stanoviská vzťahujúce sa na koordináciu spravodajských služieb, prerokúva návrhy predkladané BR SR v súvislosti s plnením úloh na úseku koordinácie spravodajských služieb. Ďalej posudzuje návrhy všeobecne záväzných právnych predpisov (*dalej len právne predpisy*), noriem vzťahujúcich sa na koordináciu spravodajských služieb, ktoré sú predložené na prerokovanie BR SR. Uvedený výbor je dôležitý z toho hľadiska, že v EÚ sa prostredníctvom špeciálnych inštitúcií, okrem iného, sústreďujú na kontrarozviednu činnosť smerujúcu k eliminácii hybridných hrozieb.

Výbor pre hybridné hrozby, pri koordinácii plánovania opatrení zameraných na zachovanie bezpečnosti a budovania odolnosti SR voči pôsobeniu hybridných hrozieb, vyhodnocuje bezpečnostnú situáciu v SR a vo svete v oblasti hybridných hrozieb s dôrazom na hodnotenie hybridného pôsobenia na odolnosť štátu a odolnosť spoločnosti. Pripravuje pre BR SR návrhy opatrení na zvýšenie odolnosti štátu a spoločnosti voči rizikám hybridného pôsobenia. Podieľa sa na formovaní politiky SR, ako aj na vypracúvaní koncepčných dokumentov v oblasti hybridných hrozieb a na koordinácii medzirezortnej a medzinárodnej spolupráce v oblasti hybridných hrozieb.

⁵³ NBÚ. 2022. Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf>.

⁵⁴ Čl. 8 Ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.

Predkladá BR SR návrhy opatrení na zvyšovanie celospoločenského povedomia o hybridných hrozbách a prerokúva návrhy predkladané BR SR, ktoré súvisia s plnením úloh v oblasti hybridných hrozieb. Vypracúva odborné stanoviská vzťahujúce sa na hybridné hrozby a predkladá ich BR SR. Posudzuje právne predpisy a medzinárodné zmluvy vzťahujúce sa na hybridné hrozby, ktoré sú predložené na prerokovanie BR SR.

Ďalším subjektom, ktorý v bezpečnostnom prostredí SR operuje v pozícii národného kontaktného miesta pre hybridné hrozby, je Situačné centrum SR.⁵⁵ Situačné centrum SR alias SITCEN je súčasťou Kancelárie BR SR (*d'alej len KBR*) a formálne existuje od januára 2016. Úlohou SITCEN-u, ako vládneho informačného analytického pracoviska s celoštátnou pôsobnosťou, je zabezpečovať nepretržitý tok informácií a koordináciu tohto toku medzi HFC a Slovenskom, a to oboma smermi. Okrem toho sa podieľa na monitorovaní, analýze a prognóze vývoja bezpečnostnej situácie a v prípade potreby, napr. krízovej situácie, má za úlohu kontaktovať relevantné orgány na Slovensku alebo v zahraničí. V tejto súvislosti treba podotknúť, že BR SR, často práve na základe informácií od SITCEN-u predkladá vláde návrhy opatrení na zníženie alebo odstránenie rizík ohrozenia bezpečnosti Slovenska, ktoré môžu viesť ku krízovej situácii. Je zrejmé, že podstatou činnosti tohto vládneho pracoviska je príprava výstupných analytických materiálov a ich predkladanie kompetentným adresátom decíznej sféry pre ďalšie využitie, napríklad pre voľbu strategických rozhodnutí v rámci smerovania bezpečnostnej politiky SR, príp. aj na operačno-taktickej úrovni.

Dôležitú funkciu na tomto úseku plní aj Národné bezpečnostné analytické centrum (*d'alej len NBAC*), zastávajúce úlohu národného kooperačného centra pre hybridné hrozby, ktorého poslaním je sústreďovať informácie o hybridných hrozbách na základe prijatých hlásení od orgánov štátnej správy, prípadne od iných subjektov (*fyzických a právnických osôb*) a následne ich vyhodnocovať a distribuovať určeným adresátom pre ďalšie využitie (*najčastejšie práve SITCEN-u*).⁵⁶ NBAC je definované ako analytické, komunikačné a kooperačné pracovisko Slovenskej informačnej služby (*d'alej len SIS*), s celoštátnou pôsobnosťou v oblasti bezpečnostných hrozieb. Napriek tomu, že centrum vzniklo v januári 2013 na základe projektu, ktorého iniciátorom a zároveň aj gestorom bola SIS, NBAC vo svojej podstate reprezentuje novú formu medzirezortnej organizačnej štruktúry. Na jeho platforme spolupracujú vyslaní zástupcovia SIS, Vojenského spravodajstva (*d'alej len VS*), Policajného zboru, Kriminálneho úradu finančnej správy, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, Generálneho štábu Ozbrojených síl SR a Úradu vlády SR. Medzi jeho hlavné úlohy patrí príprava komplexných analytických hodnotení bezpečnostných incidentov na základe hlásení prijatých od štátnych orgánov SR, monitorovanie bezpečnostnej situácie v SR z odkrytých zdrojov a poskytovanie analytických produktov o bezpečnostných hrozbách v SR určeným príjemcom. NBAC funguje ako analytické pracovisko založené na aktívnej participácii rozhodujúcich štátnych orgánov SR, ktoré pôsobia v bezpečnostnej oblasti. Ďalšie participujúce štátne subjekty poskytujú NBAC informačnú podporu formou hlásení o zaznamenaných bezpečnostných incidentoch. Informačné produkty spracované analytickým pracoviskom NBAC sú poskytované všetkým zúčastneným štátnym orgánom a inštitúciám a prípadne aj ďalším subjektom v zriaďovateľskej pôsobnosti štátnych orgánov za účelom rozhodovania a prijímania bezpečnostných opatrení.

⁵⁵ Uznesenie vlády Slovenskej republiky č. 486/2018 zo dňa 17. októbra 2018.

⁵⁶ Slovenská informačná služba. 2020. O nás: Národné bezpečnostné analytické centrum (NBAC). [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/o-nas/nbac.html>.

Z uvedeného je zrejmé, že SIS ako všeobecná bezpečnostná a spravodajská služba SR plní dôležitú funkciu na úseku boja proti hybridným hrozbám, napriek tomu, že v osobitnom právnom predpise, ktorý bližšie upravuje pôsobnosť, organizáciu a činnosť tejto informačnej služby nie je výslovná zmienka o plnení úloh na tomto úseku. Napriek tomu, z analogického výkladu ustanovení zákona reglementujúcich úlohy tejto spravodajskej služby možno vyvodiť záver, že všetky aspekty boja proti hybridným hrozbám spadajú do jej pôsobnosti (*činnosti ohrozujúcej ústavné zriadenie, územnú celistvosť a zvrchovanosť; činnosti smerujúcej proti bezpečnosti SR; aktivity cudzích spravodajských služieb; organizovaná trestná činnosť; terorizmus, vrátane informácií o účasti na terorizme, jeho financovaní alebo podporovaní; politický a náboženský extrémizmus a extrémizmus prejavujúci sa násilným spôsobom a škodlivé sektárske zoskupenie; aktivity a ohrozenia v kybernetickom priestore, ak ohrozujú bezpečnosť štátu; nelegálna medzinárodná preprava osôb a migrácia osôb; skutočnosti spôsobilé vážne ohroziť alebo poškodiť hospodárske záujmy SR; ohrozenie alebo únik informácií a vecí chránených podľa osobitného predpisu alebo medzinárodných zmlúv alebo medzinárodných protokolov*).⁵⁷ Plnenie zákonom stanovených úloh často sprevádza zásah do práv a slobôd občanov a súvisí s oprávnením SIS používať osobitné prostriedky, a to informačno-technické prostriedky v súlade so zákonom o ochrane pred odpočúvaním⁵⁸ a zákonom o SIS⁵⁹ aj informačno-operatívne prostriedky, kde možno zaradiť sledovanie osôb a vecí, legalizačné dokumenty a legendu, využívanie osôb konajúcich v prospech informačnej služby, zámenu vecí a predstieraný prevod vecí a iné oprávnenia (*napr. oprávnenie na nosenie a používanie strelnej zbrane; oprávnenie na používanie osobitných finančných prostriedkov a nakladania s majetkom štátu; oprávnenie držať nebezpečné látky a zakázané veci; oprávnenie požadovať poskytnutie pomoci, podkladov a informácií; oprávnenie poskytovať ochranu príslušníkov informačnej služby*). Je zrejmé, že na úseku identifikácie a minimalizácie hybridných hrozieb realizovaných nepriateľskými tajnými službami iných štátov bude v spravodajskej činnosti SIS prevládať používanie informátorov, legend a legalizačných dokumentov, ale aj nasadenie sledovania, či informačno-technických prostriedkov.

Zo správy o činnosti SIS za rok 2021 (*správa o činnosti SIS za rok 2022 a logicky aj za rok 2023 doteraz neboli oficiálne publikované*) vyplýva, že táto informačná služba v priebehu sledovaného obdobia zaznamenala zintenzívnenie hybridného pôsobenia zo strany Ruskej Federácie, a to v informačnej, spravodajskej, spoločenskej a kultúrnej sfére. Okrem toho, pokračovalo hybridné a vplyvové pôsobenie Číny na SR, aj keď viditeľnosť a intenzita informačných aktivít vo verejnom priestore sa v porovnaní s prechádzajúcim rokom znížila.⁶⁰ V kontexte medializovaných informácií, možno uviesť, že SIS na sklonku roka 2020 poskytla podklady na rozhodnutie o vyhostení trojice príslušníkov ruských spravodajských služieb, ktorí na území SR pôsobili pod diplomatickým krytím. Podľa neutajovanej správy SIS, boli v hodnotenom období aktivity týchto služieb na území SR čiastočne obmedzené, napriek tomu, že sa naďalej pokúšali získať prístup k predstaviteľom štátnej správy, členom vlády, poslancom parlamentu a iným osobnostiam s cieľom ovplyvňovať ich rozhodovanie. *Aj na základe týchto skutočností sa očakáva pokračujúci záujem týchto služieb o získavanie informácií z bezpečnostného prostredia (napr. Ozbrojených síl*

⁵⁷ § 2, ods. 1 zákona č. 46/1993 Z. z. o Slovenskej informačnej službe.

⁵⁸ § 2, ods. 2 zákona č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (*zákon o ochrane pred odpočúvaním*).

⁵⁹ § 10, ods. 1, písm. a) zákona č. 46/1993 Z. z. o Slovenskej informačnej službe.

⁶⁰ Slovenská informačná služba. 2021. Správa o činnosti Slovenskej informačnej služby 2021. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby>.

SR, Ministerstva obrany SR a NATO) so zameraním na poskytovanie pomoci Ukrajine. Okrem ruských špiónažných aktivít sa SIS venovala aj monitorovaniu pôsobenia spravodajských služieb Čínskej ľudovej republiky na území SR, osobitne vo vzťahu k témam súvisiacim s tzv. politikou jednej Číny (Taiwan, Tibet, Hongkong). V našom prostredí pretrvávali lobistické aktivity zamerané najmä na podporu prieniku čínskych spoločností do kritickej technologickkej infraštruktúry orgánov štátnej a verejnej správy SR a do prostredia akademických a vzdelávacích inštitúcií.⁶¹ Z uvedeného je zrejma dôležitá úloha, ktorú plní SIS na úseku identifikácie a minimalizácie hybridného pôsobenia realizovaného cudzími (nepriateľskými) spravodajskými službami.

V tomto ohľade si osobitnú pozornosť zasluhuje aj samotné VS, ktoré patrí medzi spravodajské služby legitímne operujúce v bezpečnostnom a obrannom prostredí SR. VS na účely planenia úloh, stanovených v zákone o VS, získava, sústreďuje a vyhodnocuje informácie dôležité na zabezpečenie obrany, obranyschopnosti a bezpečnosti SR na území SR a mimo územia SR, zamerané aj na hybridné hrozby a dezinformácie, ak ohrozujú obranu alebo obranyschopnosť SR.⁶² Náplňou práce tejto spravodajskej služby je, vo svojej podstate, realizácia spravodajskej činnosti, ktorú možno v zmysle predmetného zákona definovať, ako súhrn spravodajských, analytických a iných úkonov vykonávaných VS spravidla utajeným spôsobom vrátane zabezpečenia realizácie týchto úkonov a jej podpora, zameraných na získavanie informácií a vecí, a to aj používaním osobitných prostriedkov a využívaním osobitných oprávnení, sústreďovanie a vyhodnocovanie získaných informácií.⁶³ Skutočnosť, že pojem spravodajská činnosť má svoju oporu, explicitné vyjadrenie, vo všeobecne záväznom právnom predpise, možno hodnotiť jednoznačne pozitívne, aj vzhľadom na to, že donedávna (*t. j. do nadobudnutia účinnosti nového zákona o VS dňom 1. 2. 2023*) tomu tak nebolo. Aj týmto počínom sa štát otvorene hlási k tomu, že spravodajská činnosť je bezo sporu legitímnym nástrojom presadzovania práva a ochrany záujmov SR ako suverénneho, demokratického a právneho štátu. Uvedené uvádzame aj v širšom historickom kontexte, nakoľko vojenská spravodajská činnosť do roku 1992 na našom území fungovala v tzv. právnom vákuu. Zmenu právneho statusu realizátorov vojenskej spravodajskej činnosti priniesol až zákon č. 67/1992 Zb. o vojenskom obrannom spravodajstve a neskôr aj zákon č. 198/1994 Zb. o Vojenskom spravodajstve, ktorý zákonnou cestou vymedzil pôsobnosť, organizáciu, riadenie a kontrolu týchto spravodajských či špeciálnych služieb, ktoré oficiálne operovali v bezpečnostnom a obrannom prostredí nášho štátu, ale aj v zahraničí, sledujúc pritom oprávnené záujmy nášho štátu.

Aj podľa odborníkov, je pri realizácii spravodajskej činnosti potrebné rešpektovať určité odporúčané pravidlá a postupy, kde dôležitú úlohu zohráva princíp ústavnosti, zákonnosti a princíp pacta sunt servanda, ako aj zásady organizačno-technické a taktické (*zásada riadenia z jedného centra; zásada efektívnosti, primeranosti a vhodnosti použitia metód, foriem a prostriedkov; zásada vzájomnej kooperácie; zásada plánovitosti*) a zásady spravodajskej profesionality (*zásady aktuálnosti – objektívnosti a včasnosti; zásada spravodajskej intuície a erudície; zásada utajenia resp. konšpirácie; zásada nevyhnutnej znalosti – tzv. need to know*).⁶⁴ Práve týmto postupom je možné docieľiť úspešné a efektívne plnenie stanovených cieľov a úloh, ktoré sú v súlade s platným právnym rámcom. Už z podstaty veci vyplýva, že VS ako subjekt

⁶¹ Pravda. 2021. SIS poskytla podklady na vyhostenie troch ruských špiónov. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://spravy.pravda.sk/domace/clanok/631443-sis-poskytla-v-roku-2021-podklady-na-vyhostenie-troch-ruskych-spionov/>.

⁶² § 5 zákona č. 500/2022 Z. z. o Vojenskom spravodajstve.

⁶³ § 3, písm. a) zákona č. 500/2022 Z. z. o Vojenskom spravodajstve.

⁶⁴ STIERANKA, J. a kol. Spravodajská činnosť, s. 58 – 67.

spravodajskej činnosti môže pri výkone svojich právomocí a v rámci svojej pôsobnosti, v nevyhnutnej miere a na dosiahnutie sledovaného účelu, zasahovať do práv a slobôd občanov, pričom charakter a intenzita tohto zásahu je v podmienkach SR striktne regulovaná právom.⁶⁵ V tejto súvislosti platí, že kontrolu činnosti VS vykonáva parlament prostredníctvom tzv. osobitného kontrolného výboru na kontrolu činnosti VS (*pre doplnenie uvádzame, že aj pre účely kontroly činnosti SIS je v parlamente zriadený takýto osobitný kontrolný výbor*). Zároveň, riaditeľ VS, ktorý je za výkon svojej funkcie zodpovedný ministrovi obrany SR, predkladá výboru, minimálne raz ročne, podrobnú správu o činnosti VS, ako aj podklady potrebné na kontrolu čerpania limitu finančných prostriedkov VS z rozpočtu ministerstva a informáciu o vykonaní aktívnej obrany. Okrem toho, VS prostredníctvom ministra obrany, najmenej raz ročne, predkladá zákonodarnému orgánu stručnú správu o plnení úloh VS. Do pozície kontrolovaného objektu sa VS a SIS dostávajú aj z pohľadu právneho statusu orgánov štátnej správy⁶⁶ a zároveň sú tieto spravodajské služby v centre optiky monitoringu zákonnosti používania informačno-technických prostriedkov (*dalej len ITP*), kde bola pre tento účel (*v zmysle zákona o ochrane pred odpočúvaním*) zriadená osobitná komisia. Napr. zo správy o činnosti VS za rok 2021 vyplýva, že VS za príslušný kalendárny rok „... podalo celkom 44 žiadostí na použitie ITP, pričom k všetkým vydal zákonný sudca súhlas na ich použitie. VS tiež predložilo zákonnému sudcovi celkom 29 žiadostí na predĺženie doby použitia ITP v tom istom prípade a k všetkým 29 žiadostiam zákonný sudca vydal písomný súhlas na použitie ITP. Z realizovaných použití ITP v roku 2021 bolo z hľadiska dosiahnutia uznaného účelu a cieľa, na ktorý slúži, vyhodnotených 35 prípadov použitia ITP. Zákonom uznaný účel a cieľ bol dosiahnutý v 34 prípadoch použitia ITP. V jednom prípade nebol účel a cieľ použitia ITP dosiahnutý.“⁶⁷ Analogicky aj zo správy o činnosti SIS za rok 2021 vyplýva, že „... SIS v roku 2021 požiadala o realizovanie ITP v **484 prípadoch**, z toho súd neudelil súhlas ôsmim žiadostiam SIS. Napriek tomu, všetky prípady použitia ITP v roku 2021 boli podložené potrebným súhlasom sudcu a v žiadnom prípade nedošlo k nezákonnému použitiu ITP“.⁶⁸

Z doteraz uvedeného je zrejmé, že plnenie zákonom stanovených úloh, ktoré často sprevádza zásah do práv a slobôd občanov, súvisí s oprávnením VS používať osobitné prostriedky (*služobného psa, služobnú techniku, informačno-technické prostriedky, informačno-operatívne prostriedky – sledovanie osôb a vecí, legendu a krycie doklady, osoby konajúce v prospech VS, zámenu vecí a predstieraný prevod vecí*) a osobitné oprávnenia (*oprávnenie držať nebezpečné látky a zakázané veci, vykonávať technickú ochranu, osobitne nakladať s finančnými prostriedkami a majetkom štátu, používať osobitné spôsoby vykazovania údajov, vyžadovať poskytnutie pomoci, podkladov a informácií*). Z povahy vecí vyplýva, že pri identifikácii hybridných hrozieb v praxi dominuje u

⁶⁵ Napr. zákonom č. 500/2022 Z. z. o Vojenskom spravodajstve, zákonom č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (*zákon o ochrane pred odpočúvaním*), ale na VS sa vzťahujú aj ďalšie zákony, napr. zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (*zákon o slobode informácií*).

⁶⁶ Napr. v zmysle zákona č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov, zákona č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákona č. 39/1993 Z. z. o Najvyššom kontrolnom úrade SR v znení neskorších predpisov.

⁶⁷ Vojenské spravodajstvo. 2021. Správa o činnosti Vojenského spravodajstva 2021. [online]. [cit. 2023-7-3]. Dostupné na internete: https://vs.mosr.sk/sprava_o_cinnosti_vs_2021_svk.pdf, s. 26.

⁶⁸ Slovenská informačná služba. 2021. Správa o činnosti Slovenskej informačnej služby 2021. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby>.

VS, v rámci vymedzeného spektra osobitných aplikačných nástrojov (*metód, foriem a prostriedkov*) spravodajskej činnosti, práve používanie služobnej techniky a analogicky ako u SIS, aj používanie spolupracujúcich osôb, informačno-technických prostriedkov, sledovania osôb a vecí, ale aj legend a krycích dokladov. Uvedené aplikačné nástroje zlepšujú možnosti a schopnosti realizátorov spravodajskej činnosti efektívne a účelovo získavať informácie z rôznych informačných zdrojov, relevantných pre realizáciu identifikácie. Vzhľadom na to, že spravodajská činnosť má charakter poznávacieho resp. informačného procesu, aj pre potreby identifikácie hybridných hrozieb, možno tento proces čisto teoreticky rozčleniť do viacerých fáz spravodajského cyklu. Samotná etapizácia spravodajskej činnosti vychádza z poznania aplikačnej praxe a je objektivizovaná výsledkami aplikovaného výskumu, realizovaného nielen u nás, ale aj v zahraničí. V odbornej literatúre sa stretávame s rozčlenením spravodajského cyklu do cca 4 – 7 etáp, pričom pre účely tejto vedeckej štúdie postačuje, ak uvedieme, že základnými fázami tohto cyklu sú: *1. zadanie požiadavky a definovanie problému; 2. zber a získavanie informácií; 3. spracovanie informácií (triedenie, ukladanie, hodnotenie a analýza); 4. interpretácia spravodajskej informácie, 5. vyhodnotenie spravodajského cyklu.*⁶⁹

Aj z týchto čiastkových informácií možno nepriamo vydedukovať niekoľko záverov, ktoré nás nasmerujú k uvažovaniu o podstate tejto činnosti. V prvom rade, úlohou tejto spravodajskej služby, a to nielen vo vzťahu k hybridným hrozbám, je získavať, zhromažďovať, spracovať a distribuovať spravodajské informácie práve pre potreby rozhodovania konkrétnych príjemcov decíznej sféry, sledujúc pritom primárne bezpečnostné a obranné záujmy SR. V tomto ohľade, je to napr. BR SR, ktorá môže prostredníctvom ministra obrany SR ukladať úlohy pre VS a SIS v rozsahu ich pôsobnosti. Zároveň, aj najvyšší štátni predstavitelia (*prezidentka SR, premiér, predseda parlamentu, príslušní členovia vlády*) môžu takýmto spôsobom od týchto služieb žiadať spravodajské informácie, ktoré sú významné pre ich rozhodovanie a činnosť. Okrem toho, tieto služby môžu poskytovať spravodajské informácie aj iným subjektom, napr. v prípade VS ministromi obrany SR, náčelníkovi Generálneho štábu ozbrojených síl SR a v prípade oboch spravodajských služieb aj orgánom činným v trestnom konaní a iným orgánom verejnej moci. V zásade ide iba o také spravodajské informácie, ktoré sú významné pre ich rozhodovanie a činnosť, pričom pri zdieľaní takýchto informácií je potrebné rešpektovať základné zásady spravodajskej činnosti (*osobitne v tomto ohľade – zásadu utajenosti, ktorá chráni identitu informačného zdroja, realizátora spravodajskej činnosti a spôsob, t. j. metódy, prostriedky a formy získania informácií*). Napríklad, podľa správy o činnosti VS za rok 2021, „... VS spracovalo a poskytlo 862 spravodajských produktov oprávneným a zmluvným subjektom u nás a v zahraničí, z toho 265 spravodajských informácií a 597 výmenných spravodajských informácií pre partnerské spravodajské služby.“ V konkrétnych reáliách to značí, že VS reprezentuje informačnú službu (*resp. informačný, analytický, bezpečnostno-obranný servis*), ktorej náplňou práce je poskytovanie spravodajských informácií (*alias výstupného produktu spravodajskej činnosti*) oprávneným používateľom, ktorí ich potrebujú pre rozhodovací proces a následné prijímanie opatrení, sledujúc pritom legitímne záujmy spoločnosti a štátu.

Kvalita spravodajskej činnosti na úseku identifikácie hybridných hrozieb je v konečnom dôsledku ovplyvňovaná celým radom faktorov. Na jednej strane, tu zohráva kľúčovú úlohu existujúci rámec (*legislatívny, inštitucionálny, organizačno-riadiaci, personálny, logistický, technický, taktický a pod.*) a na druhej strane tu stoja informačné zdroje a možnosti/schopnosti realizátorov tejto

⁶⁹ STIERANKA, J. a kol. Spravodajská činnosť, s. 136.

činnosti vyťažiť z týchto informačných zdrojov maximum. Ako informačný zdroj (*v materiálnom, formálnom aj funkčnom zmysle – nosič informácií*) môže poslúžiť čokoľvek, čo znižuje úroveň entropie o danom probléme a posúva naše poznávacie limity od tzv. neznalosti k znalosti. V zahraničnej odbornej literatúre sa informačné zdroje, a v nadväznosti na tieto zdroje aj samotné spravodajstvo, často klasifikujú ako:

1. ľudské zdroje (*angl. Human Source Intelligence – HUMINT*),
2. technické zdroje (*angl. Measurement and Signature Intelligence – MASINT*), ktoré subsumujú rádiolokačné zdroje (*angl. Radio Location Intelligence – RADINT*) a akustické zdroje (*angl. Acoustic Intelligence – ASINT*),
3. obrazové zdroje (*angl. Imagery Intelligence – IMINT*),
4. signálne zdroje (*angl. Signal Intelligence – SIGINT*), ktoré subsumujú elektronické zdroje (*angl. Electronic Intelligence – ELINT*), komunikačné zdroje (*angl. Communication Intelligence – COMINT*), telemetrické zdroje (*angl. Foreign Instrumentation Signals Intelligence – FISINT*),
5. otvorené zdroje (*angl. Open Sources Intelligence – OSINT*).⁷⁰

Z uvedeného je zrejmé, že informačné zdroje determinujú charakter spravodajstva (*kladú špecifické požiadavky na možnosti a schopnosti realizátorov spravodajskej činnosti a zároveň aj na spôsoby ich zberu/získavania, fixovania a spracovávaní*). Okrem toho, potenciálne spektrum informačných zdrojov pri realizácii spravodajskej činnosti je skutočne široké, vrátane utajovaných aj neutajovaných zdrojov, pričom na úseku identifikácie hybridných hrozieb tajnými službami sa často využíva práve HUMINT, OSINT, IMINT a v poslednom období aj nový informačný zdroj – GEOINT (*geo-priestorové spravodajstvo*). Napríklad, posledné dve spomenuté spravodajstvá zohrávali dôležitú úlohu pri hodnotení migračnej krízy na bielorusko-poľskej hranici v lete 2021 alebo pri hodnotení bezpečnostnej situácie na ukrajinsko-ruskej hranici koncom roka 2021.⁷¹

Efektívny, ale nie jednoduchý spôsob odhalenia pripravovaných hybridných hrozieb sú včasné spravodajské prieniky do centrál spravodajských služieb protivníka, kde sa rodia a koordinujú nápady pre hybridné hrozby.⁷² Eliminácia hybridných hrozieb vykonávaných nepriateľskými spravodajskými službami sa riadi nasledujúcimi princípmi: princíp legality, princíp legitimacy, princíp spolupráce, princíp dodržiavania základných práv a slobôd osôb, princíp nepretržitosti, princíp utajenosti, princíp jednotnosti a princíp aplikácie špeciálnych foriem, metód a prostriedkov.

Neutralizácia hybridných hrozieb môže byť podporená vzdelávaním občanov k vlastenectvu a dodržiavaním právneho systému štátu a taktiež bezpečnostnými opatreniami smerujúcimi proti realizátorom hybridných útokov. V neposlednej rade je to skúmanie pohnútok a dôvodov osôb, ktoré sa podieľajú na hybridných útokoch z radov obyvateľstva. Skúsenosti z posledného obdobia nám signalizujú skutočnosť, že pohnútkou a dôvodom k realizácii hybridných útokov zo strany obyvateľov štátu sa stáva aktívna činnosť v radoch radikálnych skupín, nesprávna orientácia v politickej situácii a snaha získať výhodnejšie materiálne a finančné podmienky.

⁷⁰ STIERANKA, J. a kol. Spravodajská činnosť, s. 136.

⁷¹ Vojenské spravodajstvo. 2021. Správa o činnosti vojenského spravodajstva 2021. [online]. [cit. 2023-7-3]. Dostupné na internete: https://vs.mosr.sk/sprava_o_cinnosti_vs_2021_svk.pdf. s. 26.

⁷² PORADA, V. a kolektív. Bezpečnostní vědy, s.666.

Dôležité pre boj proti hybridným hrozbám bude dôsledné plnenie úloh spravodajských služieb na uvedenom úseku, doceňovanie spravodajských opatrení smerujúcich k identifikácii hybridných útokov alebo ich minimalizácii. Pri vykonávaní opatrení proti hybridným útokom bude dôležité realizovať ohlasovaciu povinnosť zo strany zamestnancov verejnej správy, navrhovať závery pre vlastnú prácu a previesť záznamy o formách a metódach hybridných útokov a využitých prostriedkov pri realizácii týchto útokov.

4. PRIESKUM VEREJNEJ MIENKY VO VZŤAHU K PERCEPCII PREJAVOV HYBRIDNÝCH HROZIEB V BEZPEČNOSTNOM PROSTREDÍ SLOVENSKEJ REPUBLIKY

Za účelom posúdenia charakteru a úrovne percepcie hybridných hrozieb na Slovensku, výskumný tím pod záštitou Akadémie Policajného zboru v Bratislave, ktorého členmi sú aj predkladatelia tejto vedeckej štúdie, realizoval prieskum verejnej mienky dotazníkovou technikou. Zber dát prebiehal od 17. 2. do 18. 5. 2023 elektronickou cestou. Výskumnú vzorku tvorilo 60 respondentov – pedagógov, pracovne alebo služobne zaradených na Akadémii Policajného zboru v Bratislave na pracovných pozíciách, ktoré vyžadujú ukončené vysokoškolské vzdelanie minimálne 2. stupňa, z toho 37 mužov a 23 žien.

Úlohou respondentov, okrem iného, bolo posúdiť stupeň závažnosti hybridných hrozieb vo vzťahu k ohrozeniu SR. Na margo hodnotenia stupňa závažnosti hybridnej hrozby – pôsobenie cudzej moci, kam možno bezo sporu zaradiť aj činnosť (*tajných*) spravodajských služieb iného štátu, 37 % opýtaných hodnotilo túto kategóriu hybridnej hrozby stupňom „závažné“ a 33 % opýtaných stupňom „vysoko závažné“. Iba 12 % opýtaných považuje túto hybridnú hrozbu za „stredne závažnú“ a rovnaký počet opýtaných za „menej závažnú“. Len 7 % respondentov nevníma tento prejav hybridnej hrozby za závažný takmer vôbec (*priradilo hodnotenie „nezávažná hybridná hrozba“*). Z uvedeného vyplýva záver, že drvivá väčšina opýtaných (93 % respondentov) považuje prejav hybridnej hrozby – pôsobenie cudzej moci za závažný (*v rôznej intenzite*) v kontexte ohrozenia záujmov SR. Keď si porovnáme jednotlivé hodnotené prejavy hybridných hrozieb, z výsledkov prieskumu vyplýva, že respondenti najčastejšie hodnotili stupňom „vysoko závažné“ hybridné hrozby, ktoré atakujú bezpečnostné a obranné záujmy SR, práve oblasť kybernetickej bezpečnosti (48 % respondentov) a oblasť energetickej a priemyselnej bezpečnosti (40 % respondentov). Uvedená skutočnosť pravdepodobne koreluje s registrovanými zmenami v bezpečnostnom prostredí, ktoré si vyžiadali nárast kybernetických útokov a hrozbu energetickej krízy v súvislosti so zneužívaním energetickej závislosti Európy na vybraných komoditách, do istej miery determinovaných aj negatívnym vývojom bezpečnostnej situácie na Ukrajine. Okrem hybridnej hrozby – pôsobenie cudzej moci, respondenti najčastejšie priradovali stupeň „závažné“ k hybridnej hrozbe v oblasti organizovaného zločinu a strategickej korupcie (42 % respondentov). V tejto súvislosti je potrebné uviesť, že problematika strategickej korupcie a organizovaného zločinu patrí k skutočne citlivým témam na Slovensku, ktorým je v informačnom aj reálnom priestore prikladaná patričná váha, dôkazom čoho je celý rad mediálne ostro sledovaných káuz. Aj z tohto uhla pohľadu možno fakt, že táto oblasť bola respondentmi takmer rovnako často hodnotená stupňom „závažné“ ako oblasť pôsobenia cudzej moci, vnímať ako relevantný prejav toho, že činnosť spravodajských či tajných služieb nie je fiktívnou hrozbou pre bezpečnostné a obranné záujmy SR. Pre doplnenie komplexného obrazu uvádzame, že hybridné hrozby vo sfére extrémizmu a vo sfére environmentálnej bezpečnosti boli v spektre hybridných hrozieb najčastejšie

hodnotené stupňom „*stredne závažné*“, napriek tomu, že ich frekvencia výskytu je mierne vyššia v porovnaní s hybridnou hrozbou – pôsobenie cudzej moci.

Na margo skúmanej premennej frekvencie realizácie hybridnej hrozby sme dospeli k nasledovným čiastkovým záverom. Najčastejšie (*nepretržite*) sú v bezpečnostnom prostredí realizované hrozby v oblasti kybernetickej bezpečnosti, poukázala na to až tretina opýtaných (32 % *respondentov*). Všetky ostatné prejavy sú registrované na úrovni „*často*“ resp. respondenti z pohľadu početnosti výskytu najčastejšie ohodnotili tieto hybridné hrozby, vrátane pôsobenia cudzej moci, týmto stupňom frekvencie ich realizácie. Do pozornosti však kladieme zistenie, že hybridná hrozba – pôsobenie cudzej moci sa podľa respondentov síce realizuje často (*vypovedá o tom fakt, že početnosť výskytu „často“ bola najčastejšie vybranou alternatívou v hodnotení respondentov – 32 % respondentov*), avšak, keď si tento prejav hybridnej hrozby porovnáme s ostatnými hodnotenými prejavmi hybridných hrozieb, je zrejmé, že pôsobenie cudzej moci je najmenej častým registrovaným prejavom v celom spektre hybridných hrozieb. Okrem toho, len 3 % opýtaných uviedlo, že hybridná hrozba – pôsobenie cudzej moci sa nerealizuje nikdy a len 22 % uviedlo, že sa realizujú veľmi zriedka. Zvyšní respondenti (75 % *respondentov*) uviedli, že sa táto hybridná hrozba realizuje často (32 % *respondentov*), veľmi často (28 % *respondentov*), alebo nepretržite (15 % *respondentov*). Summa summarum, pôsobenie cudzej moci, vrátane činnosti tajných spravodajských služieb, možno hodnotiť ako závažný a častý prejav hybridného pôsobenia konkrétnych subjektov v bezpečnostnom prostredí SR.

Na druhej strane, v prieskume sme sa zamerali aj na to, ako SR zvláda boj s jednotlivými prejavmi hybridných hrozieb. V tejto súvislosti musíme uviesť, že väčšina respondentov vo svojom hodnotení v rámci prezentovanej škály preferovala „*priemernú*“ úroveň zvládania prejavu hybridnej hrozby, tzn. že išlo o najčastejšie vybranú úroveň. Ani jeden respondent neoznačil vynikajúcu úroveň. Vo vzťahu k prejavu hybridnej hrozby – pôsobenie cudzej moci, až 23 % opýtaných uviedlo, že štát nezvláda túto hybridnú hrozbu, 27 % opýtaných uviedlo, že ju zvláda málo, 37 % opýtaných – že ju zvláda priemerne a 13 % – že ju zvláda dobre. Z uvedeného vyplýva, že zvládanie tejto hybridnej hrozby v podmienkach SR nie je na takej úrovni, ako by sme si želali, poukázala na to viac ako polovica respondentov. Dokonca, v kontexte ostatných prejavov hybridných hrozieb, pôsobenie cudzej moci je hodnotené ako najmenej zvládnutá oblasť boja proti hybridným hrozbám zo strany štátu. Uvedená skutočnosť koreluje aj so zistením, že hrozba pôsobenia cudzej moci býva v spoločnosti veľmi často podceňovaná na úkor iných hrozieb. Iba 5 % respondentov sa domnieva, že tu nie je žiadne takéto riziko, rovnaký počet respondentov hodnotilo toto riziko – stupňom nízke, až 28 % respondentov – stupňom stredné, 45 % respondentov – stupňom vysoké a 17 % respondentov – stupňom kritické. Je zrejmé, že respondenti vnímajú v bezpečnostnom prostredí SR existenciu skutočného rizika, ktoré vedie k bagatelizácii tejto hybridnej hrozby zo strany štátu. Možných vysvetlení tohto postoja je pravdepodobne niekoľko, avšak respondenti v tomto kontexte poukázali na vypuklý problém, akým je aj absencia jednotného postoja k tejto hrozbe naprieč celým politickým spektrom (*poukázalo na to až 42 % respondentov*) a zároveň upozornili na nejednoznačnosť postoja verejnosti k vnímaniu a existencii tejto hrozby (*túto alternatívu, ako vysoké riziko, najčastejšie označilo až 42 % respondentov*). Okrem toho, väčšina opýtaných vníma korene problému v zlyhaní systému detekcie aktivít cudzej moci. Pri hodnotení tohto aspektu, len 5 % respondentov v rámci škálovania označilo alternatívu – žiadne riziko, 3 % respondentov – nízke riziko, až 33 % respondentov – stredné riziko, 38 % respondentov – vysoké riziko a 20 % respondentov – kritické riziko.

Aj tieto skutočnosti oprávnené poukazujú na potrebu hľadania nových, inovatívnych, systémových, koncepčných a aj technických riešení, ktoré prispievajú k posilneniu spôsobilostí spravodajských zložiek štátu identifikovať a minimalizovať hybridné pôsobenie cudzích mocností realizované aj prostredníctvom rozvratnej činnosti tajných (*spravodajských*) služieb.

ZÁVER

Hybridné hrozby priamo vplyvajú na systém ochrany vnútornej bezpečnosti štátu. Cieľom je, rôznymi formami činnosti štátnych a neštátnych subjektov spravodajských služieb nevynímajúc, narušiť alebo zásadne ovplyvniť rozhodovacie procesy štátnych orgánov a inštitúcií, ktoré zabezpečujú základné funkcie štátu. Smerujú do takých životne dôležitých oblastí pre fungovanie štátu, ako je infraštruktúra, doprava, energetické siete, ochrana verejného poriadku, verejné zdravie, kybernetická bezpečnosť, či fungovanie finančných a platobných prostriedkov. Zásadným spôsobom môže ovplyvňovanie rozhodovania štátnych orgánov a inštitúcií, negatívne zasiahnuť do existencie spoločnosti, jednotlivca a štátu. Môže zároveň narušiť vzťahy medzi jednotlivcami, skupinami obyvateľstva a dôveru týchto subjektov na schopnosť štátu garantovať ich bezpečnosť. Následne môžu hybridné útoky oslabiť demokratické hodnoty, realizáciu práv a slobôd jednotlivcov a deštruktívne pôsobiť na štátny, politický a policajný systém štátu.

Uvedené skutočnosti sa v určitom zmysle stávajú výzvou pre bezpečnostné vedy. Hľadanie ukotvenia vedeckého problému, akým minimalizácia resp. eliminácia hybridných hrozieb štátnymi orgánmi a inštitúciami v systéme bezpečnostných vied bezo sporu je, dáva priestor pre vedecké bádanie a poznávanie samotného systému hybridných hrozieb. V tejto vedeckej štúdii, ktorú predkladáme ctenej odbornej verejnosti do konštruktívnej diskusie, sme si za cieľ stanovili – analýzu systému identifikácie a minimalizácie hybridných hrozieb s bližším zameraním na postavenie a funkciu spravodajských (*tajných*) služieb v tomto systéme. Zároveň sme sa zamerali aj na ďalší, nemenej dôležitý aspekt formulovaného vedeckého problému, a to analýzu systému realizácie (*šírenia*) hybridných hrozieb týmito službami. Aj týmito konštatáciami, podporenými a verifikovanými dátami získanými z realizovaného prieskumu, chceme zdôrazniť zložitost' a širokospektrálnosť tohto problému a na potrebu hľadania koncepčných, multidisciplinárnych, no predovšetkým systémových riešení.

Zdroje

1. *Annual progress reports on countering hybrid threats – JOIN(2017) 30 final*, 19. 7. 2017.
2. *Annual progress reports on countering hybrid threats – JOIN(2018) 14 final*, 13. 6. 2018.
3. *Annual progress reports on countering hybrid threats – SWD(2019) 200 final*, 29. 5. 2019.
4. *Annual progress reports on countering hybrid threats – SWD(2020) 153 final*, 24. 7. 2020.
5. *Annual progress reports on countering hybrid threats – SWD (2021) 729*, 22. 7. 2021.
6. *Annual progress reports on countering hybrid threats – SWD(2022) 308*, 16. 9. 2022.
7. *Council conclusions on CSDP – Consilium 8971/15*, 18. 5. 2015, *European Council meeting (25 and 26 June 2015) – Conclusions – EUCO 22/15*, 26. 6. 2015.
8. EEAS, 2023. *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.

9. *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats: Establishment and adoption of its Terms of Reference – 10027/19*, 8. 7. 2019.
10. CHURANĚ, M. a kol. 2000. *Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti*. Praha: LIBRI, 2000. s. 432. ISBN 80-7277-020-9.
11. Kódex postupov proti šíreniu dezinformácií bol prijatý v roku 2018 a revidovaný v roku 2022. In EURÓPSKA KOMISIA, 2018. *EU Code of Practice on Disinformation*. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://digital-strategy.ec.europa.eu/sk/library/2018-code-practice-disinformation> – L 95/1, 15. 4. 2010.
12. *Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách) – L 277/1*, 27. 10. 2022.
13. NBÚ. 2022. *Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024*. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNYPPLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf>.
14. *Odporúčanie Rady z 8. decembra 2022 o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry 2023/C 20/01 – C 20/1*, 20. 1. 2023.
15. *Oznámenie Komisie Európskemu parlamentu a Rade o piatej správe o pokroku pre vykonávaní Stratégie EÚ pre bezpečnostnú úniu – COM(2022) 745 final*.
16. *Oznámenie Komisie Európskemu parlamentu a Rade o tretej správe o pokroku v plnení Stratégie EÚ pre bezpečnostnú úniu – COM(2021) 799 final*.
17. *Oznámenie Komisie Európskemu parlamentu a Rade: Stratégia vnútornej bezpečnosti EÚ: päť krokov k bezpečnejšej Európe – COM(2010) 673 v konečnom znení*, 22. 11. 2010.
18. *Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – O stratégii EÚ pre bezpečnostnú úniu – COM(2020) 605 final*.
19. *Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Európsky program v oblasti bezpečnosti – COM(2015) 185 final*.
20. *Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov – Boj proti dezinformáciám na internete: európsky prístup – COM(2018) 236 final*, 26. 4. 2018.
21. PORADA, V. a kolektív. 2019. *Bezpečnostní vědy*. Plzeň: Aleš Čeněk, 2019, 784 s. ISBN 9788073807580.
22. Pravda. 2021. *SIS poskytla podklady na vyhostenie troch ruských špiónov*. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://spravy.pravda.sk/domace/clanok/631443-sis-poskytla-v-roku-2021-podklady-na-vyhostenie-troch-ruskych-spionov/>.
23. Rada EÚ. 2022. *Strategický kompas pre silnejšiu bezpečnosť a obranu EÚ v nasledujúcom desaťročí: Tlačová správa z 21. 3. 2022*. [online]. [cit. 2023-9-3]. Dostupné na internete: <https://www.consilium.europa.eu/sk/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>.
24. Slovenská informačná služba. 2020. *O nás: Národné bezpečnostné analytické centrum (NBAC)*. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/o-nas/nbac.html>.
25. Slovenská informačná služba. 2021. *Správa o činnosti Slovenskej informačnej služby 2021*. [online]. [cit. 2023-7-3]. Dostupné na internete: <https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby>.

26. *Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES – L 333, 27.12.2022, s.164.*
27. *Spoločné oznámenie Európskemu parlamentu a Rade – Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie – JOIN(2016) 18 final – 6. apríl 2016.*
28. *Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade – Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby – JOIN(2018) 16 final.*
29. STIERANKA, J. a kol. *Spravodajská činnosť*. Bratislava: Akadémia PZ v Bratislave, 2013. 216 s. ISBN 978-80-8054-549-9.
30. ŠKVRNDA, F. 2007. *Spravodajské služby a bezpečnosť sveta*. Bratislava: Ekonóm, 2007. 248 s. ISBN 978-80-225-2272-4.
31. *The Lanscape of Hybrid Threats: A conceptual Model (prostredie hybridných hrozieb: koncepčný model), JRC117280, vypracované na základe spolupráce medzi Spoločným výskumným centrom a Európskym centrom excelentnosti pre boj proti hybridným hrozbám.*
32. *Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.*
33. *Uznesenie vlády Slovenskej republiky č. 486/2018 zo dňa 17. októbra 2018.*
34. *Vojenské spravodajstvo. 2021. Správa o činnosti vojenského spravodajstva 2021. [online]. [cit. 2023-7-3]. Dostupné na internete: https://vs.mosr.sk/sprava_o_cinnosti_vs_2021_svk.pdf.*
35. *Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.*
36. *Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.*
37. *Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
38. *Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
39. *Zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
40. *Zákon č. 39/1993 Z. z. o Najvyššom kontrolnom úrade SR v znení neskorších predpisov.*
41. *Zákon č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov.*
42. *Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.*
43. *Zákon č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.*
44. *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy [online] : Projekt podporený z Európskeho sociálneho fondu. Operačný program Efektívna verejná správa. Prijímateľ MV SR. Kód projektu ITMS2014+: 314011CDW7.*

UKAZOVATEĽ POUŽÍVANÝ NA MERANIE HYBRIDNÝCH HROZIEB V JEDNOTLIVÝCH DOMÉNACH HYBRIDNÝCH HROZIEB, JEHO ZBER A VYHODNOCOVANIE V RÁMCI SLOVENSKEJ REPUBLIKY

pplk. Ing. Daniel Blaško, PhD., EMBA, Ing. Paed. IGIP.

Akadémia Policajného zboru v Bratislave, katedra verejnej správy a krízového manažmentu; Sklabinská 1, 835 17 Bratislava 35; daniel.blasko2@minv.sk; daniel.blasko@akademiapz.sk

Abstrakt: Príspevok rieši problematiku identifikácie ukazovateľov (indikátorov) hybridných hrozieb, ich zber a vyhodnocovanie v rámci Slovenskej republiky. Taktiež v danom príspevku budú uvedené niektoré príklady indikátorov hybridných hrozieb. Indikátor nám slúži na to, aby sme vedeli merať hybridné hrozby, to je prvá časť definície, tie domény sú široké, ako od školstva, od kultúry, vojenská doména – celá šírka spoločnosti. Indikátory nám pomáhajú zistiť v ktorej časti spoločnosti sa tie indikátory vyskytujú a umožňujú nám ukazovať to samotné hybridné pôsobenie.

Kľúčové slová: indikátory, hybridné hrozby, zber a vyhodnocovanie, verejná správa.

1. INDIKÁTORY HYBRIDNÝCH HROZIEB

Čo sa týka indikátorov hybridných hrozieb, chceme identifikovať hybridné pôsobenie a práve na základe týchto indikátorov sa to dá. To znamená, že pomocou indikátorov dokážeme identifikovať hybridné pôsobenie. Následne dokážeme hybridné pôsobenie analyzovať a vyhodnocovať. Samotné hybridné hrozby sú výsledkom nekonvenčných nástrojov a práve preto je náročné ich niekedy identifikovať. Jedná sa o súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny.⁷³ Hybridná hrozba je vlastne charakteristická simultánnym použitím viacerých nástrojov koordinovaným spôsobom s cieľom využiť zraniteľnosti (slabé miesta) protivníka a následne oslabiť jeho rozhodovacie procesy pri zachovaní určitého stupňa hodnoverného popretia. Strategickým cieľom týchto hrozieb je oslabenie dôvery verejnosti v demokratické inštitúcie, prehĺbenie nezdravej polarizácie na národnej a medzinárodnej úrovni, spochybnenie základných hodnôt demokratických spoločností, zisk geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných a ovplyvňovania demokratických rozhodovacích procesov.

1.1 Nebezpečnosť hybridných hrozieb

Hybridné hrozby sa v posledných rokoch stali jednou z najdôležitejších tém v oblasti bezpečnosti tak na Slovensku, ako aj na úrovni Európskej Únie či NATO. Dôvodom, prečo je tejto oblasti prikladaný čoraz väčší význam je zmena spôsobu presadzovania strategických záujmov zo strany nepriateľských aktérov a zvyšujúci sa dopad technológií na všetky oblasti spoločnosti. Vojny sa v 21. storočí už nevyhlasujú, nahrádza ich koordinované využívanie celej širokej palety nástrojov využívajúcich informačné pôsobenie, ekonomický vplyv, energetický nátlak či pôsobenie tajných služieb. Zároveň sa technológie stali neoddeliteľnou súčasťou života celej spoločnosti a s ich využitím dnes dokážu nepriateľskí aktéri pôsobiť kdekoľvek na svete a to tak, že môžu šíriť

⁷³ Európska komisia, Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, 2018, <https://eur-lex.europa.eu>

strategickú propagandu, ovplyvňujú volebné procesy, útočia na kritickú infraštruktúru, prenikajú do počítačových sietí a pod.. Paralelným použitím nátlakových a podvratných činností, konvenčných a nekonvenčných metód (napr. nepriateľská propaganda, podpora extrémizmu, využívanie národnostných alebo náboženských komunít nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru) môžu hybridní aktéri destabilizovať spoločnosť cieľových štátov a oslabiť ich tak, aby boli ľahšie ovplyvniteľné alebo v krajnom prípade aj menej odolné voči použitiu konvenčnej vojenskej sily.⁷⁴

Bezpečnostné prostredie vo svete aj v Európe sa za posledné roky zásadne zmenilo. Dopady celosvetovej pandémie COVID-19, rapidný rozvoj nových technológií ako je umelá inteligencia a digitalizácia, dôsledky klimatickej krízy na migráciu či potravinovú bezpečnosť, alebo ruská vojenská agresia voči Ukrajine, to sú len niektoré príklady nedávnych udalostí, ktoré zásadne zmenili svet v ktorom žijeme.

Všetky tieto udalosti, vyvolávajú otrasy a zmeny, ktoré sa dotýkajú všetkých aspektov života. Zároveň tieto zmeny v bezpečnostnom prostredí zásadným spôsobom ovplyvňujú schopnosť Slovenskej republiky zabezpečovať ochranu svojich životne dôležitých a strategických záujmov definovaných v Bezpečnostnej stratégii Slovenskej republiky¹. Slovenská republika nie je ostrov odtrhnutý od sveta a čelí rovnakým typom hrozieb ako aj iné členské štáty Európskej Únie a NATO.

V rámci realizácie opatrení zameraných na budovania odolnosti voči hybridným hrozbám pripravovalo a pripravuje Centrum boja proti hybridným hrozbám Inštitútu správnych a bezpečnostných analýz Ministerstva vnútra Slovenskej republiky (ďalej len „MVSR“) prvú národnú simuláciu krízových scenárov s prvkami hybridných hrozieb pre subjekty verejnej správy. Centrum boja proti hybridným hrozbám vykonáva vzdelávacie aktivity v oblasti hybridných hrozieb, monitoruje indikátory hybridných hrozieb, analyzuje zraniteľnosti štátnej správy, ako aj organizuje simulačné cvičenia.⁷⁵

1.2 Indikátory - ukazovatele

Indikátor nám slúži na to, aby sme vedeli merať hybridné hrozby. Domény sú, ako sme už opisovali vyššie širokého rozsahu, a to od školstva, od kultúry, vojenská doména, vlastne celá šírka spoločnosti. Indikátory nám pomáhajú zistiť v ktorej časti spoločnosti sa tie indikátory vyskytujú a umožňujú nám ukazovať to hybridné pôsobenie. Spomínali sme, že chceme identifikovať hybridné pôsobenie a práve na základe týchto indikátorov to dokážeme. Následne ich vieme analyzovať a vyhodnotiť. Musíme zachytávať tie indikátory v čase a dávať ich do nejakého kontextu, aby sme vedeli vyhodnotiť hybridné pôsobenie. Zjednodušene, slúžia na to, aby sme vedeli identifikovať prítomnosť hybridnej hrozby.⁷⁶

Čo sa týka Indikátorov definovaných v Koncepcii pre boj SR proti hybridným hrozbám, jedná sa, alebo môže ísť o Externý alebo interný politický nátlak na najvyšších predstaviteľov a štátne

⁷⁴ Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, <https://eur-lex.europa.eu/legal-content/TXT/SK/>

⁷⁵ Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BKO2016_LQ.pdf

⁷⁶ Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, str.2, <https://eur-lex.europa.eu/legal-content/SK/TXT>

inštitúcie; Ekonomický alebo energetický nátlak na rozšírenie politického nátlaku; Rozsiahle sabotáže proti kľúčovej infraštruktúre, ktorá je definovaná ako zariadenia, služby a informačné systémy životne dôležité pre obyvateľov a riadenie štátu, ktorých nefunkčnosť alebo zničenie môže ohroziť bezpečnostné záujmy štátu. Do kritickej infraštruktúry patria najmä objekty osobitnej dôležitosti, ďalšie dôležité objekty, vybrané informačné a komunikačné prostriedky, zariadenia na výrobu a zásobovanie vodou, elektrickou energiou, ropou a zemným plynom a ďalšie časti majetku štátu a podnikateľských právnických a fyzických osôb určené vládou SR alebo iným kompetentným orgánom štátnej správy, ktoré sú nevyhnutné na zvládnutie krízových situácií, ochranu obyvateľstva a majetku, na zaistenie minimálneho chodu ekonomiky a správy štátu, ako aj jeho vonkajšej a vnútornej bezpečnosti a ktoré treba špeciálne ochraňovať.; Kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu; Informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu; Ovpływňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely; taktiež hrozba použitia vojenskej sily; Pri hybridných hrozbách existuje istá variabilita a nemôžeme pri nich počítať s taxatívnym vyčerpávajúcim výpočtom, preto sú nasledujúce indikátory vypísane skôr príkladmo, ide o indikatívny výpočet. Tieto indikátory sa môžu meniť a môžu byť aj iné ako máme uvedené v texte v zozname.⁷⁷

Informačné operácie (mali ste možnosť ich identifikovať aj vy) – najznámejší prejav hybridnej hrozby, dezinformačné kampane, propaganda, môžu to byť rôzne aktivity, ktoré sú najviac rozšírené.

Externý alebo politický nátlak – u nás sa až tak nevyskytuje, príklad z praxe, príklady Krymu v roku 2014 k obsadeniu Krymu, tzv. malými zelenými mužikmi. Tí boli neoznačení, nebolo ich možné stotožniť s nijakou krajinou. Spôsobili nátlak, obsadili parlament, obsadzovali vojenské základne a tým vytvárali tlak tak, aby došlo k referendu. Dobrý učebnicový príklad – zároveň týmto bol zmenený spôsob vedenia vojny.

Ekonomický alebo energetický nátlak – aj na Slovensku o tom vieme hovoriť, manipulácia a zneužívanie dodávok zemného plynu. Slovenska republika mala odpojenú dodávku zemného plynu, takýto príklad bol aj v Bulharsku. Dodávka energetických komodít je zneužívaná štátnymi aktérmi na manipuláciu cieľového štátu, alebo viacerých štátov. Ide o ropu, pohonné hmoty, elektrickú energiu a podobne. Nesmieme zabudnúť spomenúť aj Vojenský konflikt na Ukrajine.

Kybernetické útoky – Estónsko v roku 2008, kde ruskí hackeri zaútočili na Estónsko, čo malo za následok výpadok internetu v rozsahu troch dní. Prestali fungovať informačné systémy v bankách, bankomaty, nemocnice, integrované dopravné systémy, doprava ako taká. Takéto útoky Môžu spôsobiť škody veľkého rozsahu. V prípade Slovenska sú to zatiaľ menšie útoky. Kybernetický útok je jedným z častých indikátorov hybridných hrozieb a určite bude v budúcnosti narastať na sile.

Aktivity cudzích spravodajských služieb – táto aktivita bola medializovaná na Slovensku – boli za to odsúdené aj osoby. Vojenský pridelenec ruskej ambasády podával na ulici 500 eur redaktorovi.

⁷⁷ Vid' napr. Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, <https://www.nato-pa.int/download-file?filename=sites/default/files>

V konečnom dôsledku redaktor sa rovná médiá. No my nie sme vyšetrovatelia, u nás na Slovensku na to slúži Vojenské spravodajstvo a Slovenská informačná služba.⁷⁸

Ovplyvňovanie etnických náboženských a kultúrnych menšín a ich manipulácia na politické účely – Slovensko došlo k medializácii. V rámci sveta, ako aj na Slovensku existujú čínske policajné stanice, ktoré sú zriadené nelegálne a vlastne tieto policajné stanice môžu ovplyvňovať čínsku menšinu v zahraničí. Ide o kontrolu a ovplyvňovanie. Predĺžené ruky Číny, ktorá sa navonok tvári že je zriadená za účelom pomoci pre svojich občanov v zahraničí, no v skutočnosti existuje 51 čínskych policajných staníc, kde jedna z nich sa údajne nachádza aj v hlavnom meste Slovenskej republiky v Bratislave.

Hrozby použitia vojenskej sily – u nás na Slovensku to nie je najhorúcejšia hrozba. Čo sa týka vojenskej agresie Ruskej federácie na Ukrajinu - pred vypuknutím invázie v roku 2021, to všetko mohlo byť brané ako nátlak, to znamená ako indikátor hybridnej hrozby. Situácia na juhu a východe Ukrajiny je varovaním, že ozbrojený konflikt v Európe nemusí mať iba podobu priameho vojenského stretu medzi štátmi, ale aj hybridného spôsobu vedenia bojových činností. Hybridná hrozba predstavuje súbor nátlakových a podvrtných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód a nástrojov, využívaných koordinovane na dosiahnutie konkrétnych politických cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Zahŕňať môžu ovplyvňujúce, centrálné riadené spravodajské a informačné pôsobenie, pôsobenie neštátnych aktérov, vrátane polovojenských skupín, či nasadenie ozbrojených síl štátneho aktéra bez označenia. Takéto hybridné aktivity sa môžu začať skôr než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené. Hybridné aktivity môžu byť zamerané aj na oslabovanie podpory verejnosti pre plnenie medzinárodných záväzkov, či ochromenie reakcie medzinárodného spoločenstva.

Indikátory, ktoré sú definované v Koncepcii pre boj Slovenskej republiky proti hybridným hrozbám, tieto uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu. Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie na Slovensku, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku či kampane. V rámci koncepcie z roku 2018, tam sú taktiež definované indikátory, ale sú tam definované aj rozsiahle sabotáže proti kľúčovej infraštruktúre – Nordstream – výbuch – išlo o sabotáž, Kachovská priehrada - kybernetické útoky na železnice, v nemocnici a na letiská. Čo sa týka sabotáží, nemusí ísť len o fyzické útoky, môže ísť aj o kybernetické útoky s cieľom ochromiť samotnú kritickú infraštruktúru. Aktualizácia týchto dokumentov je plánovaná. Toto prostredie sa veľmi rýchlo mení a päť rokov starý dokument už nedokáže komplexne reflektovať na túto problematiku a preto je potrebná a nutná aktualizácia. V rámci krízového managementu poznáme tri základné piliere. Prvým pilierom je plánovanie, ak poznáme riziká, hrozby, ktoré negatívne ovplyvňujú komfort života obyvateľstva, ako aj samotný život v štáte. Plánujeme rôzne metódy, postupy proti hybridným hrozbám. Druhým pilierom je organizácia. Tam sa organizujú rôzne

⁷⁸ Koncepcia pre boj SR proti hybridným hrozbám, schválená vládou SR dňa 11. júla 2018 uznesením č. 345/2018, <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668>

inštruktážno metodické zamestnania, odborné metodické zamestnania, výcviky na získanie teoretických, alebo praktických skúseností a znalostí, čo má za úlohu znižovať stresory človeka. Tretím pilierom je kontrolovanie. Ide o kontrolu plánovania a organizovania, či nie je potrebné dokumenty a samotné výcviky aktualizovať, meniť, alebo doplniť. Samozrejme niekde medzi tým je aj výcvik a príprava personálu na krízové riadenie.⁷⁹

1.3 Prístup NATO k hybridným hrozbám

Severoatlantická aliancia ako vojenská obranná organizácia, ktorej je Slovensko členom venuje pozornosť hybridným hrozbám a hybridnej vojne vo svojich dokumentoch, doktríne ale i pri budovaní odolnosti a pripravenosti členských krajín. Prístup NATO k problematike hybridných hrozieb je postavený na troch pilieroch: pripraviť, odradiť, brániť.⁸⁰ Od roku 2015 má NATO stratégiu pre svoju úlohu v boji proti hybridnej vojne. NATO zabezpečí, aby Aliancia a spojenci boli dostatočne pripravení čeliť hybridným útokom a to bez ohľadu na ich podobu. Bude odrádzať hybridné útoky na Alianciu a v prípade potreby bude brániť dotknutých spojencov. Aliancia podporuje úsilie spojencov o identifikáciu národných zraniteľností a posilnenie ich vlastnej odolnosti, ak o to samozrejme požiadajú. NATO slúži aj ako centrum odborných znalostí a poskytuje spojencom podporu v oblastiach, ako je civilná pripravenosť a reakcia na chemické, biologické, rádiologické a jadrové incidenty; ochrana kritickej infraštruktúry; strategická komunikácia; ochrana civilného obyvateľstva; kybernetická obrana; energetická bezpečnosť a boj proti terorizmu. Pri príprave na boj proti hybridným hrozbám zohráva významnú úlohu aj odborná príprava, cvičenia a vzdelávanie. Patrí sem nácvik rozhodovacích procesov a spoločných vojenských a nevojenských reakcií v spolupráci s inými aktérmi. Európske centrum výnimočnosti pre boj proti hybridným hrozbám so sídlom v Helsinkách vo Fínsku slúži ako centrum odborných znalostí a pomáha zúčastneným krajinám pri zlepšovaní ich civilno-vojenských spôsobilostí, odolnosti a pripravenosti na boj proti hybridným hrozbám. V októbri 2017 ho slávnostne otvoril generálny tajomník NATO Jens Stoltenberg spolu s vysokou predstaviteľkou Európskej únie pre zahraničné veci a bezpečnostnú politiku/podpredsedníčkou Európskej komisie Federicou Mogheriniovou. Centrum je iniciatívou fínskej vlády, ktorú podporuje 32 ďalších krajín, ako aj NATO a Európskej Únie.⁸¹

2. ZBER A VYHODNOCOVANIE INDIKÁTOROV HYBRIDNÝCH HROZIEB

Spomínali sme vyššie, že chceme identifikovať hybridné pôsobenie a práve na základe týchto indikátorov sa to dá, to znamená, že pomocou indikátorov dokážeme identifikovať hybridné pôsobenie, následne dokážeme hybridné pôsobenie analyzovať a vyhodnocovať. Centrum boja proti hybridným hrozbám vykonáva vzdelávacie aktivity v oblasti hybridných hrozieb, monitoruje indikátory hybridných hrozieb, analyzuje zraniteľnosti štátnej správy, ako aj organizuje simulačné cvičenia.

⁷⁹ Sun-c', Umenie vojny, resp. Galatík, V., Krásný, A., Zetocha, K. (eds.), Vojenská stratégia, 2008

⁸⁰ Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, <https://www.nato-pa.int/download-file?filename=sites/default/files/2018>

⁸¹ John F. Kennedy, Address before the American Newspaper Publishers Association, 1961,

2.1 Inštitucionálny rámec v oblasti vyhodnocovania indikátorov v rámci Slovenska

Začneme Ústredným orgánom štátnej správy s tým, že ak je zachytený nejaký indikátor hybridnej hrozby sú zodpovedný za monitorovanie a vyhodnocovanie incidentov vo svojej pôsobnosti vo vzťahu k hybridným hrozbám. V rámci Centra boja proti hybridným hrozbám a na Protiteroristickej centrále Národnej kriminálnej agentúry pracujú zamestnanci, ktorí sa danej problematike v širšom uhle venujú. Ústredný orgán štátnej správy má za úlohu vo svojej pôsobnosti informácie monitorovať a vyhodnocovať. Následne sa zistené informácie posúvajú na Národné bezpečnostné analytické centrum. Národné bezpečnostné analytické centrum ich zbiera, prijíma informácie a zaraďuje dané informácie do procesu vyhodnocovania. Centrum boja proti hybridným hrozbám a Protiteroristická centrála Národnej kriminálnej agentúry tomu dávajú ten kontext, že si vyžadujú informácie od iných Ústredných orgánov Štátnej správy a robia z tých informácií istú syntézu. Potom máme ďalší útvar a to Situačné centrum na Úrade vlády, Spravodajské a situačné centrum Európskej únie na Úrade vlády, ktoré prijíma informácie z Európskej Únie a to zbiera a komunikuje na Slovensku prostredníctvom Národného bezpečnostného analytického centra. Spravodajské a situačné centrum Európskej únie je kontaktným bodom. Syntéza sa deje na Národné bezpečnostné analytické centrum. Ide tu o obojstranný proces, tieto štruktúry na to reflektujú.⁸²

Ministerstvo vnútra Slovenskej republiky, ako garant ochrany ústavného zriadenia, vnútornej bezpečnosti, zdravia a životov občanov si už aj pred ruskou inváziou na Ukrajinu uvedomovalo možné dopady hybridných hrozieb na Slovensko. Preto MVSR spolu s partnermi, ako Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstvom obrany Slovenskej republiky a Úradom vlády Slovenskej republiky iniciovalo realizáciu série opatrení smerujúcich k posilneniu kapacít štátu, ale aj spoločnosti ako takej brániť sa a odolávať hybridným hrozbám. Vďaka národnému projektu, ktorý je realizovaný spolu s partnermi od roku 2022 vznikli špecializované útvary Centrum boja proti hybridným hrozbám MVSR – máme viac informácií, máme lepší prehľad o tom, čo sa deje v prostredí sociálnych sietí a internetu a vieme preto aj rýchlejšie reagovať na šírené dezinformácie. Aby Slovensko dokázalo lepšie a efektívnejšie komunikovať s občanmi, boli zvýšené personálne kapacity MVSR a Policajného zboru Slovenskej republiky v oblasti komunikácie. Nie je náhoda, že Útvary Policajného zboru a ich facebooková stránka je najúspešnejší komunikátor spomedzi všetkých slovenských štátnych orgánov. Ministerstvo vnútra Slovenskej republiky výrazne zvýšilo svoju aktivitu a prítomnosť na sociálnych sieťach, realizovali mnohé kampane pripomínajúce si demokratické tradície a hodnoty Slovenska.⁸³

2.2 Aktivity MVSR zamerané na budovanie odolnosti voči hybridným hrozbám

Ministerstvo vnútra Slovenskej republiky v rámci svojich aktivít zameraných na budovanie odolnosti voči hybridným hrozbám realizovalo okrem iných konkrétnych výstupov aj iné aktivity, ako:

⁸² Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN> Vojenská doktrína Ruskej federácie, 2014, <http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c>

⁸³ Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, <https://www.nato-pa.int/download-file?filename=sites/default/files/2018-04/2018%20>

Hĺbkovú analýzu zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám, verejná verzia by už mala byť k dispozícii na webstránke www.hybridnehrozby.sk;

Vytvorenie systému identifikovania a vyhodnocovania indikátorov hybridných hrozieb v rezorte MVSR;

Podporu rezortnej strategickej komunikácie;

Realizáciu prvej národnej simulácie komplexného scenára krízovej situácie s hybridnými hrozbami CHIMÉRA '23 – cvičenie pre verejnú správu;

Komplexnú právnu analýzu zákona o volebnej kampani s návrhmi legislatívnych zmien;

Odbornú a obsahovú spoluprácu na príprave akreditovaného vzdelávania pre pracovníkov verejnej správy a Polície Slovenskej republiky o hybridných hrozbách, ktorá je realizovaná našou alma mater Akadémiou Policajného zboru Slovenskej republiky v Bratislave;

Koncepciu budovania odolnosti SR voči hybridným hrozbám – aplikácia a rozpracovanie konkrétnych opatrení z hĺbkovej analýzy zraniteľnosti;

E-learning o hybridných hrozbách pre verejnú správu;

Spustenie webovej stránky www.hybridnehrozby.sk – portál obsahujúci všetky informácie, relevantné dokumenty, analýzy, výstupy k téme hybridných hrozieb;

Účelom nariadenia je vytvoriť systém zberu a zdieľania indikátorov hybridných hrozieb v rámci MV SR, ktoré budú slúžiť ako podklad pre analýzu a následné rozhodovanie Národného bezpečnostného analytického centra. Cieľom je teda vytvoriť systém včasného varovania; identifikovať potenciálne hybridné pôsobenie; pripraviť a uskutočniť adekvátnu reakciu orgánov štátnej správy prostredníctvom nastavených procesov. Adekvátnou reakciou môže byť strategická komunikácia, teda komunikovať s verejnosťou so Sekciou Verejnej Správy a podobne. Pri tvorbe daného nariadenia sa vychádza z Koncepcie pre boj Slovenskej republiky proti hybridným hrozbám; z Akčného plánu koordinácie boja proti hybridným hrozbám za rok 2022- 2024; z Plánu úloh MVSR; z Organizačného poriadku MVSR; z Národného projektu: „Zvyšovanie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“;

2.3 Navrhovaný inštitucionálny rámec definovaný v rámci MVSR

Protiteroristická centrála Národnej kriminálnej agentúry vykonáva zber dezinformácií a zbiera aj relevantné informácie k hybridným hrozbám. Odbor počítačovej kriminality Národná centrála osobitných druhov kriminality vykonáva zber dezinformácií a zbiera hlásenia so sociálnych sietí. Sekcia informatiky telekomunikácií bezpečnosti MVSR vykonáva zber kybernetických incidentov. Sekcia Krízového riadenia vykonáva zber hybridných hrozieb na kritickú infraštruktúru a krízové situácie. Sekcia Verejnej správy má pod dohľadom voľby, neziskové organizácie, výrobu a úpravu zbraní a streliva. Odbor komunikácie a prevencie Prezídia Policajného zboru vykonáva zber dezinformácií. Tlačový odbor Kancelárie MVSR vykonáva zber dezinformácií, šírenia poplašných správ, neautentické správania. Všetky tieto informácie sú odovzdávané pripravenými a vopred dohodnutými formulármi na Centrum boja proti hybridným hrozbám na Inštitút správnych a bezpečnostných analýz. Odtiaľ sú informácie posúvané na Protiteroristickú centrálu Národnej kriminálnej agentúry, ktorá ďalej posúva informácie na Národné bezpečnostné analytické centrum, ktoré to všetko spracováva a rieši. V rámci tohto nariadenia je definovaný manuálnym spôsobom, alebo automatizovane; nastupuje prvotné zasielanie: Útvar MVSR na určené útvary MVSR; Takým spôsobom, že informácie zasiela manuálne prostredníctvom formuláru, alebo sprístupní databázu; Analýzu a vyhodnotenie vykoná Útvar MVSR, Centrum boja proti hybridným hrozbám takým spôsobom, že vykoná analýzu a vyhodnotenie pripraví do stanoveného formátu na elektronické zaslanie, ktorý zašle Protiteroristickej centrále Národnej kriminálnej agentúry a Prezídiu

Policajného zboru; Ďalej to postupuje na Národné bezpečnostné analytické centrum priamo na Útvár MVSR, Protiteroristickej centrále Národnej kriminálnej agentúry a to spôsobom, že komunikuje stanoveným spôsobom s Národným bezpečnostným analytickým centrom.⁸⁴

3. PRÍKLADY INDIKÁTOROV HYBRIDNÝCH HROZIEB

Aby sme si vedeli predstaviť čo to vlastne indikátor hybridnej hrozby je, uvedieme pár príkladov čo dokreslí danú problematiku. Ak ide o individuálny výskyt, či sa jedná alebo nejedná o hybridnú hrozbu, nie je to len jedna izolovaná aktivita. Takže, predstavme si, že máme individuálny prelet dronom – môže to byť nejaké dieťa, ktoré dostalo dron na vianoce, či iný sviatok a počas toho, ako sa s ním hralo, preletel daný dron nad vojenskou základňou. My vieme, že už na používanie dronu potrebujeme povolenie, nie kvôli obsluhu dronu, ale aby sme vedeli v akej výške ho môžeme používať, aby sme nenarušili letovú prevádzku, a aby sme s dronom nevykonávali činnosti, ktoré sú v rozpore so zákonom. Avšak, v prípade ak nie je napojený daný dron na cudziu štátnu moc a nebolo jeho cieľom destabilizovať spoločnosť, len ťažko možno hovoriť o hybridnej hrozbe. Ak je takýto incident spojený s narušením ochrany utajovaných skutočností, teda ide o neoprávnený vstup, tak to môže byť, ak si to spojíme dokopy indikátor a môže to byť vyhodnotený ako indikátor hybridnej hrozby. Ale je potrebné to rozlišovať. Niečo je indikátor a niečo je hybridná hrozba. Indikátor je prvý krok na to, aby sme vedeli, či je tu hybridná hrozba. Je tu možnosť, že sa už niečo deje. Musíme si to dať do kontextu. V rámci koncepcie z roku 2018 musia byť splnené 3 indikátory v rámci širšej kampane. Ale už sa uvažuje o tom, či sa musí jednať o 3 indikátory, že možno by stačili len dva indikátory alebo jeden, ale musí to byť posúdené v rámci nejakej analytickej činnosti. Inštitucionálny rámec v oblasti vyhodnocovania indikátorov v rámci Slovenskej republiky tu sa musí riešiť o aký ekosystém, resp. architektúru sa jedná.⁸⁵

3.1 Modelový príklad postupu pri zistení indikátora deepfake video

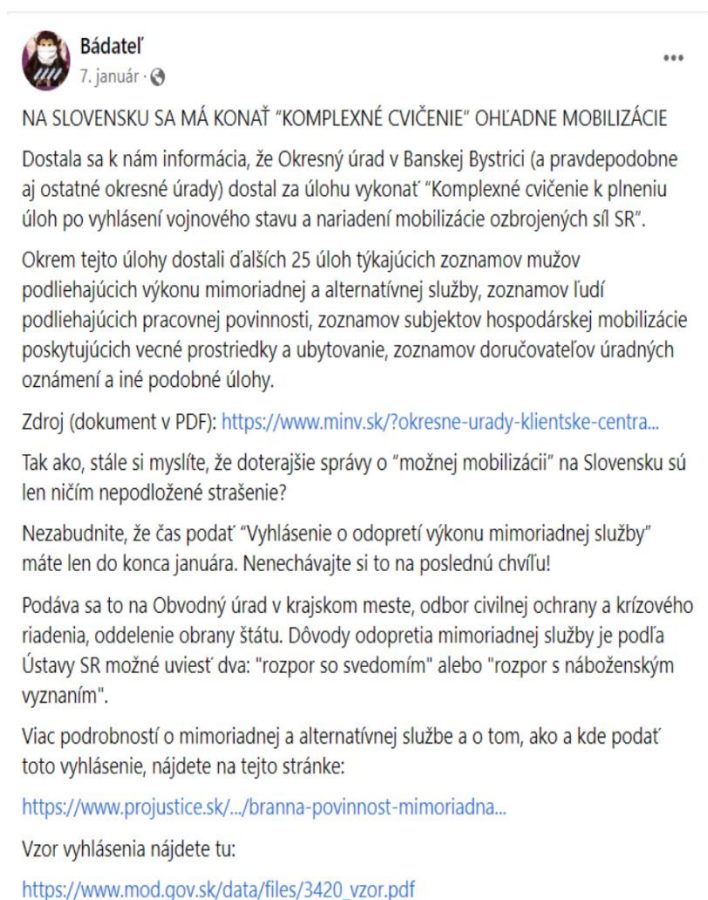
Ide o video „dipfejk video“. Je to označenie pre realistickú úpravu videa. Upravuje sa predovšetkým tvár zobrazovaných osôb, mimika tváre a reč jednotlivých aktérov videa. Jedinci potom vykonávajú činnosti, ktoré v skutočnosti nikdy nevykonávali a nevykonávajú, a hovoria slová, ktoré v skutočnosti nikdy nevyslovili. Tlačový odbor Kancelárie MVSR dostane podnet o šírení deepfake videa, nahlási tento indikátor Centru boja proti hybridným hrozbám MVSR prostredníctvom formulára. Centrum boja proti hybridným hrozbám zaznamená podnet, vyhodnotí ho a následne informuje Národné bezpečnostné analytické centrum. To poskytne dodatočné informácie od ostatných zapojených subjektov a posunie informáciu o indikátore a podklady na tlačový odbor Kancelárie MVSR. Tlačový odbor Kancelárie MVSR pripraví komunikačnú reakciu.

⁸⁴ Prítomnosť vojsk Ruskej federácie na východnej Ukrajine bola potvrdená vo viacerých oficiálnych dokumentoch prijatých na pôde EÚ, napr: Rozhodnutie Rady 2015/241 z 9. februára 2015, ktorým sa mení rozhodnutie 2014/145/SZBP o reštriktívnych opatreniach vzhľadom na konanie, ktorým sa narúša alebo ohrozuje územná celistvosť, zvrchovanosť a nezávislosť Ukrajiny, <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32015D0241&from=EN>

⁸⁵ Presný popis jednotiek ozbrojených síl Ruskej federácie, ktoré sa zapájali do bojov na východnej Ukrajine, je napríklad v analýze Igora Sutyagina z britského thinktanku RUSI (Royal United Services Institute) z roku 2015,

3.2 Modelový príklad indikátora hybridnej hrozby informačná operácia "mobilizácia"

Facebooková stránka „Bádateľ“ zverejnila na svojom profile príspevok v rámci ktorého vyvolávala obavy a strach u svojich fanúšikov prezentujúc skreslené a nezinterpretované informácie o „plánovanej mobilizácii“ na Slovensku. Samozrejme tieto informácie boli doplnené o výzvy na podávanie „Vyhlásenia o odopretí výkonu mimoriadnej služby“, o vzory tlačív a inštrukcie k postupu, prezentované expresívnym slovníkom, ktorý mal pôsobiť hrozivo a vyvolávať u užívateľov akútny strach. Príspevok dosahoval vysoký počet zdieľaní, komentárov a rôznych reakcií. Cieľom uvedeného príspevku bolo vyvolanie paniky z možného priameho zapojenia Slovenskej republiky do vojnového konfliktu Ruskej federácie a Ukrajiny, ale aj vyvolanie informačného chaosu a nedôvery k bezpečnostným zložkám Slovenskej republiky. Zároveň došlo k distribúcii falošných povolávacích rozkazov v rámci Slovenska a k úniku neutajovaných dokumentov Okresných úradov o plánovanom každoročnom cvičení k mobilizácii.



Obrázok č. 1 Dokument Facebooková stránka „Bádateľ“

Keďže uvedená informačná operácia mohla mať dosah na bezpečnosť Slovenskej republiky, bola informácia o šírení uvedeného naratívu prostredníctvom sociálnych sietí, riešená aj v rámci kompetencií Národného bezpečnostného analytického centra. Na základe zistených skutočností boli vypracované odporúčania na jednotnú komunikáciu uvedenej situácie rezortmi na poukázanie na prebiehajúcu informačnú operáciu, ktorá spočíva v šírení naratívov o chystanej mobilizácii,

cieľom týchto hybridných aktivít je znížiť podporu verejnosti v otázke vojenskej a materiálnej pomoci Ukrajine. Mobilizačné cvičenia prebiehajú periodicky a to každý rok. Ich cieľom je overiť pripravenosť jednotlivých zložiek Ozbrojených síl Slovenskej republiky. Vplyvom uvedenej informačnej operácie stúpol počet podaných žiadostí o odopretie mimoriadnej vojenskej služby oproti predchádzajúcemu roku skoro 30 násobne, t.j. vyše 40 tisíc žiadostí.

3.3 Modelový príklad indikátora hybridnej hrozby „Informačná operácia Ruskej federácie na Slovensku "cintorín Ladomirová"

Veľvyslanectvo Ruskej federácie na Slovensku zverejnilo na svojej facebookovej stránke informáciu o zničení cintorína z čias prvej svetovej vojny v obci Ladomirová okres Svidník. Veľvyslanectvo dôrazne odsúdilo tento rúhavý čin, vyzvalo Slovenskú republiku k dôslednému dodržiavaniu medzivládnej dohody z roku 1995 o hroboch padlých vojakov a civilných obetí vojny a v tomto zmysle zaslalo aj informáciu Ministerstvu zahraničných vecí a európskych záležitostí SR. Informácia sa ihneď začala šíriť sociálnymi sieťami. Starosta Ladomirovej bol obviňovaný zo strany komentujúcich z neúcty k obetiam vojny, k slovanstvu a k pamiatke Ľudovíta Štúra, z barbarstva, bol vyzývaný k náprave. Slovensko sa malo ospravedlniť Ruskej federácii. V súvislosti so statusom veľvyslanectva začal dostávať starosta Ladomirovej výhražné správy od verejnosti, v niektorých boli vyhrážky smrťou. Uvedený hoax, ktorý na Slovensku vytvoril oficiálny predstaviteľ Ruskej federácie, preberali aj ruské médiá.⁸⁶



Obrázok č. 2 Dokument „Posolstvo Ruska na Slovensku“

⁸⁶ Ценность науки в предвидении. Новые вызовы требуют п Russian Forces in Ukraine, https://rusi.org/sites/default/files/201503_bp_russian_forces_in_ukraine.pdf осмыслить формы и способы ведения боевых действий Promyšlenno-Vojennyj Kurier, 23.2.2013, <https://www.vpk-news.ru/articles/14632>, англійський переклад článku Valerija Gerasimova "Hodnota vedy je v predvídaní - Nové požiadavky si vyžadujú prehodnotenie foriem a spôsobov vykonávania bojových operácií", https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

Odbor komunikácie a prevencie Prezídia Policajného zboru sa skontaktoval so starostom, ktorý uviedol, že cintorín nebol poškodený, boli z neho len odstránené časti betónu, ktoré sa rozpadávali a spôsobovali ťažkosti pri starostlivosti o cintorín. Obec sa o cintorín príkladne roky stará, nedotkla sa pozostatkov tiel a nezasahovala ani do hrobov. Obec chce uvedené pietne miesto skrášliť. Uvedené plány chceli konzultovať aj s veľvyslancom Ruskej federácie, ten ich však odignoroval. O celej vzniknutej situácii boli informované participujúce bezpečnostné zložky a orgány štátnej správy, do ktorých vecnej pôsobnosti patrí boj proti hybridným hrozbám, ako Úrad vlády Slovenskej republiky, Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky, Centrum boja proti hybridným hrozbám MVSR a iné. Overovaním zverejnených informácií bolo zistené, že sa jedná o dezinformáciu. V tomto kontexte pripravili špecializované útvary odporúčania na jednotnú komunikáciu uvedenej situácie. Cieľom dezinformačného príspevku Veľvyslanectva Ruskej federácie na Slovensku bolo vyvolanie senzácie a prehlušenie informačného priestoru na úkor nových správ z Ukrajiny svedčiacich o možných vojnových zločinoch zo strany armády Ruskej federácie.⁸⁷

ZÁVER

Uviedli sme, že chceme identifikovať hybridné pôsobenie a práve na základe indikátorov to dokážeme. Následne hybridné pôsobenie vieme analyzovať a vyhodnotiť. Musíme zachytávať tie indikátory v čase a dávať ich do nejakého kontextu aby sme vedeli vyhodnotiť hybridné pôsobenie. Zjednodušene slúžia na to aby sme vedeli identifikovať prítomnosť hybridnej hrozby.

Ako postupovať pri podozrení na indikátor hybridných hrozieb?

- Zašlite podnet na emailovú adresu hybrid@minv.sk;
- Popíšte stručne situáciu;
- Priložte fotografie, screenshoty , URL linky;
- Môže sa jednať o informácie zo sociálnych sietí, webov alebo akýchkoľvek zdrojov aj v tlačenej podobe atď.
- Viac informácií nájdete na www.hybridnehrozby.sk

Zdroje

1. Európska komisia, Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, 2018, <https://eur-lex.europa.eu>
2. Európska komisia, Spoločný rámec pre boj proti hybridným hrozbám, 2016, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>

⁸⁷ Za pôvodcu tohto pojmu sa považuje popredný bezpečnostný analytik zaoberajúci sa Ruskom, pôsobiaci v Institute of International Relations, Mark Galeotti, ktorý ako prvý použil názov Gerasimova doktrína vo svojom blogu z roku 2014, "Gerasimova doktrína a ruská nelineárna vojna", <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>. V marci 2018 uverejnil vo Foreign Policy článok, v ktorom žiada o nepoužívanie termínu "Gerasimova doktrína", pretože je podľa neho nepresný a zavádzajúci. Zároveň v ňom však konštatuje, že "je nepochybné, že Západ čelí rozsiahlej, mnohostrannej, rozvracajúcej a rozdeľujúcej kampani využívajúcej skryté politické, aktívne opatrenia zo strany Ruska, <https://foreignpolicy.com/2018/03/05/imsorry-for-creating-the-gerasimov-doctrine/>

3. Ministerstvo obrany Slovenskej republiky, Biela kniha o obrane Slovenskej republiky, 28. september 2016, http://www.mod.gov.sk/data/BKO2016_LQ.pdf
4. Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, <https://www.nato-pa.int/download-file?filename=sites/default/files>
5. Koncepcia pre boj SR proti hybridným hrozbám, schválená vládou SR dňa 11. júla 2018 uznesením č. 345/2018, <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668>
6. Sun-c', Umenie vojny, resp. Galatík, V., Krásný, A., Zetocha, K. (eds.), Vojenská stratégia, 2008
7. Parlamentné zhromaždenie NATO, Výbor pre obranu a bezpečnosť, Countering Russia's Hybrid Threats: An update, Draft Special Report, 2018, <https://www.nato-pa.int/download-file?filename=sites/default/files/2018>
8. John F. Kennedy, Address before the American Newspaper Publishers Association, 1961,
9. Vojenská doktrína Ruskej federácie, 2014, <http://www.mid.ru/documents/10180/822714/41d527556bec8deb3530.pdf/d899528d-4f07-4145-b565-1f9ac290906c>
10. <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32015D0241&from=EN>
11. Ценность науки в предвидении. Новые вызовы требуют п Russian Forces in Ukraine, https://rusi.org/sites/default/files/201503_bp_russian_forces_in_ukraine.pdf переосмыслить формы и способы ведения боевых действий Promыshlenno-Vojennyj Kurier, 23.2.2013, <https://www.vpk-news.ru/articles/14632>, anglický preklad článku Valerija Gerasimova "Hodnota vedy je v predvídaní - Nové požiadavky si vyžadujú prehodnotenie foriem a spôsobov vykonávania bojových operácií", https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf
12. <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war>
13. <https://foreignpolicy.com/2018/03/05/imsorry-for-creating-the-gerasimov-doctrine/>
14. Vláda SR, Bezpečnostná stratégia Slovenskej republiky, 2017, <https://rokovania.gov.sk/RVL/Material/22364/1>
15. <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668>
16. Európsky parlament, Rada EÚ, Smernica 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, 2016, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L1148&from=EN>
17. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý nadobudol účinnosť 1. apríla 2018
18. Európsky parlament, Rada EÚ, Nariadenie 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), 2016, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
19. The Council of the European Union, Network and Information Security: Proposal for a European Policy Approach, 2001, <http://ec.europa.eu/transparency/regdoc/index.cfm?fuseaction=list&coteId=1&year=2001&number=298&language=EN>

20. Komisia Európskych spoločností, Stratégia pre bezpečnú informačnú spoločnosť – „Dialóg, partnerstvo a aktívne pôsobenie“, 2006, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52006DC0251&from=en>
21. Koncepcia boja proti extrémizmu na roky 2015 – 2019, 2015, https://www.minv.sk/swift_data/source/policia/naka_opr/nptj/koncepcia%20extremizmus%202015-2019.pdf
22. Národný akčný plán boja proti terorizmu na roky 2015 – 2018, 2015, https://www.minv.sk/swift_data/source/policia/naka_opr/nptj/NAP%20terorizmus%202015-2018.pdf
23. Zákon č. 180/2014 Z. z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov, <http://www.zakonypreludi.sk/zz/2014-180>
24. Zákon č. 181/2014 Z. z. o volebnej kampani a o zmene a doplnení zákona č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov

CHARAKTERISTIKA STRATEGICKEJ KORUPCIE VO VEREJNEJ SPRÁVE

PhDr. JUDr. Ondrej Blažek, PhD.

Katedra správneho práva, Akadémia Policajného zboru v Bratislave; Sklabinská 1, 835 17 Bratislava; ondrej.blazek@akademiapz.sk; ondrej.blazek2@minv.sk

Abstrakt: Príspevok sa zaoberá problematikou strategickej korupcie vo verejnej správe, ktorá je vnímaná ako jedna nevojenských činností, pre ktorú je charakteristická snaha páchatel'a o poškodenie záujmov Slovenskej republiky a presadenie svojich záujmov, pri dosahovaní svojich medzinárodnopolitických cieľov. Autor sa v príspevku zaoberá charakteristikou strategickej korupcie, hybridných hrozieb a postupom páchatel'ov pri presadzovaní záujmov poškodzujúcich Slovenskú republiku.

Kľúčové slová: hybridné hrozby, strategická korupcia, verejná správa, korupcia, hrozba, ohrozenie.

1. CHARAKTERISTIKA HYBRIDNÝCH HROZIEB V KONTEXTE RIEŠENEJ PROBLEMATIKY

Strategická korupcia je zaraďovaná do tematických oblasti skúmania hybridných hrozieb, nakoľko ide o jednu z foriem hybridných hrozieb.⁸⁸ Hrozba je v zmysle krátkeho slovníka slovenského jazyka chápaná ako *blizkosť niečoho nebezpečného*. Už z tohto jazykovedného významu je možné odvodiť, že pojmy hrozba a nebezpečenstvo sú vzájomne úzko prepojené, ale nie totožné. Hrozba je priblížené nebezpečenstvo v takej miere, že ho možno považovať za prebiehajúce (už skôr aktivované), pričom nebezpečenstvo je latentnou vlastnosťou objektu, spôsobiť neočakávaný negatívny jav. Ide o skrytú vlastnosť systému spôsobiť škodu. Lingvistický obsah pojmu hrozba je do značnej miery podobný s doktrínalnym obsahom pojmu hrozba, kde je hrozba chápaná ako aktivované nebezpečenstvo, pričom k jej aktivácii mohlo dôjsť „*pôsobením objektívnych a subjektívnych determinujúcich faktorov, rôznymi spôsobom a v rôznych podmienkach*“.⁸⁹ Síce autori v oblasti teórie bezpečnostných rizík (napríklad Buzalka) venujúci sa výkladu tohto pojmu, uprednostňujú namiesto pojmu „*hrozba*“ skôr pojem „*ohrozenie*“⁹⁰, môžeme považovať poznatky, ktoré máme o pojme ohrozenie, aj za poznatky, ktoré sa vzťahujú na pojem hrozba.⁹¹ Hrozba je chápaná ako nezávisle existujúci vonkajší fenomén, ktorý poškodzuje určitú hodnotu, pričom jej závažnosť je úmerná tomu, akú povahu má táto hodnota z hľadiska nášho subjektívneho vnímania. Hrozby, ktoré sú riešené v kontexte problematiky tzv. *hybridných hrozieb* považujeme za jednoznačne intencionálne hrozby. Strategická korupcia je bezpečnostnou hrozbou, nakoľko ohrozuje mieru bezpečnosti štátu a je schopná znížiť alebo eliminovať mieru bezpečnosti štátu. Vieme s istotou tvrdiť, že korupcia, vrátane tej strategickej korupcie je hrozba, kde zdroj ohrozenia (nebezpečenstvo) je sociogénneho charakteru a patrí medzi riziká verejnej správy.⁹² Hybridnú

⁸⁸ Pozri bližšie: LISON, M., FIDLER, L. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In: Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave Roč. 30 č. 2. s. 38-53.

⁸⁹ BUZALKA, J. *Teória bezpečnostných rizík*. Bratislava : Akadémia Policajného zboru v Bratislave, 2012. s. 25.

⁹⁰ Ohrozenie je tradičný pojem vo vojenskom prostredí.

⁹¹ Dôvod spočíva v preklade anglického výrazu „threat“. Pozri viac: BUZALKA, J. *Teória bezpečnostných rizík*. Bratislava : Akadémia Policajného zboru v Bratislave, 2012. s. 28.

⁹² Na základe zaradenia korupcie medzi hrozby. Pozri viac: BUZALKA, J. *Teória bezpečnostných rizík*. Bratislava: Akadémia Policajného zboru v Bratislave, 2012. s. 49.

hrozbu a jej definovanie nemožno realizovať bez predchádzajúceho definovania hybridnej vojny a hybridného konfliktu. „Hybridný konflikt a hybridná vojna sú dve špecifické kategórie, ktoré slúžia štátu na to, aby prostredníctvom niektorých foriem hybridnej taktiky dosiahol strategické ciele.“⁹³ Hybridná vojna teda využíva kombináciu jednotlivých nástrojov, ktorých použitím sa dosahujú čiastkové ciele vychádzajúce z hlavného cieľa nepriateľa.⁹⁴ Tieto čiastkové ciele sú vnímané nepriateľom ako nebezpečenstvo, ktoré po aktivácií predstavuje hrozbu. Čiastkovým cieľom hybridnej taktiky môže byť napríklad podplatenie konkrétneho zamestnanca vo verejnej správe, ktorý v prípade úspechu ďalšieho čiastkového cieľa hybridnej taktiky (napríklad kybernetického útoku) bude zámerne vytvárať nevhodné podmienky pre vyšetovanie tohto kybernetického útoku. Problémom Slovenskej republiky a ďalších štátov ako subjektov, ktoré sa bránia hybridným hrozbám je skutočnosť, že **nepoznajú presný hlavný cieľ nepriateľského štátu**, pričom sa k poznaniu presného cieľa len približujú jeho predikciou za pomoci rôznych vedeckých metód. Čiastkové ciele jednotlivých foriem hybridnej taktiky, ktoré v našom ponímaní chápeme ako hybridné hrozby sú taktiež **dopredu nespresnené** a možno ich len predikovať. Výsledok je taký, že pri boji proti hybridným hrozbám nie je so 100% istotou známe, čo je zamýšľaným koncovým cieľom nepriateľa a tak len odhadujeme, že ide **pravdepodobne** o rozšírenie vplyvu svojej moci z hľadiska teritoriálneho, ekonomického, politického, sociologického alebo iného pôsobenia. Problémom nepoznania hlavného cieľa je aj možnosť neustálej zmeny hlavného cieľa a prispôbovania hlavného cieľa aktuálnej situácií, bez toho, aby ten, kto bojuje proti naplneniu tohto cieľa o danej zmene vedel. Ciele v hybridnej vojne teda podľa nášho názoru podliehajú zmenám. Hybridné hrozby celkom presne vystihuje ich opis, že ide o „*intencionálnu činnosť, ktorej funkčnosť je vyjadrená v jej výstupoch. Je to prostriedok, ktorým jej aktéri môžu zvýšiť úroveň svojich možností a schopností pri dosahovaní stanovených cieľov.*“⁹⁵ Tým, že presne nepoznáme zámery a cieľ nepriateľa a nepoznáme ani presný čiastkový cieľ použitia niektorých foriem hybridnej taktiky, musí byť boj proti hybridným hrozbám realizovaný uvažene a musí byť braná na zreteľ skutočnosť, že **neadekvátna reakcia proti niektorým formám hybridnej taktiky môže napomôcť dosiahnutiu cieľa tej samotnej hybridnej taktiky (proti ktorej sa bojuje) alebo môže napomôcť k dosiahnutiu cieľa ďalšej hybridnej taktiky.** Dôležitou skutočnosťou je aj to, že pri boji proti hybridným hrozbám musíme zachovávať aj princípy právneho štátu a štátne orgány pri výkone svojej činnosti v boji proti hybridným hrozbám musia rešpektovať čl. 2 ods. 2 Ústavy Slovenskej republiky, ktorý znie, že: „*Štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.*“⁹⁶ Nerešpektovanie tohto ustanovenia naopak môže napomáhať dosiahnutiu cieľa a čiastkového cieľa, ktorý si nepriateľ stanovil.⁹⁷ Samotný pojem „*hybridné hrozby*“ je predmetom mnohých

⁹³ HULLOVÁ, M. *Indikátory hybridných hrozieb – nástroj ich identifikácie a eliminácie.* In. Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave, Roč. 31 č. 2. s. 5-26.

⁹⁴ Nepriateľ je v kontexte tohto príspevku štátny aktér, ktorý využíva hybridnú taktiku na dosiahnutie strategického cieľa.

⁹⁵ LIŠŇ, M., FIDLER, L. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb.* In. Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave Roč. 30 č. 2. s. 38-53.

⁹⁶ Čl. 2 ods. 2 Ústavy Slovenskej republiky.

⁹⁷ Napríklad: Pri hybridnej taktike bude prvým čiastkovým cieľom nepriateľa presvedčiť verejnosť, že predstavitelia ich štátu nehovoria pravdu. Náhle sa pri realizácii objaví aj ďalšia skutočnosť, ktorá sa môže štátu, ktorý sa obraňuje proti hybridnej taktike zdať ako naplnenie ďalšieho cieľa nepriateľa, ktorý ale stále nepoznáme (t.j. *ďalší možný útok, napr. psychologická operácia*). Tým, že brániaci štát nepozná presný cieľ nepriateľa, môže prehnane reagovať na zdanlivý útok (napríklad *môže varovať obyvateľstvo*). V reálnom čase a priestore sa však okolnosti môžu zmeniť, zdanlivý útok napokon útokom nemusí byť a brániaci štát, sa ocitne v pozícii, kedy varovanie obyvateľstva nebolo

diskusí a odlišných názorov, avšak **hybridné hrozby a snaha o dosiahnutie vojenských cieľov pomocou nevojenských prostriedkov nie je žiadnou novinkou, len ich potenciál bol umocnený exponenciálnou expanziou prostredníctvom informačných technológií.**⁹⁸

2. STRATEGICKÁ KORUPCIA

Strategická korupcia predstavuje jednu z foriem hybridných hrozieb, „*kedy sa štáty alebo iné vplyvné subjekty snažia systematicky využívať korupčné praktiky na získavanie politického vplyvu*“⁹⁹ na presadzovanie vlastných geopolitických cieľov (známych, neznámych alebo predpokladaných). „*Je predpoklad, že v našom prostredí sú spájané predovšetkým s mocenskými ambíciami Ruska, Číny a USA.*“¹⁰⁰ Okrem toho však zdanlivé formy hybridnej taktiky využívajú všetky štáty, ktorých ambíciou je získavanie politického vplyvu mimo svojho územia, pre dosiahnutie vlastných politických cieľov, ktorých priame dosiahnutie by nebolo možné alebo by bolo porušením medzinárodného práva. V júli 2021 bolo v Spojených štátoch amerických schválené Memorandum o stanovení boja proti korupcii ako základného záujmu národnej bezpečnosti Spojených štátov, kde sa spomína potreba prijatia stratégie o spolupráci s medzinárodnými partnermi v boji proti strategickej korupcii zahraničných predstaviteľov krajín a strategickej korupcii štátom vlastnených podnikov. Stratégia je zameraná aj na postupné odstraňovanie medzier, ktoré sú využívané na zasahovanie do demokratických procesov prostredníctvom strategickej korupcie.¹⁰¹ Vláda Spojených štátov amerických osobitne označuje strategickú korupciu ako hrozbu pre národnú bezpečnosť a uvádza, že zahraniční protivníci používajú korupčné praktiky ako zbraň ako súčasť svojej zahraničnej politiky na presadzovanie svojich geopolitických cieľov.¹⁰² V rámci iniciatívy MCDC¹⁰³ bola publikovaná informácia, ktorá určovala štyri možné ciele strategickej korupcie ako formy hybridných nástrojov boja. Prvým cieľom je, že nepriateľský štát využíva korupciu personálneho substrátu verejnej správy ako **nástroj na získanie informácií**.¹⁰⁴ Ide predovšetkým o informácie, ktoré sú využívané na vydieranie, zastrašovanie, prípadne neskoršiu diskreditáciu oponentov. Vo verejnej správe sa nepriateľ snaží využiť strategickú korupciu aj napríklad na získanie informácií o činnosti hraničnej

potrebné. Nastane tak opačný efekt, kedy samotné varovanie oslabilo dôveru v štátne inštitúcie, čo napomohlo realizácii prvého čiastkového cieľa - presvedčiť verejnosť, že predstavitelia ich štátu nehovoria pravdu.

⁹⁸ CULLEN, J. P., WEGGE, N. *A Deadlier Peril: The role of corruption in Hybrid Warfare*. MCDC Countering Hybrid Warfare Project : marec 2019. Dostupné aj online na WWW [14.10.2023, 11:49]: https://assets.publishing.service.gov.uk/media/5caf5dd8e5274a59c06bf116/20190318-MCDC_CHW_Info_note_7.pdf

⁹⁹ LIŠOŇ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In. Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave Roč. 30 č. 2. s. 43.

¹⁰⁰ Taktiež. s. 43.

¹⁰¹ Čl. 2 písm. f) Memoranda o stanovení boja proti korupcii ako základného záujmu národnej bezpečnosti Spojených štátov. Dostupné aj online na WWW [08.10.2023, 13:36]: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/>

¹⁰² HANEBERG, M. *Strategic corruption : Being ready to act*. In. thomsonreuters.com. Dostupné aj online na WWW [08.10.2023, 13:39]: <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/strategic-corruption-ready-to-act/>

¹⁰³ MCDC je skratka pre *Multinational Capability Development Campaign* čo je projekt, ktorý vedú Spojené štáty americké a ďalších 23 štátov a medzinárodných vládnych organizácií na rozvoj riešenia nevojenských aktivít, s cieľom uspokojiť súčasné a budúce operačné potreby spojené s vedením spoločných, mnohonárodných a koalíčných operácií.

¹⁰⁴ CULLEN, J. P., WEGGE, N. *A Deadlier Peril: The role of corruption in Hybrid Warfare*. MCDC Countering Hybrid Warfare Project : marec 2019. Dostupné aj online na WWW [14.10.2023, 11:49]: https://assets.publishing.service.gov.uk/media/5caf5dd8e5274a59c06bf116/20190318-MCDC_CHW_Info_note_7.pdf

a cudzineckej polície pre lepšiu organizáciu ďalších nepriateľských činností (napríklad na umožnenie obchodovania s ľuďmi prostredníctvom danej krajiny). Tento prvý cieľ získavania informácií slúži na prípravu ďalších foriem hybridnej taktiky. **To znamená, že každá ďalšia forma hybridnej taktiky sa môže v čase vyvíjať, v závislosti od úspechu alebo neúspechu pôvodnej formy hybridnej taktiky nepriateľa, čo podporuje naše tvrdenie v úvode, že presný cieľ nepriateľa s istotou nikdy nepoznáme a sám o sebe podlieha zmenám, v závislosti od naplnenia iných čiastkových cieľov.** Druhým cieľom je korupcia ako **nástroj zvýšenia účinnosti dopadu ďalších aktivít.** Korupciou možno rozšíriť už vopred identifikované nedostatky v systémoch cudzích (brániacich sa) štátov. Nepriateľ (cudzí štátny aktér) môže za pomoci korupcie zabrániť zmenám v systéme, ktoré by umožnili systémové chyby odstraňovať. Príkladom môže byť systém krízového riadenia, ktorý nemusí byť v niektorom zo štátov plne spôsobilý adekvátne reagovať na krízové situácie, kedy sa za pomoci korupcie budú akékoľvek snahy o prijímanie opatrení (napríklad: zmeny zákonov, návrhy vyhlášok, participácia na modernizačných projektoch) na zlepšenie tohto systému blokovať, aby sa niektoré systémové zmeny neuskutočnili. Korupcia sa dá zneužiť aj na to, aby nepriateľ naopak prehľboval už identifikované systémové nedostatky. Takúto strategickú korupciu je možné opätovne (ako aj v prvom celi) realizovať prostredníctvom korupčného správania personálneho substrátu, ktorý participuje na rozhodovacích procesoch vo verejnej správe. Tretí a štvrtý cieľ strategickej korupcie je podobný tým, že korupcia, ak už bola realizovaná v danom štáte sa stáva ďalším nástrojom hybridnej taktiky, hoci nepriamej. Môže ísť o **úmyselné narušenie a rozvrat štátneho pilieru bezpečnosti, sociálneho rozvoja a správy vecí verejných.** Čiže korupcia použitá na rozvrátenie štátnej politiky vo všetkých nevojenských smeroch, kde verejnosť, že nevie, že je za tým strategická korupcia nepriateľa. Korupcia bude vplývať na verejnosť psychologicky tak, že spoločnosť bude mať pocit, že systém nefunguje z vlastnej viny správcov štátu (z ich neschopnosti spravovať štát). Štvrtým cieľom a zároveň nástrojom je **zneužitie vedomosti o korupcii,** kedy nepriateľ úmyselne a cielene rozšíri informáciu o korupcii, aby tým emocionálne vplýval na verejnosť. Táto forma hybridnej taktiky sa môže využiť napríklad v snahe ovplyvniť výsledok referenda alebo volieb, či iných nástrojov priamej alebo nepriamej demokracie.

Korupciu možno korupciu vyjadriť matematicky aj tak, že ju chápeme ako rozdiel súčtu monopolu moci a voľnosti rozhodovania na základe vlastnej úvahy a súčtu vyvoditeľnej zodpovednosti spolu s transparentnosťou, ochranou oznamovateľov a ďalšími faktormi.¹⁰⁵ Hoci **korupcia** sa celosvetovo bežne definuje ako „*zneužívanie verejnej moci na súkromný zisk*“ alebo „*zneužívanie verejných inštitúcií a úradu na úkor spoločného dobra*“¹⁰⁶, tak tieto definície nepostačujú na vymedzenie a vystihnúť všetky druhy korupcie. Dôležitou skutočnosťou, čím sa líši strategická korupcia od bežnej korupcie je, že ciele korupcie nie sú súkromný zisk ale skôr politický vplyv. V súčasnosti je strategická korupcia vymedzená niektorými autormi tak, že strategická korupcia predstavuje: „*najmä využívanie korupčných praktík a nelegálnych peňazí na získavanie*

¹⁰⁵ KLITGAARD, R. *Addressing Corruption Together*. Paríž: OECD, 2015. s. 37. Dostupné aj online na WWW [11.09.2023, 12:02]: <https://www.oecd.org/dac/conflict-fragility-resilience/publications/FINAL%20Addressing%20corruption%20together.pdf>

¹⁰⁶ CULLEN, J. P., WEGGE, N. *A Deadlier Peril: The role of corruption in Hybrid Warfare*. MCDC Countering Hybrid Warfare Project : marec 2019. Dostupné aj online na WWW [14.10.2023, 11:49]: https://assets.publishing.service.gov.uk/media/5caf5dd8e5274a59c06bf116/20190318-MCDC_CHW_Info_note_7.pdf

politického vplyvu a ovplyvňovanie verejnej mienky. “¹⁰⁷ Pričom je nutné doplniť, že táto definícia je ďalej rozvíjaná v kontexte hybridných hrozieb tak, že iniciátormi strategickej korupcie sú predovšetkým „predstavitelia cudzích štátov alebo iných vplyvných subjektov usilujúcich sa využívať politický vplyv na presadzovanie vlastných geopolitických cieľov.“¹⁰⁸ **Strategická korupcia** sa ale podľa iných autorov musí rozlišovať od **byrokratickej korupcie** a **rozsiahlej korupcie**. Kým *byrokratická korupcia* predstavuje skôr úplatkárstvo, kde cieľom je získať úkon alebo výkon vo verejnej službe (napríklad získanie vodičského preukazu), *rozsiahla korupcia* predstavuje trestnú činnosť páchanú podnikateľmi, oligarchami alebo zločincami, ktorí platia vysokých úradníkov výmenou za preferenčné zaobchádzanie alebo výmenou za kontrolu nad kľúčovými sektormi hospodárstva, kde je možné dosiahnuť veľké zisky, najčastejšie bankami, telekomunikáciami a prírodnými zdrojmi, ako je ropa a plyn. Pri byrokratickej a rozsiahlej korupcii je jasné, že zneužívanie verejnej moci slúži na súkromný zisk a že sa ten, kto dáva úplatok, a ten, kto berie, len snažia obohatiť. V strategickej korupcii je síce u niektorých páchatel'ov motivácia aj súkromný zisk, avšak **korupčné trestné činy v konkrétnej krajine sú vykonávané v súlade s národnou stratégiou nepriateľskej krajiny.**¹⁰⁹

3. STRATEGICKÁ KORUPCIA VO VEREJNEJ SPRÁVE

Strategická korupcia sa odohráva nielen vo verejnej správe a preto je potrebné vymedziť aj pojem verejná správa, ktorou v skratke chápeme „*správu verejných záležitostí, ktorá sa realizuje vo verejnom záujme ako prejav výkonnej moci v štáte a subjekty, ktoré ju realizujú, ju realizujú ako právom uloženú povinnosť*“.¹¹⁰ Ide teda o realizáciu len výkonnej moci v štáte (nie súdnej, ani zákonodarnej) a preto sa strategická korupcia sústreďí na realizáciu činností, ktoré vykonávajú ústredné orgány štátnej správy, orgány štátnej správy s celoštátnou pôsobnosťou, miestne orgány štátnej správy a orgány územnej alebo aj záujmovej samosprávy. Z tohto dôvodu možno vymedziť charakter strategickej korupcie vo verejnej správe ako nezákonné korupčné správanie majúce vplyv na realizáciu výkonnej moci v štáte, ktoré je v súlade s cieľmi nepriateľskej krajiny. V rámci analýzy legislatívneho rámca je v boji proti strategickej korupcii v súčasnosti v platnosti viacero právnych predpisov. Samozrejme za najznámejší možno považovať Trestný zákon, v ktorom sa nachádzajú skutkové podstaty trestných činov prijímania úplatku a podplácania, kde je navyše doplnené prijímanie úplatku zahraničným verejným činiteľom. V prípade prijímania úplatku ide skutkovú podstatu: „*Kto ako zahraničný verejný činiteľ priamo alebo cez sprostredkovateľa pre seba alebo pre inú osobu prijme, žiada alebo dá si slúbiť úplatok v súvislosti s výkonom úradných povinností alebo v súvislosti s výkonom jeho funkcie v úmysle, aby sa získala alebo zachovala neprimeraná výhoda, potrestá sa odňatím slobody na päť rokov až dvanásť rokov.*“¹¹¹ Za zahraničného verejného činiteľa sa považuje osoba, ktorá zastáva funkciu aj vo

¹⁰⁷ PIŠKO, M. *Hybridné hrozby na Slovensku. Strategická korupcia. Analýza legislatívy, štruktúr a procesov.* Bratislava: GLOBSEC, 2019. s. 4. Dostupné aj online na WWW [14.10.2023, 15:37]: <https://www.globsec.org/sites/default/files/2019-06/Hybridne-hrozby-na-Slovensku-Strategicka-korupcia.pdf>

¹⁰⁸ Taktiež. s. 4

¹⁰⁹ ZELINKOW, F. D., EDELMAN, E., HARRISON, CH., GENTER, C. W. *Подъём стратегической коррупции. Как государства превратили вранки в оружие.* In. Россия в глобальной политике, 2020. Prevzaté z Foreign Affairs, č. 4/2020. Dostupné aj online na WWW [14.10.2023, 16:00]: <https://globalaffairs.ru/articles/podyom-strategicheskoy-korruptcii/>

¹¹⁰ HAŠANOVÁ, J., DUDOR, L., *Základy správneho práva.* 5. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. s. 11.

¹¹¹ § 330 zákona Národnej rady Slovenskej republiky č. 300/2005 Z. z. – Trestný zákon v znení neskorších predpisov.

výkonnom orgáne alebo v inom orgáne verejnej správy cudzieho štátu.¹¹² Tieto skutkové podstaty boli do Trestného zákona¹¹³ doplnené na základe Dohovoru o boji s podplácaním zahraničných verejných činiteľov v medzinárodných obchodných transakciách. Vo vzťahu k strategickej korupcii preventívne pôsobia aj ďalšie právne predpisy. Napríklad v zmysle zákona o politických stranách a politických hnutiach je zakázané aby politická strana prijala dar alebo nejaké iné bezodplatné plnenie od fyzickej osoby, ktorá nemá trvalý pobyt na území Slovenskej republiky, ani od právnickej osoby, ktorá má sídlo v zahraničí.¹¹⁴ Ďalším právnym predpisom, ktorý slúži na identifikovanie prípadnej strategickej korupcie vo verejnej správe je zákon o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu, ktorý stanovuje povinnosti pre povinné osoby ohlásiť bez zbytočného odkladu ohlásiť Finančnej spravodajskej jednotke neobvyklú obchodnú operáciu alebo pokus o jej vykonanie.¹¹⁵ Kľúčovým zákonom na boj proti strategickej korupcii vo verejnej správe je ale zákon o registri partnerov verejného sektora¹¹⁶, ktorý môže odhaliť zahraničných aktérov pri ovplyvnení rozhodnutí v rámci verejnej správy v Slovenskej republike. Register partnerov verejného sektora môže pomôcť „*pri odhaľovaní pozadia prípadov, pri ktorých by sa zahraniční aktéri alebo ich spolupracovníci mohli snažiť ovplyvňovať rozhodnutia v slovenskej verejnej správe cez legálne transakcie, napríklad cez verejné obstarávanie.*“¹¹⁷

ZÁVER

Charakteristickými črtami strategickej korupcie vo verejnej správe je, že je realizovaná v prostredí orgánov verejnej správy, pričom jej cieľom je vplyvať na rozhodovaciu činnosť orgánov verejnej správy, ktorá je prostredníctvom metód činnosti verejnej správy vyjadrená v jednotlivých formách činností verejnej správy. V obsahu jednotlivých foriem činností verejnej správy je zachytený priamy výsledok korupčného pôsobenia nepriateľského štátu (druhého štátneho aktéra), ktorý prostredníctvom štátnych alebo neštátnych aktérov naplňa svoje ciele uvedené v jeho národnej stratégii. Materiálnym dôkazom páchania strategickej korupcie je výsledná forma činnosti verejnej správy, v ktorej sa pôsobenie korupčného správania prejavuje. Charakter a hlavná príčina strategickej korupcie vo verejnej správe je motivovaná na rozdiel od iných typov korupcie vždy politickými príčinami. Boj proti strategickej korupcii musí odrážať samotný charakter strategickej korupcie a jeho realizácia musí byť zabezpečená prijatím adekvátnych legislatívnych a inštitucionálnych opatrení.

¹¹² § 128 ods. 2 písm. a) zákona Národnej rady Slovenskej republiky č. 300/2005 Z. z. – Trestný zákon v znení neskorších predpisov.

¹¹³ Zákon Národnej rady Slovenskej republiky č. 300/2005 Z. z. – Trestný zákon v znení neskorších predpisov.

¹¹⁴ § 24 ods. 1 písm. f) a g) zákona Národnej rady Slovenskej republiky č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov.

¹¹⁵ § 17 zákona Národnej rady Slovenskej republiky č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

¹¹⁶ Zákon Národnej rady Slovenskej republiky č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

¹¹⁷ PIŠKO, M. *Hybridné hrozby na Slovensku. Strategická korupcia. Analýza legislatívy, štruktúr a procesov.* Bratislava: GLOBSEC, 2019. s. 4. Dostupné aj online na WWW [14.10.2023, 15:37]: <https://www.globsec.org/sites/default/files/2019-06/Hybridne-hrozby-na-Slovensku-Strategicka-korupcia.pdf>

Zdroje

1. BUZALKA, J. *Teória bezpečnostných rizík*. Bratislava : Akadémia Policajného zboru v Bratislave, 2012. 168 s. ISBN 978-80-8054-547-5.
2. CULLEN, J. P., WEGGE, N. A *Deadlier Peril: The role of corruption in Hybrid Warfare*. MCDC Countering Hybrid Warfare Project : marec 2019. Dostupné aj online na WWW [14.10.2023, 11:49]: https://assets.publishing.service.gov.uk/media/5caf5dd8e5274a59c06bf116/20190318-MCDC_CHW_Info_note_7.pdf
3. HANEBERG, M. *Strategic corruption : Being ready to act*. In. thomsonreuters.com. Dostupné aj online na WWW [08.10.2023, 13:39]: <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/strategic-corruption-ready-to-act/>
4. HAŠANOVÁ, J., DUDOR, L., *Základy správneho práva*. 5. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. 403 s. ISBN 978-80-7380-842-6.
5. HULLOVÁ, M. *Indikátory hybridných hrozieb – nástroj ich identifikácie a eliminácie*. In. Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave, Roč. 31 č. 2. s. 5-26. ISSN 1335-1370.
6. KLITGAARD, R. *Addressing Corruption Together*. Paríž: OECD, 2015. s. 37. Dostupné aj online na WWW [11.09.2023, 12:02]: <https://www.oecd.org/dac/conflict-fragility-resilience/publications/FINAL%20Addressing%20corruption%20together.pdf>
7. LIŠŇ, M., FIDLER, Ľ. *Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb*. In. Policajná teória a prax. Bratislava: Akadémia Policajného zboru v Bratislave Roč. 30 č. 2. s. 38-53. ISSN 1335-1370.
8. PIŠKO, M. *Hybridné hrozby na Slovensku. Strategická korupcia. Analýza legislatívy, štruktúr a procesov*. Bratislava: GLOBSEC, 2019. s. 4. Dostupné aj online na WWW [14.10.2023, 15:37]: <https://www.globsec.org/sites/default/files/2019-06/Hybridne-hrozby-na-Slovensku-Strategicka-korupcia.pdf>
9. ZELINKOW, F. D., EDELMAN, E., HARRISON, CH., GENTER, C. W. *Подъём стратегической коррупции. Как государства превратили вранку в оружие*. In. Россия в глобальной политике, 2020. Prevzaté z Foreign Affairs, č. 4/2020. Dostupné aj online na WWW [14.10.2023, 16:00]: <https://globalaffairs.ru/articles/podyom-strategicheskoy-korruptzii/>
10. Memorandum o stanovení boja proti korupcii ako základného záujmu národnej bezpečnosti Spojených štátov. Dostupné aj online na WWW [08.10.2023, 13:36]: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/>
11. Zákon Národnej rady Slovenskej republiky č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
12. Zákon Národnej rady Slovenskej republiky č. 300/2005 Z. z. – Trestný zákon v znení neskorších predpisov.
13. Zákon Národnej rady Slovenskej republiky č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
14. Zákona Národnej rady Slovenskej republiky č. 85/2005 Z. z. o politických stranách a politických hnutiach v znení neskorších predpisov.

INFORMAČNÉ TECHNOLOGIE AKO HYBRIDNÉ HROZBY

Mgr. Nataša Brabcová, LL.M., MBA, PhDr. JUDr. Mgr. Ervín Šimko, LL.M

TRIVIS – SŠV A VOŠ PK a KŘ Praha, s.r.o., externý doktorand, vedoucí odborných predmetu, Hovorčovická 281/11, 182 00 Praha 8, tel: + 420 773 658 103, e-mail: natašabracova@gmail.com, Katedra verejnej správy a krízového manažmentu, externý doktorand, Akademia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava 35, tel: + 421 917 113 038, e-mail: simko.ervin@gmail.com

Abstrakt: So súčasným dynamicky sa vyvíjajúcim prostredím plným nových a vylepšujúcich sa technológií narastá aj počet nových hybridných hrozieb. Z dôvodu rozsiahleho spektra pôsobnosti sú tieto hrozby stále viac nebezpečné a je ťažšie zaistiť potrebnú ochranu a obranu bezpečnostných záujmov štátu a jeho obyvateľov proti nim. Ohrozenie hybridnými hrozbami je v súčasnosti, vzhľadom na ľahký prístup k moderným technológiám, veľmi reálne. Bezpečnosť je relatívny jav ako aj stav, ktorý môžeme sledovať v premenných súvislostiach na dennej báze nášho života. V relatívnom stave pri ideálnych podmienkach môžeme deklarovať, že sa cítime byť v bezpečí no je dnešný stav ideálny je to stav, o ktorom môžeme hovoriť ako o bezpečnosti: či už fyzickej bezpečnosti alebo bezpečnosti dnešného virtuálneho sveta.

Kľúčové slová: bezpečnosť, informačne technológie, online priestor, kybernetická bezpečnosť, verejná správa, analýza.

ÚVOD

Informačne technológie ako hybridne hrozby môžeme chápať v širšom slova zmysle ako budovanie systému hrozieb v oblasti napadnutia informačných technológií pôsobiacich v celom priestore Slovenskej Republiky. Priestor kde pôsobia informačne technológie a na nich pôsobiace hybridne hrozby môžeme primárne definovať ako kybernetický priestor. Kybernetickým priestorom sa do nedávna chápalo prostredie, v ktorom prebiehalo spracovanie a prenos digitálne zaznamenananej informácie. V terajšej dobe sa ním už označuje celá informačná a komunikačná infraštruktúra organizácie, štátu, ale aj globálna informačná a komunikačná infraštruktúra. Približne až 97 % všetkých informácií sa už nachádza niekde v kybernetickom priestore. Následkom čoho sme sa stali závislí na jeho stabilite a spoľahlivosti dnes sa dá povedať až životne závislí. Následky hrozieb, ktoré z tohto prostredia môžu pochádzať, môžu mať v niektorých prípadoch veľké devastčné účinky, ktoré pôsobia na životy ľudí, majetok, životné prostredie, kultúrne a sociálne hodnoty. Musíme preto vytvárať podmienky a predpoklady na elimináciu ich tvorby a vnášanie do prostredia, ktoré musíme chrániť.

V príspevku sme sa zamerali na popísanie hybridných hrozieb so zameraním sa na informačné technológie, ich odhaľovanie a dotkneme sa aj postihu za vytváranie hrozieb v trestnoprávnej rovine, kde budeme len simulovať možnosť odhalenia a následného vyvodenia dôsledku čo by trestu v rovine právnej de lege lata ale poukážeme aj na možno úpravu de lege ferenda.

Predikciou tohto článku musí byť pochopenie, že hybridne hrozby sú riziko, ohrozenie, strata rovnováhy systému narušenie primárneho chodu a následne začatie sanovania škôd podľa zistenia reálneho stavu. „*Riziko predstavuje také javy a procesy, ktoré síce priamo a bezprostredne nepôsobia na ľudstvo, národy, štáty, jednotlivcov, ale ktoré za istého neadekvátneho alebo chybného správania sa, alebo za konkrétnej situácie, za istých konkrétnych podmienok v istej fáze*

svojho vývoja môžu vyvolať javy a procesy, ktoré sa transformujú na hrozby“.¹¹⁸ Hrozba má potenciálnu schopnosť poškodiť záujmy a hodnoty chránené štátom kde s titulu povahy hrozby je nutne rozlíšiť hrozby cielene na jednotlivé subjekty a objekty priamo alebo hrozby pôsobiace vo všeobecnosti s účelom spôsobiť narušenie a pripraviť sa na následný cielený útok. Hrozba pôsobí v konkrétnom čase, mieste a na konkrétne subjekty a objekty.

Na základe rozvoja technológií môžeme priam tvrdiť, že kráčať z reálnou dobou je stav priam nemožný musíme teda hľadať koncepciu ochrany jednotlivých systémov aby sme vedeli minimálnym spôsobom v stanovenom čase detekovať a následne reagovať na možné hybridne hrozby. Z názvu hybrid môžeme vyčítať nekonzistentnú sústavu javov a dejov v stave nízkej pripravenosti sa s nimi vysporiadať musíme sa preto zamerať na sanáciu a na jednotlivé fázy takýchto hrozieb, kde deduktívnou ale najmä analytickou činnosťou pripravujeme súbor opatrení na odvrátenie alebo profylaxiu systémov pred hybridnými hrozbami. Ak budeme pátrať po špecifikáciách alebo manuáloch na jednotlivé hybridne hrozby priamo v pôsobení na informačne technológie tak ich nenájdeme ani v tej namodrenejšej literatúre. Je preto nutne skĺbiť viacero defenzívnych prostriedkov ako sme už spomínali na úrovni jednotlivých atribútov, ktoré majú vplyv na obranu schopnosť systémov.

Ak sa pozrieme na platnú legislatívu, ktorá hovorí o jednotlivých stupňoch ochrany potom môžeme povedať že sme „SAFE“ v bezpečí, no reálny stav je že terajšia legislatíva nie je obsiahnutá reflexiou na vyvíjajúcu sa situáciu v oblasti hybridných hrozieb a ak by sme sa chceli cítiť nadpriemerne bezpečný v oblasti, ktorú legislatíva priamo definuje aj tam si musíme povedať, že je nutne novelizovať ju. Tým máme namysli

Zákon o Kybernetickej Bezpečnosti č. 69/2018 Z. z.

Zákon o Informačných technológiách vo verejnej správe č. 95/2019 Z. z.

Zákon o kritickej infraštruktúre č. 45/2011 Z. z.

Vybrali sme nosné legislatívne pramene, ktoré by mohli byť na pretrase v oblasti ochrany pred hybridnými hrozbami v oblasti informačných technológií a nehovoriac o tom že v demokratickom štáte musíme mať nástroj aj na sankcie voči spáchaniu škôd, ujmy, či nebudaj nejakej katastrofe tak namiesto je položiť si otázku kde v priestupkovom zákone alebo trestnom zákone nájdeme priamu definíciu, že za pôsobenie hybridnými hrozbami nám hrozí taký alebo onaký postih

Preto musíme povedať, je nutne definovať hybridne hrozby aj v týchto legislatívnych normách

Trestný zákon č. 300/2005 Z. z.

Zákon o priestupkoch č. 372/1990 Z. z.

Definovať hybridne hrozby môžeme nasledovne : hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.

Hybridné nástroje definujeme ako: nástroje alebo technológie kombinujúce viacero rôznych technologických prístupov alebo metód na riešenie konkrétneho problému. Hybridným nástrojom je napríklad kombinácia umelej inteligencie a strojového učenia s ľudskou interakciou. Táto

¹¹⁸ VOLNER, Š. Bezpečnosť, riziká a hrozby 21. storočia, Bratislava: IRIS 2012, ISBN: 978-80-8925-674 7

kombinácia umožňuje nástroju učiť sa z ľudských interakcií a následne využívať tieto informácie na zlepšovanie svojej funkčnosti a poskytovanie efektívnejších riešení. Hybridné nástroje sa často používajú v oblastiach, ako sú napríklad medicína, financie, priemysel alebo výroba. Ich výhodou je, že umožňujú využívať najlepšie vlastnosti viacerých technológií a zároveň minimalizovať ich nedostatky.

Podstatou hybridných hrozieb je: vedenie boja, ktoré v sebe spája rôzne formy a stratégie. Slovenská republika sa najčastejšie stretáva s pokusmi o ovplyvňovanie verejnej mienky v kybernetickom priestore, ktorý má sám o sebe hybridnú povahu. Nie je totiž vlastnený ani prevádzkovaný výlučne verejnými alebo súkromnými subjektmi. Pokrok v boji proti hybridným hrozbám si preto vyžaduje úzku spoluprácu medzi verejným a súkromným sektorom, ako aj civilno-vojenskú interakciu, pričom sa musí prijať celospoločenský prístup k problému.

Hybridne hrozby vnímame na každodennom prístupe k informáciám a ich prejavy považujeme za samozrejmú k následkom sa často krát dostávame až keď je neskoro. Niektoré ďalšie príklady hybridných nástrojov zahŕňajú kombináciu softvéru a hardvéru, kombináciu rôznych typov dátových úložísk alebo kombináciu tradičných a moderných technológií v informačných technológiách. No treba brať na zreteľ, že všetko to, čo dokáže ľudstvo posunúť vo vývoji vpred, sa dá naopak využiť, respektíve presnejšie zneužiť na nekalé účely s cieľom dosiahnuť výhody, ktoré mu neprináležia.

Hybridné hrozby sú kombináciou viacerých typov hrozieb, ktoré sa prelínajú a navzájom podporujú. Ide o spojenie rôznych metód útoku, ktoré zahŕňajú nebezpečenstvo v oblasti kybernetickej bezpečnosti, informačnej bezpečnosti, ale aj hybridnej vojny a terorizmu. Hybridné hrozby sú **rôznorodé a pôsobia naprieč doménami** infraštruktúry, kybernetického priestoru, vesmíru, ekonomiky, obrany, kultúry, spoločnosti, verejnej správy, práva, spravodajských služieb, diplomacie, politiky a informácií. Majú pritom tendenciu byť zložitejšie a čoraz viac sofistikovanejšie. Môžu byť vyvolané rôznymi faktormi, vrátane politickej motivácie hospodárskeho zisku alebo túžbou po moci a kontrole. Ich cieľom je zvyčajne narušenie politických procesov, hospodárskej stability alebo destabilizácia určitej oblasti. Európske centrum na boj proti hybridným hrozbám (Hybrid CoE) definuje ciele hybridných hrozieb nasledovne: *„Hybridné hrozby sú metódy a aktivity namierené voči zraniteľným miestam oponenta. Zraniteľné miesta môžu byť vytvorené mnohými vecami, vrátane historickej pamäte, legislatívy, starých praktík, geostrategických faktorov, silnej polarizácie spoločnosti, technologickými nevýhodami či ideologickými rozdielmi. Ak záujmy a ciele toho, čo využíva hybridné metódy a aktivity, nie sú dosiahnuté, situácia môže vyústiť do hybridnej vojny, kde značne narastie úloha armády a násilia“*.¹¹⁹

Základne charakteristiky hybridných hrozieb: Základným prvkom, ktorý odlišuje hybridné spôsoby vedenia vojny od hybridných hrozieb, je využitie vojenských síl a kapacít, ako aj hrozba silou alebo priame použitie ozbrojených síl skrytým či otvoreným spôsobom na dosiahnutie politických cieľov. Hybridné hrozby nemožno jednoznačne definovať vzhľadom na ich premenlivosť a nestálosť, definičným znakom je zneužívanie zraniteľnosti cieľa a vytváranie neprehľadných situácií s cieľom narušiť rozhodovacie procesy.

¹¹⁹ Hybrid CoE 2018, podľa Milo 2018

Nástrojom hybridných hrozieb môžu byť masívne dezinformačné kampane, ako aj využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie svojich priaznivcov. Hybridné hrozby predstavujú **súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Ohrozujú fungovanie demokratických spoločností a pokúšajú sa ich oslabovať** zvnútra s využitím ich zraniteľností, ale aj ich hlavných výdobytkov, vrátane slobody prejavu a vyjadrovania, nezávislosti médií, právneho štátu, verejnej kontroly inštitúcií a demokratickej politickej súťaže, ako aj otvorenosti trhovej ekonomiky.

V prostredí Slovenskej republiky, hybridné hrozby dlhú dobu neboli identifikované ako bezprostredná hrozba. Tento pojem sa prvýkrát objavil v roku 2016, a to v Bielej knihe o obrane Slovenskej republiky z dielne Ministerstva obrany SR. V bode 56. tohto strategického dokumentu je uvedené: „Z hľadiska spôsobu vedenia konfliktov v meniacom sa bezpečnostnom prostredí je vážnou bezpečnostnou hrozbou najmä propaganda na strategickej úrovni ako súčasť informačného a psychologického pôsobenia na vybrané cieľové skupiny spoločnosti v rámci tzv. informačnej vojny a špecifické operačné postupy, ktoré sú najlepšie charakterizované pojmom *hybridný spôsob vedenia bojových činností*“.¹²⁰ Koncepcie Slovenskej republiky na boj proti hybridným hrozbám, ich definuje nasledovne: „Súčasne pôsobiace aktivity, ktoré ohrozujú základné atribúty štátu alebo ich funkčnosť, sa označujú ako hybridné hrozby. Hybridná hrozba je definovaná ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie.“ Sú realizované aktivitami charakterizovanými centrálnou riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akciovosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené“¹²¹

Základnými indikátormi hybridných hrozieb sú:

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku
- rozsiahle sabotáže proti kľúčovej infraštruktúre;
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely; hrozba použitia vojenskej sily.

¹²⁰ Ministerstvo obrany SR 2016

¹²¹ Vláda SR 2018

Uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu. Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.¹²² (Definícia hybridných hrozieb by mala však zostať dostatočne pružná, aby primerane reflektovala na vývoj hrozieb. Vo svojej podstate je to však súbor koordinovaných činností alebo metód ktoré pôsobia destabilizačne a oslabujúco voči svojim protivníkom resp. aktérom proti ktorým majú byť využité bez jednoznačného vyhlásenia vojny v “de jure” kontexte.¹²³

KOMPARÁCIA A PRÍSTUP ČESKEJ REPUBLIKY PROTI HYBRIDNÝM HROZBÁM

Prvé explicitné zmienky o prístupe Českej republiky k čeleniu hybridným hrozbám (všeobecne hybridnému pôsobeniu) možno časovo zasadiť do obdobia formulácie obsahu strategického dokumentu Audit národnej bezpečnosti z roku 2016, kde do širšieho spektra najvýznamnejších aktuálnych hrozieb pre Českú republiku boli zakomponované konkrétne aj vplyv na bezpečnosť občanov Českej republiky.¹²⁴

Audit ukázal, že bezpečnostný systém je dobre pripravený na tzv. tradičné hrozby. Štát dokáže bojovať s kriminalitou, azylová a migračná politika je nastavená dobre a zvláda otázky spojené s migráciou, aj keď vždy je priestor na spresňovanie legislatívy aj nelegislatívnych opatrení. Audit však potvrdil, že tzv. moderné hrozby a najmä ich kombinácie vyžadujú oveľa zásadnejšiu pozornosť, než tomu bolo v minulosti. Schopnosť štátu detekovať a koordinovane riešiť prepojené útoky musí byť podľa auditu posilnená. Preto zintenzívni monitoring, spoluprácu medzi rezortmi a cvičenia aj spoluprácu so zahraničím a považuje za zodpovedné zapojiť do príprav aj verejnosť. Oveľa komplexnejšie potom sa musí tiež riešiť oblasť tzv. hybridných hrozieb a s nimi spojenými dezinformačnými útokmi.

Problematika čelenia hybridnému pôsobeniu a hybridným hrozbám či oblasť hybridného boja je veľmi rozsiahla. Často záleží na perspektíve a konkrétnom postoji jednotlivých expertov, akademikov či politických autorít, akým pohľadom na danú problematiku nazerať. Význačnú a určujúcu úlohu hrá v tejto súvislosti voľba a identifikácia referenčného objektu a neopomenuteľne taktiež určitá reflexia na vlastné umiestnenie.

V Českej republike je za oblasť čelenia hybridnému pôsobeniu zodpovedná vláda, ktorá by mala v ideálnom prípade prijímať zodpovedajúce opatrenia reagujúce na konkrétne hybridné hrozby a prejavy hybridného pôsobenia. Za čelenie jednotlivým aktivitám a prejavom hybridného pôsobenia sú v rámci svojich pôsobností následne zodpovedné jednotlivé rezorty (ministerstvá).

Hoci je vymenované celé spektrum zodpovedných subjektov, v Českej republike doposiaľ neexistuje spoločný koordinačný a spolupôsobiaci prvok, ktorý by komplexne zastrelil predmetnú problematiku.

¹²² Vláda SR 2018

¹²³ Európska komisia 2016

¹²⁴ Vojenské rozhledy [online]. 2023. [cit. 2023-04-06]. Dostupné z: <https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/aktualni-pristupy-hybridni-hrozby>

Slovenská republika je členským štátom Európskej únie (EÚ) aj Severoatlantickej aliancie (NATO). V posledných rokoch sa začala aj v týchto organizáciách dostávať do popredia téma hybridných hrozieb a hybridnej vojny. Z toho dôvodu boli vytvorené aj špecializované inštitúcie, niektoré zamerané na špecifické oblasti spadajúce pod tento koncept a iné pokrývajúce hybridné hrozby ako celok. V záujme prevencie a boja proti hybridným hrozbám vznikli špecifické štruktúry patriace pod EÚ: Stredisko EÚ pre hybridné hrozby (EU Hybrid fusion cell) zriadené v rámci Centra EÚ pre analýzu spravodajských informácií (EU INTCEN) a rovnako aj The European Centre of excellence for Countering Hybrid Threats. V rámci NATO vznikol celý rad špecializovaných centier excelentnosti, z ktorých viaceré majú priamy vzťah k problematike hybridných hrozieb. Asi najvýznamnejšie z nich sú NATO StratCom CoE (Centrum excelentnosti NATO na strategickú komunikáciu) a NATO Cooperative Cyber Defence Centre of Excellence (Spoločné centrum excelentnosti NATO na kybernetickú obranu). Z pohľadu európskych inštitúcií, je jeden z najrelevantnejších bodov konceptu hybridných hrozieb pomenovaný v dokumente Spoločný rámec EÚ pre boj proti hybridným hrozbám ktorý uvádza: „*Definície hybridných hrozieb sú síce rôzne a musia zostať flexibilné, aby mohli reagovať na premenlivú povahu týchto hrozieb*”.¹²⁵ Táto definícia si uvedomuje nejednoznačnosť pojmu, ktorý sa môže meniť v závislosti od krajiny, času, alebo situácie. Komisia rovnako považuje za dôležitý koordinovaný postup v boji proti hybridným hrozbám, no dodáva, že každá krajina má svoje vlastné slabé miesta, na ktoré sa musí pri obrane zamerať.

Hybridné hrozby informačných technológií vo verejnej správe predstavujú nový typ bezpečnostnej hrozby, ktorá kombinuje tradičné metódy s modernými technológiami a sociálnymi médiami a ktoré môžu ohroziť systémy a služby, ktoré poskytuje verejná správa. Nesú so sebou veľkú strategickú a bezpečnostnú hrozbu pre verejné inštitúcie, a preto by mali byť zvlášť zvažované aj v kontexte kybernetickej bezpečnosti.

V dnešnej dobe je informačná technológia (IT) kľúčovým prvkom pre fungovanie verejnej správy. Zahŕňa všetky informačné a komunikačné technológie používané na podporu a zlepšenie výkonu verejnej správy. Tieto technológie umožňujú vládam a iným verejným inštitúciám rýchlejšie a efektívnejšie poskytovať verejné služby a zlepšiť interakciu s občanmi. Zahŕňa širokú škálu technológií a aplikácií, vrátane webových stránok, mobilných aplikácií, softvéru pre správu záznamov, inteligentných systémov pre podporu rozhodovania elektronických služieb a online komunikačných nástrojov. Zároveň je to aj oblasť, kde môžu hybridné hrozby spôsobiť vážne problémy. Môžu mať za následok zneužitie informácií, stratu dát, či narušenie kritických systémov.

V kontexte verejnej správy sa môžu prejaviť napríklad cez:

- dezinformačné kampane – sú zamerané na zavádzanie verejnosti prostredníctvom falošných informácií, s cieľom ovplyvniť verejnú mienku, posilniť určité názory, oslabiť dôveru v médiá a demokratické inštitúcie alebo destabilizovať spoločnosť. Môžu sa šíriť rôznymi spôsobmi, vrátane sociálnych sietí, internetových fór, blogov alebo tradičných médií. V praxi sa realizujú prostredníctvom falošných alebo útočných informačných kampaní. V hybridnej hrozbe môžu byť využité techniky dezinformácie na poskytnutie nepravdivých informácií, ktoré môžu spôsobiť rozkol alebo spochybniť legitimitu určitej inštitúcie. Môžu byť tiež využité na šírenie počítačových vírusov alebo zavádzať odkaz na falošné webové stránky. Často sú podporované alebo šírené

¹²⁵ Európska komisia 2016

politickými, podnikateľskými alebo inými záujmovými skupinami s cieľom dosiahnuť svoje ciele. Niektoré príklady dezinformačných kampaní zahŕňajú zavádzajúce informácie o voľbách, dezinformácie o klimatických zmenách, falošné správy o zdravotných témach, alebo propagovanie nenávisť a diskriminácie na základe rasy, pohlavia alebo sexuálnej orientácie. Je dôležité si uvedomiť, že dezinformačné kampane môžu mať vážne následky na spoločnosť a demokratické inštitúcie. Dôležité je preto kriticky sa pozerieť na informácie, ktoré dostávame, a overiť ich pravdivosť pomocou spoľahlivých zdrojov a faktov.

- kybernetické útoky – vo verejnej správe, a nielen v nej, predstavujú vážne bezpečnostné riziko pre vládne inštitúcie, organizácie a občanov. Tieto útoky môžu zahŕňať pokusy o získanie citlivých informácií, úmyselné narušenie systémov alebo poškodenie infraštruktúry a majetku, môžu viesť ku krádeži citlivých údajov, porušeniu súkromia, ba dokonca môžu až paralyzovať fungovanie kritických systémov. Zahŕňajú pokusy o zneužitie firemných sietí, slúžiacich na poskytovanie verejnej služby. Môžu to byť napríklad útoky na databázy s cennými dátami, ktorej účelom môže byť vymôcť si výkupné alebo ukradnúť informácie. Niektoré príklady kybernetických útokov na verejnú správu zahŕňajú:
 - *Phishing*: Tento typ útoku sa snaží získať citlivé informácie od používateľov prostredníctvom zavádzajúcich e-mailov alebo webových stránok.
 - *Malware*: Tento typ útoku sa snaží infikovať počítače alebo siete škodlivým softvérom s cieľom získať prístup k informáciám alebo narušiť systémy.
 - *Ransomware*: Tento typ útoku sa snaží blokovat prístup k dôležitým informáciám alebo systémom a následne požaduje výkupné za ich odblokovanie.
 - *DDoS útoky*: Tieto útoky sa snažia preťažiť webové stránky alebo sieťové systémy prostredníctvom veľkého počtu požiadaviek, čo môže spôsobiť výpadky a straty dát.
- sociálne inžinierstvo – hybridné hrozby môžu byť jeho produktom. Ide o formu kybernetického útoku, ktorý sa snaží zneužiť dôveru a ochotu pomôcť ostatným. Sociálne inžinierstvo je technika, ktorou útočníci využívajú sociálne interakcie a psychologické vplyvy na ľudí s cieľom získať citlivé informácie alebo zaviesť obeť do niečoho nebezpečného. Je predstavované šírením neznámych s cieľom získať citlivé informácie o inštitúciách verejnej správy alebo jednotlivých zamestnancov, získať prístup do životných údajov používateľa alebo prevziať kontrolu nad jeho účtom. Príklady sociálneho inžinierstva zahŕňajú *phishing* (získavanie citlivých informácií prostredníctvom zavádzajúcich e-mailov alebo webových stránok), *pretexting* (falošné tvrdenie, že útočník má oprávnenie na určité akcie) alebo *baiting* (zavádzajúce ponuky alebo príležitosti na získanie informácií alebo prístupu k systémom). Sociálne inžinierstvo sa často využíva ako prvá fáza útoku na organizácie alebo jednotlivcov, keďže môže byť účinnejšie a menej nákladné ako pokusy o prelomenie technickej ochrany. Často sa zameriava na zamestnancov organizácií, ktorí môžu byť vnímaní ako slabé miesto v systéme ochrany.

Boj proti hybridným hrozbám vychádza z nutnosti kooperácie zainteresovaných subjektov založenej na realizácii opatrení, ďalej pružnej výmene informácií, a koordinácii postupov. Ide teda o koordinovaný a komplexný prístup. Boj proti hybridným hrozbám v informačných technológiách vo verejnej správe vyžaduje kombináciu technologických a organizačných opatrení. Niektoré z možných krokov, ktoré by mohli byť účinné pri boji proti hybridným hrozbám na informačné technológie vo verejnej správe, sú:

Vyspelé technologické riešenia: Verejná správa by mala mať k dispozícii vyspelé technologické riešenia na detekciu, monitorovanie a prevenciu kybernetických útokov a iných hybridných hrozieb. Tieto technológie by mali byť prispôsobené špecifickým potrebám a rizikám verejnej správy a mali by identifikovať a rýchlo reagovať na prípadné hrozby a anomálie.

Zabezpečenie kritických systémov: Kritické systémy a informačné systémy verejnej správy by mali byť chránené pomocou vyspelých technologických riešení na detekciu a prevenciu kybernetických útokov a iných hybridných hrozieb. K tomu slúžia napr.: *antivírusový softvér*, ktorý je základnou technológiou pre detekciu a prevenciu kybernetických útokov. Pomáha chrániť počítače a siete pred škodlivým softvérom a vírusmi; *firewall* pomáha chrániť počítače a siete pred neoprávneným prístupom tým, že kontrolovať tok dát medzi sieťami a zariadeniami; *Intrusion Detection System (IDS)*, sleduje sieťovú aktivitu a hľadá neobvyklé vzory správania, ktoré by mohli naznačovať kybernetický útok; *Intrusion Prevention System (IPS)*, ktorý sa podobá na IDS, ale namiesto toho, aby iba identifikoval neobvyklé vzory správania, sa pokúsi zabrániť kybernetickému útoku ešte predtým, ako sa stane; *SIEM (Security Information and Event Management)*, zabezpečuje monitorovanie, správu a analýzu rôznych udalostí v systéme na detekciu neobvyklých vzorov a varovných signálov, ktoré by mohli naznačovať kybernetický útok. Ďalej to môžu byť bežné siete ako *Virtual Private Network (VPN)*, ktorý umožňuje šifrovanú a bezpečnú komunikáciu medzi zariadeniami a sieťami, v ktorých sú dáta prenášané.; *Advanced Threat Protection (ATP)* je technológia, ktorá používa rôzne metódy na detekciu a prevenciu pokročilých hrozieb, ako sú napríklad zero-day útoky alebo APT útoky ¹²⁶; *Data Loss Prevention (DLP)* pomáha chrániť dôverné a citlivé dáta pred únikom alebo zneužitím. Pomáha monitorovať a riadiť tok dát, čím sa minimalizuje riziko straty alebo zneužitia dát.

Školenie zamestnancov: Zamestnanci verejnej správy by mali byť pravidelne školení v oblasti kybernetickej bezpečnosti a v rámci toho by mali byť informovaní o najnovších hrozbách a o tom, ako sa im vyhnúť alebo ich odvrátiť. Mali by byť obozretní pri otváraní príloh e-mailov, návšteve nebezpečných webových stránok a používaní verejných Wi-Fi sietí.

¹²⁶ Zero-day útoky sú kybernetické útoky, ktoré využívajú zraniteľnosti v softvérových systémoch, ktoré sú zatiaľ neznáme alebo nemajú opravu. Tento typ útoku môže byť veľmi nebezpečný, pretože táto zraniteľnosť ešte nebola odhalená a neexistuje žiadna obrana alebo náprava, ktorá by ju chránila. Zero-day útoky sú často používané k šíreniu škodlivého softvéru alebo na získanie neoprávnenej prístupu k cenným dátam. Využívajú sa na útoky na rôzne ciele, vrátane podnikov, vládnych inštitúcií, bankových systémov a ďalších kritických infraštruktúr. Vývojári softvéru sa snažia minimalizovať riziko zero-day útokov tým, že systematicky vyhľadávajú zraniteľnosti a aktualizujú softvér s opravami bezpečnostných chýb. Bezpečnostné aktualizácie sú však často oneskorené alebo sa nedostanú ku všetkým používateľom, takže je dôležité, aby používatelia boli obozretní a mali aktuálny antivírusový softvér a firewall. Existujú aj špeciálne nástroje a technológie, ktoré sa používajú na detekciu zero-day útokov. Tieto nástroje monitorujú sieťovú prevádzku a vyhľadávajú neobvyklé vzory, ktoré by mohli naznačovať pokus o zero-day útok. V prípade zistenia podozrivých aktivít môžu tieto nástroje automaticky reagovať a obmedziť prístup počítača alebo používateľa. Vzhľadom na neustále sa meniace hrozby v kybernetickom priestore je dôležité mať nielen správne nástroje na detekciu a prevenciu zero-day útokov, ale aj pripravenosť a schopnosť rýchlo reagovať a minimalizovať škody v prípade, že sa takýto útok stane.

Advanced Persistent Threat (APT) útoky sú sofistikované kybernetické útoky, ktoré sú zamerané na dlhodobú infiltráciu cieľového systému alebo siete a získanie neoprávnenej prístupu k citlivým údajom alebo zdrojom. Útoky APT sa od bežných kybernetických útokov líšia tým, že sú plánované, cielené a vytrvalé, pričom útočníci používajú rôzne techniky, aby sa vyhli detekcii a zabránili zisteniu svojej identity.

Prísna kontrola prístupov: Prístup k informačným systémom by mal byť prísne kontrolovaný a overovaný, aby sa minimalizovalo riziko zneužitia prístupov. V praxi to možno realizovať napr. zavádzaním silných hesiel a autentifikačných mechanizmov, viacúrovňovým overovaním totožnosti, ad hoc vytvoreným a časovo obmedzeným prístupovým kódom.

Zabezpečená komunikácia: Komunikácia medzi informačnými systémami by mala byť zabezpečená pomocou šifrovania a iných technológií na ochranu dát.

Spolupráca a koordinácia: Boj proti hybridným hrozbám by mal byť koordinovaný a spolupracujúci a malo by ho charakterizovať úsilie medzi rôznymi orgánmi verejnej správy, ako aj súkromným sektorom a občianskou spoločnosťou.

Pravidelné aktualizácie a overenia: Informačné systémy a technologické riešenia by mali byť pravidelne aktualizované a overované, aby sa zabezpečilo, že sú stále účinné proti najnovším hrozbám. Tieto opatrenia môžu zahŕňať pravidelné aktualizácie softvéru, zálohovanie dôležitých dát.

Vytvorenie protokolov a postupov pre rýchlu a účinnú reakciu : Je dôležité mať pripravené plány a protokoly na rýchlu a efektívnu reakciu na hybridné hrozby. Organizácie verejnej správy by mali mať zostavené tzv. bezpečnostné plány. Na ochranu proti hybridným hrozbám existuje niekoľko protokolov a postupov, ktoré pomáhajú identifikovať a eliminovať hrozbu. Spomenúť možno napr. tzv. *Hybrid Threat Response (HTR) framework*, ktorý bol vyvinutý NATO a EÚ. Tento rámec poskytuje štruktúrovaný postup na reakciu na hybridné hrozby, ktorý zahŕňa detekciu hrozby, analýzu, hodnotenie a plánovanie reakcie. HTR rámec sa zameriava na koordinovanú reakciu a spoluprácu medzi rôznymi inštitúciami a organizáciami. Ďalším protokolom je tzv. *Cyber Incident Response Plan (CIRP)*, ktorý sa zameriava na reakciu na kybernetické útoky, ktoré môžu byť súčasťou hybridných hrozieb. CIRP zahŕňa definíciu zodpovednosti a úloh, koordináciu, plánovanie, analýzu a správu kybernetických incidentov. Okrem týchto protokolov existujú aj ďalšie postupy a nástroje, ktoré sa používajú na reakciu na hybridné hrozby. Patrí sem napríklad pripravenosť a plánovanie, ktoré zahŕňajú predbežné opatrenia a pravidelné cvičenia a simulácie, aby sa zvýšila efektivita a rýchlosť reakcie. Dôležitou súčasťou protokolov na reakciu na hybridné hrozby je tiež spolupráca medzi rôznymi inštitúciami a organizáciami. Spolupráca umožňuje zdieľanie informácií a skúseností, koordináciu a lepšiu efektivitu pri riešení hrozby.

Zlepšenie legislatívy a regulácie: Zavedenie a presadzovanie prísnych noriem a nariadení na ochranu informačných systémov, kritických infraštruktúr a sietí. Ochrana informačných systémov verejnej správy je kritickou otázkou pre bezpečnosť štátu a občanov. Preto existujú právne predpisy, ktoré upravujú ochranu informačných systémov verejnej správy. V Európskej únii sú najdôležitejšie smernice o kybernetickej bezpečnosti, ktoré sa týkajú aj ochrany informačných systémov verejnej správy. *Smernica NIS (Network and Information Systems Directive)*¹²⁷ stanovuje minimálne bezpečnostné požiadavky pre prevádzkovateľov kritických služieb a digitálne služby, vrátane verejnej správy. Ďalšou smernicou, ktorá sa týka ochrany informačných systémov verejnej správy, je *GDPR (General Data Protection Regulation)*. Táto smernica stanovuje pravidlá na ochranu osobných údajov a ich spracovávanie. GDPR tiež ukladá povinnosť poskytovať bezpečnostné opatrenia na ochranu osobných údajov a informačných

¹²⁷ Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

systémov. V rámci Slovenskej republiky existuje zákon č. 69/ 2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorý sa zameriava na ochranu informačných systémov a kybernetickú bezpečnosť. Tento zákon stanovuje povinnosť prevádzkovateľov kritických informačných infraštruktúr a digitálnych služieb na poskytovanie informácií o kybernetickej bezpečnosti a oznámenie bezpečnostných incidentov. Ďalší zákon, ktorý sa týka ochrany informačných systémov verejnej správy, je zákon č. 18/2018 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Tento zákon stanovuje pravidlá na ochranu osobných údajov a ich spracovávanie a ukladá povinnosť zabezpečiť bezpečnostné opatrenia na ochranu osobných údajov.

Okrem toho existujú aj iné právne predpisy a smernice, ktoré sa týkajú ochrany informačných systémov verejnej správy. Ich cieľom je zabezpečiť vysokú úroveň kybernetickej bezpečnosti a ochrany osobných údajov, čo prispieva k ochrane štátu a občanov pred kybernetickými hrozbami. Hoci sa legislatíva na ochranu informačných systémov verejnej správy neustále vyvíja a aktualizuje, vzhľadom na rastúce množstvo kybernetických hrozieb je nutné venovať jej väčšiu a dôslednejšiu pozornosť. De lege ferenda by sme navrhli v rámci legislatívnej úpravy:

- *zvýšenie sankcií a trestov za kybernetické útoky a zneužívanie osobných údajov* – zákony by mali byť prísnejšie a vynucovanie by malo byť dôraznejšie na tých, ktorí porušujú zákony;
- *zabezpečenie vyšších národných štandardov kybernetickej bezpečnosti* – štát by mal stanoviť minimálne bezpečnostné požiadavky pre informačné systémy verejnej správy a definovať postupy na identifikáciu a odstránenie bezpečnostných slabín;
- *zavedenie kontroly na dodávateľov a dodávateľské reťazce* – je dôležité, aby dodávatelia boli skúmaní z hľadiska bezpečnosti ich produktov a služieb, ktoré dodávajú verejnej správe.

Celkovo by zlepšenie legislatívy na ochranu informačných systémov verejnej správy malo prispieť k väčšej ochrane kritických informačných infraštruktúr, osobných údajov a kybernetickej bezpečnosti, čo by malo mať pozitívny vplyv na bezpečnosť štátu a občanov.

Celkový prístup k boju proti hybridným hrozbám by mal byť založený na spolupráci a koordinácii rôznych orgánov a sektorov a mal by byť prispôsobený aktuálnym hrozbám a trendom. Úspešná ochrana proti hybridným hrozbám by mala byť založená na komplexnom a dobre koordinovanom prístupe, ktorý zahŕňa kombináciu technických, organizačných a ľudských opatrení.

Na záver konštatujeme, že za jednu z najviac zraniteľných oblastí, ktorá výraznou mierou prispieva k tomu, že riziko hybridnej hrozby aj v oblasti informačných technológií vo verejnej správe je veľmi vysoké, považujeme nízke povedomie spoločnosti ako takej o kybernetickej bezpečnosti. Z tohto dôvodu je zvýšenie povedomia o tomto fenoméne mimoriadne dôležité. Veríme, že tento článok k tomu prispel.

Hybridne hrozby v rovine priestupkov by mohli podľa nášho názoru byť definované ako základná forma zneužitia technologických ale verejne prístupných nástrojov alebo prostriedkov na šírenie hoaxov, dezinformácií a iných hybridných hrozieb, ktoré sme v predošlých častiach vymenovali a definovali. Zároveň môžeme zaviesť aj inú metriku rozdelenia a povahy vzhľadom na spôsobenú škodu kde sa budeme opierať najmä o podstatu identifikovania hybridnej hrozby kde predikovať je ich ťažké ale následne po pôsobení na systém inštitúcií, ekonomiku, subjekt a i... , môžeme

vytvoriť škálu priestupkov a k nim vyšpecifikovať určité sankcie. Tu by však mala existovať funkčnosť právneho systému na úrovni prejednavania takýchto priestupkov. Je nutne ich vedieť správne posúdiť a v prípade nutnosti požadovať aj o odborne stanovisko pre následne udelenie sankcie čo značne predražuje a komplikuje prejednanie priestupku samotného s ohľadom na hospodárnosť a účelnosť konania samotného. Následne na uvedené je na zvážení zákonodarcu či v legislatívnej norme ako je zákon o priestupkoch by našiel odvahu definovať hybridné hrozby ako priestupok.

Hybridne hrozby v rovine trestnoprávnej: ak sme sa zaoberali ako vyšpecifikovať alebo vydefinovať v oblasti zákona o priestupkoch hybridne hrozby tak v trestnoprávnej rovine by sme ich mohli definovať jednoduchým spôsobom a to jedným paragrafovým znením a zaradiť ho do trestného zákona, ale ak uvažujeme nad spôsobom ako ho paragrafovom znení nazvať, napadá nám myšlienka skôr kde ho zaradiť a to najmä do oblasti spôsobenia škody na majetku. Pozor! Bude to postačujúce? Preto sa nám vynorila v mysli myšlienka definovať v trestnom kódexe slovenskej republiky hybridne hrozby viac širšie a následne sa s nimi vysporiadať čo do jednotlivých presahov jednotlivých druhov trestného práva. Napríklad v rovine majetkovej, rovine duševného vlastníctva alebo rovine hospodárskej, rovine šírenia poplašnej správy ako aj iných mnohých. Navrhli by sme aby v tejto oblasti jednali a tvorili základ rozdelenia odborne skupiny kde by sa definovala nielen miera spôsobenej škody ale aj spôsob akým by boli vytvorené a aký účel mali splniť a najmä čo nimi páchatel sledoval. Potom by predpokladáme vznikla škála na ich ukotvenie v právnych kódexoch slovenskej republiky, ktorými sa dnes riadi celá naša vyspela spoločnosť. Upriamujúc na rastúcu mieru digitalizácie a presahu informačných technológií do nášho každodenného života, konštatujeme: „Bezpečnosť je život a život musí byť bezpečný aj s ohľadom na spejúcu dobu informatizácie“.

ZÁVER

Bez ohľadu na definíciu pojmu hybridných hrozieb je nevyhnutné, aby každý štát vedel dostatočne reagovať na hybridné útoky konané proti svojim občanom. Legislatíva je nutným základom, mala by zabezpečiť aby bezpečnostné zložky mohli reagovať v čo najkratšom, reálnom čase. Obrana musí byť najefektívnejšia, ktorá je spôsobilá útoku zabrániť, odvrátiť alebo zmenšovať škody, či už na národnej úrovni, alebo v rámci medzinárodnej spolupráce. Veľmi účinnou a lacnou zbraňou proti hybridným hrozbám je vzdelaná, sebavedomá demokratická spoločnosť, ktorá je ochotná brániť demokratické hodnoty aj svoju národnú identitu.

Zdroje

1. MARCHEVKA, P., NÉMETH, L., 2010. *Diskusia k základným pojmom krízového riadenia*. (<http://fsi.umiza.sk>).
2. MILO, D. 2018. *Mapovanie zraniteľnosti SR v oblasti hybridných hrozieb*. GLOBSEC. Bratislava (<https://www.globsec.org/wpcontent/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnychhrozieb-web.pdf>).
3. VOLNER, Š. 2009. *Bezpečnosť, riziká a hrozby 21. storočí*. Bratislava: IRIS, ISBN 978-80-8925-636 5.
4. VOLNER, Š. 2012. *Bezpečnosť, riziká a hrozby 21. storočí*, Bratislava: IRIS, ISBN: 978-80-8925-674 7.

5. Ministerstvo obrany SR. 2016. *Biela kniha o obrane SR. Ministerstvo obrany: Bratislava* (https://www.mod.gov.sk/data/BKO2016_LQ.pdf).
6. Vláda SR. 2018. Konceptia pre boj Slovenskej republiky proti hybridným hrozbám. Bratislava (<https://rokovania.gov.sk/RVL/Material/23100/1>).
7. Európska komisia. 2016. *Spoločné oznámenie Európskemu parlamentu a rade: Spoločný rámec pre boj proti hybridným hrozbám - reakcia Európskej únie. Brusel.* (<https://eurlex.europa.eu/legalcontent/SK/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>)
8. Vojenské rozhledy [online]. 2023. [cit. 2023-04-06].
Dostupnéz:<https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/aktualni-pristupy-hybridni-hrozby>
9. Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
10. Trestný zákon č. 300/2005 Z. z.
11. Zákon o priestupkoch č 372/1990 Z. z.

HYBRIDNÉ HROZBY V SÚČASNOSTI

JUDr. Martina Cíhová, PhD.

Katedra verejnej správy a krízového manažmentu Akadémie Policajného zboru v Bratislave; Sklabinská 1, 835 17 Bratislava; martina.cichova@akademiapz.sk

Abstrakt: Príspevok sa zaoberá hybridnými hrozbami v rámci Slovenskej republiky. Má za cieľ interpretovať všeobecné východiská konceptu hybridných hrozieb a následne pomocou interpretatívnej prípadovej štúdie analyzovať vybraný prípad slovenského politického a spoločenského diania a aplikovať koncept hybridných hrozieb.

Kľúčové slová: hybridné hrozby, indikátory hybridných hrozieb, koncept hybridných hrozieb.

ÚVOD DO PROBLAMETIKY

Bezpečnosť Slovenskej republiky a partnerských krajín, či už zo Severoatlantickej aliancie alebo Európskej únie, je v súčasnosti konfrontovaná so širokou škálou predovšetkým nevojenských bezpečnostných hrozieb, napríklad v podobe medzinárodného terorizmu, nelegálnej masovej migrácie, organizovaného zločinu alebo kybernetických útokov na verejné i súkromné počítačové siete, servery a systémy, atď. Vojenské hrozby, najmä po ruskej anexii Krymu a prepuknutí konfliktu na juhovýchodnej Ukrajine, taktiež nemožno úplne vylúčiť. Nedostatočné riešenie globálnych problémov ľudstva (sociálnych, ekonomických, environmentálnych a bezpečnostných), negatívne následky prehlbujúcej sa globalizácie, zlyhávajúce štáty, finančné, sociálne alebo energetické krízy, ako aj neistota a nestabilita z dôvodu politických, ekonomických, náboženských, teritoriálnych alebo etnických sporov v euroatlantickom priestore alebo v jeho blízkosti zároveň vytvárajú vhodné podmienky pre vznik kríz značného rozsahu s možnosťou prepuknutia do rozsiahleho konfliktu. Keďže vývoj a udalosti z posledných rokov naznačujú, že bude pokračovať stieranie hraníc medzi štátnymi a neštátnymi aktérmi (teroristické, náboženské a nacionalistické organizácie, skupiny organizovaného zločinu a pod.) môžu byť Slovensko a jeho partneri konfrontovaní s protivníkom, ktorý je na dosiahnutie svojich cieľov schopný súbežne a koordinovane využiť kombináciu klasických, konvenčných nástrojov a spôsobov vedenia boja a netradičných, nekonvenčných nástrojov a spôsobov; to znamená s protivníkom, ktorý je schopný viesť voči Slovensku a jeho partnerom hybridnú vojnu.

Vzhľadom na to, že pre hybridnú vojnu je charakteristické, že dochádza k stieraniu hraníc medzi mierom a vojnou, že napadnutý štát alebo spoločnosť nie je schopná rozoznať či ide o vojnu, bezpečnostnú hrozbu alebo len prechodné riziko, identifikovať protivníka a prijať adekvátne a účinné opatrenia, je v rámci obrany pred protivníkom využívajúcim hybridný spôsob vedenia boja absolútne nevyhnutné, aby bola na obranu pripravená celá spoločnosť, nielen ozbrojené sily a ďalšie ozbrojené zložky štátu. Samozrejme, tie, aby mohli splniť svoju časť úloh, musia byť adekvátne tejto hrozbe financované, vyzbrojené, vybavené, vystrojené, pripravené a personálne zabezpečené.

V spoločenskovedných odboroch sa často stretávame s pojmami, ktoré nemajú jednotnú definíciu. Jedným z týchto pojmov sú aj hybridná vojna a hybridné hrozby. Naprieč literatúrou môžeme nájsť celé spektrum autorov s rozdielnym vnímaním tohto fenoménu. Takéto rozdielne vnímanie je však

logické nielen z geografického hľadiska, ale aj z hľadiska historických skúseností a súčasnej bezpečnostnej situácie aktérov.

Termín hybridné hrozby/vojny bol začlenený do bezpečnostného slovníka len nedávno ale kombinácia týchto aktivít sa prejavovala už v historicky, a to napríklad v Peloponézskych vojnách (5. storočie pred našim letopočtom) vo forme asymetrického konfliktu, kde nedochádzalo len k priamym stretom (Lukáčová, 2019). Následne sa ich prvky objavujú v diele Umenie vojny čínskeho filozofa Sun-c a v jeho téze: *„Vojenská dokonalosť nespočíva v obsadení územia nepriateľa použitím brilantnej bojovej stratégie, ale v schopnosti zlomiť nepriateľovu vôľu vzdorovať bez použitia boja“*.

V novodobej histórii môžeme hybridné hrozby alebo ich prvky pozorovať aj v praktikách Nemecka počas druhej svetovej vojny, ktoré používalo nielen politické prostriedky, ale aj propagandu, informačné prostriedky alebo prostriedky ekonomického charakteru.

Označenie hybridná označuje kombináciu už pomenovaných typov vojny ako je konvenčná, nekonvenčná, politická a informačná. Pojem hybridná vojna tak neopisuje nový druh vojny (Kofman – Rojansky, 2015). Moderná vojna je súhrnom rôznych metód, stratégií a nástrojov národných štátov, ktoré môžeme zhrnúť do tzv. „smart power“ (kombinácií nástrojov „hard power“ a „soft power“). Pre dosiahnutie cieľov je vhodné použiť súbor strategických nástrojov ako sú politické, ekonomické, informačné a humanitárne opatrenia, ktoré využívajú tzv. protestný potenciál cieľovej krajiny. To môže byť doplnené intenzívnymi kybernetickými útokmi, skrytou vojenskou intervenciou, psychologickou vojnou či pôsobením súkromných bezpečnostných služieb (Grohmann, 2015). Psychologická vojna zahŕňa aj dezinformácie, mediálnu propagandu, hrozby a psychologické techniky, ktoré sú využívané k zastrašeniu či porazeniu protivníka (Veebel, 2015).

1. DEFINOVANIE POJMU „HYBRIDNÉ HROZBY“

Hybridné hrozby sú koordinované podvratné a vplyvové aktivity pôsobiace súbežne vo viacerých oblastiach spoločnosti, ktorých cieľom je oslabiť či poškodiť daný štát a pomôcť presadiť strategické ciele a záujmy cudzieho nepriateľského štátu či neštátnej skupiny.

V Koncepcii pre boj SR proti hybridným hrozbám z roku 2018, sú hybridné hrozby definované ako *„súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie“*. Na to, aby mohlo ísť o hybridnú hrozbu je potrebné súčasné využitie niekoľkých, najmenej troch druhov nástrojov či aktivít. Takéto hybridné hrozby vo svojom dôsledku polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok. Svojim dopadom majú negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené. Tieto aktivity sú často koordinované, zameriavajú sa na lokálne zraniteľnosti a sú navrhnuté tak, aby aj po ich prípadnom odhalení bolo ťažké určiť kto za nimi stojí, čo sťažuje schopnosť reakcie a adekvátnej odpovede.

1.1 Ako sa hybridné hrozby prejavujú?

Najčastejšie sa s témou hybridných hrozieb spájajú pojmy ako dezinformácie, propaganda, špionáž, kybernetické útoky, vplyvové a informačné operácie, zasahovanie do volieb, strategická korupcia, polovojenské skupiny, alebo energetický a ekonomický nátlak, keďže patria medzi najčastejšie využívané nástroje hybridných hrozieb.

Nástrojov hybridných hrozieb je však oveľa viac a v dokumente Prostredie hybridných hrozieb: Koncepčný model od Spoločného výskumného centra EÚ je ich obsiahnutých až 40. Nie každé využitie jedného z vyššie uvedených nástrojov však automaticky znamená, že sa jedná o prípad výskytu hybridnej hrozby. Hybridnou hrozbou sa stáva až koordinované, centrálné riadené využívanie viacerých nástrojov s rovnakým cieľom rovnakým nepriateľským aktérom. Presadzovanie vlastných ekonomických či geopolitických záujmov v medzinárodných vzťahoch pomocou diplomacie a ostatných „mäkkých“ foriem pôsobenia je bežnou súčasťou vzťahov medzi štátmi. To, čím sa hybridné hrozby líšia od týchto foriem medzinárodnej politiky je úroveň koordinácie medzi rôznymi nástrojmi a najmä cieľ takéhoto pôsobenia, ktorým je ochromenie a rozvrat spoločnosti, či jej bezpečnostných a vládnych štruktúr, ako príprava na vojenský útok, či ako samostatný cieľ.

Najviditeľnejším prejavom hybridného pôsobenia v SR je zámerné vytváranie a šírenie dezinformácií so strategickým zámerom ovplyvniť verejnú mienku obyvateľov SR v prospech záujmov nepriateľských mocností a čoraz častejšie kybernetické útoky na štátne inštitúcie ale i kritickú infraštruktúru.

1.2 Prečo sú hybridné hrozby nebezpečné?

Hybridné hrozby sa v posledných rokoch stali jednou z najdôležitejších tém v oblasti bezpečnosti tak na SR, ako i na úrovni EÚ či NATO. Dôvodom prečo je tejto oblasti prikladaný čoraz väčší význam je zmena spôsobu presadzovania strategických záujmov zo strany nepriateľských aktérov a zvyšujúci sa dopad technológií na všetky oblasti spoločnosti.

Vojny sa v 21. storočí nevyhlasujú, nahrádza ich koordinované využívanie celej palety nástrojov využívajúcich informačné pôsobenie, ekonomický vplyv, energetický nátlak či pôsobenie tajných služieb. Zároveň sa technológie stali neoddeliteľnou súčasťou života celej spoločnosti a s ich využitím dnes dokážu nepriateľskí aktéri pôsobiť kdekoľvek na svete – šíria strategickú propagandu, ovplyvňujú volebné procesy, útočia na kritickú infraštruktúru, prenikajú do počítačových sietí.

Paralelným použitím nátlakových a podvratných činností, konvenčných a nekonvenčných metód (napr. nepriateľská propaganda, podpora extrémizmu, využívanie národnostných alebo náboženských komunit nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru) môžu hybridní aktéri destabilizovať spoločnosť cieľových štátov a oslabiť ich tak, aby boli ľahšie ovplyvniteľné alebo v krajnom prípade aj menej odolné voči použitiu konvenčnej vojenskej sily.

Bezpečnostné prostredie vo svete aj v Európe sa za posledné roky zásadne zmenilo. Dopady celosvetovej pandémie COVID-19, rapidný rozvoj nových technológií ako je umelá inteligencia a

digitalizácia, dôsledky klimatickej krízy na migráciu či potravinovú bezpečnosť alebo ruská vojenská agresia voči Ukrajine to sú len niektoré príklady nedávnych udalostí, ktoré zásadne zmenili svet v ktorom žijeme.

Všetky tieto udalosti, vyvolávajú otrasy a zmeny, ktoré sa dotýkajú všetkých aspektov života. Zároveň tieto zmeny v bezpečnostnom prostredí zásadným spôsobom ovplyvňujú schopnosť Slovenskej republiky zabezpečovať ochranu svojich životne dôležitých a strategických záujmov definovaných v Bezpečnostnej stratégii SR. SR nie je ostrov odtrhnutý od sveta a čelí rovnakým typom hrozieb ako iné členské štáty EÚ a NATO.

1.3 Kto sú aktéri hybridných hrozieb?

Aktérmi hybridných hrozieb sú väčšinou cudzie nepriateľské štáty, ktorých politické či strategické ciele sú v rozpore so životnými a strategickými záujmami SR a organizácií ktorých je Slovensko členom ako sú EÚ či NATO. Najčastejšie sa preto v našich podmienkach pri hybridných hrozbách vyskytujú aktivity Ruskej federácie, ktorá dokonca zaradila SR spolu s ďalšími krajinami EÚ na zoznam nepriateľských krajín a Číny, ktorá využíva primárne ekonomické formy a nástroje. Takéto hodnotenie vyplýva jednak z výročných správ Slovenskej informačnej služby či Vojenského spravodajstva ako aj dokumentov prijímaných na úrovni EÚ a NATO. Hybridnými aktérmi môžu byť aj neštátne subjekty, typickým príkladom je ISIS, ktorý využíval na vrchole svojich aktivít viaceré vzájomne prepojené a koordinované nástroje v oblasti informačných operácií, kybernetických útokov či terorizmu.

2. INŠTITUCIONÁLNY RÁMEC

Zahraničnopolitické smerovanie Slovenskej republiky (ďalej len „SR“) je jasne definované euroatlanticky. Potvrdzujú to aj programové vyhlásenia posledných vlád, teda obdobia, kedy sa hybridné hrozby stali jednou z najdôležitejších tém. Programové vyhlásenie vlády Slovenskej republiky na obdobie rokov 2021-2024 uvádza, že *„Vláda SR vysoko hodnotí členstvo Slovenska v Európskej únii a plne si je vedomá záväzkov v rámci Severoatlantickej aliancie, ktorá je bezpečnostnou zárukou pre našich občanov, že môžu žiť v mieri“*.

Opomenúť však nesmieme ani fakt, že vzťahy SR a Ruska sú reprezentované viacvrstvovým javom, ktorý v sebe zahŕňa nielen históriu, ekonomiku, zahraničnú politiku ale i bezpečnosť. Neochota Slovenskej vlády zapájať sa do otvorenej konfrontácie medzi EÚ a Ruskom, je odrazom verejnej mienky v krajine a na základe vyššie uvedených skutočností, môžeme SR charakterizovať ako krajinu s troma atribútmi vo vzťahu k Rusku. SR má silné historické väzby s Ruskom. Politická rétorika Slovenska je značne proruská = „zmierlivá voči Rusku“. V SR je zaznamenaná rastúca popularita a vznik nových politických síl s proruským svetonázorom a odmietaním euroatlantickej politickej orientácie.

Čo sa týka SR, hybridné hrozby dlhú dobu neboli identifikované ako bezprostredná hrozba. Tento pojem sa prvýkrát objavil v roku 2016, a to v Bielej knihe o obrane SR z dielne MO SR. V bode 56. tohto strategického dokumentu je uvedené, že *„z hľadiska spôsobu vedenia konfliktov v meniacom sa bezpečnostnom prostredí je vážnou bezpečnostnou hrozbou najmä propaganda na strategickej úrovni ako súčasť informačného a psychologického pôsobenia na vybrané cieľové*

skupiny spoločnosti v rámci tzv. informačnej vojny a špecifické operačné postupy, ktoré sú najlepšie charakterizované pojmom, hybridný spôsob vedenia bojových činností“.

Slovenská informačná služba (ďalej len „SIS“) však už vo svojej správe o činnosti za rok 2015 identifikovala aktivity Ruska s propagandistickým charakterom namierené voči západu za jednu z oblastí jej záujmu: *„V kontexte pretrvávajúceho napätia vo vzťahoch RF so Západom venovala SIS pozornosť problematike snáh RF o ovplyvňovanie verejnej mienky v SR a subjektom, ktoré sa na týchto aktivitách aktívne podieľali.“* Pro-kremeľská propaganda sa stala podľa MO SR bezpečnostným rizikom a bola identifikovaná za jednu z hybridných hrozieb v roku 2016. Dôvodom, prečo je považovaná za hrozbu je to, že vytvára a podporuje informačné kanály a s nimi spojené subjekty, ktoré *„šíria proruský naratív a spochybňujú hodnotové zakotvenie Slovenska v euroatlantickom priestore“*. Toto znenie sa premietlo aj do Koncepcie SR na boj proti hybridným hrozbám, v ktorej stojí: *„Súčasne pôsobiace aktivity, ktoré ohrozujú základné atribúty štátu alebo ich funkčnosť, sa označujú ako hybridné hrozby. Hybridná hrozba je definovaná ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie.“* Sú realizované aktivitami charakterizovanými centrálnou riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené.

Definovanie inštitucionálneho rámca pre reakciu SR na hybridné hrozby vychádza z nutnosti kooperácie zainteresovaných subjektov založenej na realizácii opatrení v rámci vlastnej pôsobnosti smerujúcej k pružnej výmene informácií a koordinácii postupov. Nastavenie musí dať možnosť reagovať na hybridné hrozby rýchlo, odborne a flexibilne s využitím základných indikátorov hybridných hrozieb:

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- rozsiahle sabotáže proti kľúčovej infraštruktúre;
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely;
- hrozba použitia vojenskej sily;

Uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu. Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.

Definícia hybridných hrozieb by mala však zostať dostatočne pružná, aby primerane reflektovala na vývoj hrozieb. Vo svojej podstate je to však súbor koordinovaných činností alebo metód ktoré pôsobia destabilizačne a oslabujúco voči svojim protivníkom resp. aktérom proti ktorým majú byť využité bez jednoznačného vyhlásenia vojny v “de jure” kontexte.

3. ORGANIZÁCIA NOČNÍ VLCI

V lete 2018 sa v médiách objavila informácia o zriadení základne ruskej nacionalistickej organizácie Noční vlci na Slovensku v obci Dolná Krupá, neďaleko Bratislavy. Táto informácia sa dostala aj do zahraničia, keď o nej písala aj britská BBC. V základni sa podľa snímok z dronov nachádzali obrnené vozidlá a tanky, ktoré však podľa následných informácií polície neboli schopné streľby. V čele slovenskej pobočky stojí Jozef Hambálek (ČT 24, 2018).

Pohľady najdôležitejších politických predstaviteľov na tento prípad boli rôzne. Najkritickejší postoj zaujal prezident Andrej Kiska nazval Nočných vlkov „*nástrojom režimu, ktorý sa podieľa na okupácii susednej krajiny*“ (Webnoviny, 2018). Kisku však za tento prístup skritizoval premiér Pellegrini. Podľa neho to nie je Kiska, ale policajné orgány a generálna prokuratúra musia rozhodnúť o tom, či sú Noční vlci bezpečnostným rizikom pre Slovensko alebo nie (SME, 2018). Hovorca slovenského ministerstva zahraničných vecí Peter Susko sa zas vyjadril kriticky, no taktiež opatrne. Pre BBC povedal, že aktivity Nočných vlkov budú musieť byť „*starostlivo monitorované, pričom si ministerstvo myslí, že vplyv ich členov je škodlivý, najmä pri šírení ich názorov, ktoré sa snažia prepísať históriu*“ (BBC, 2018). Predseda Národnej rady SR Andrej Danko zas nemal informácie o bezpečnostných rizikách Nočných vlkov (Webnoviny, 2018). V budúcnosti sa však ukázalo, že Danko nemal problém s Nočnými vlkami. Noční vlci pozvali našich poslancov do svojho klubu počas ich služobnej cesty v Rusku na prelome júna a júla tohto roka. Na otázku, či by prijal toto pozvanie, najskôr odpovedal, že v rovnakom čase mal naplánované stretnutie s ruským ministrom obchodu a priemyslu Denisom Manturovom, no neskôr pripustil, že takéto pozvanie by mohol prijať (Aktuality, 2019).

V slovenskom prostredí sa dovtedy o Nočných vlkoch písalo predovšetkým v rámci ich spomienkových jázd po osi Moskva-Berlín, čím si pripomínali víťazstvo nad fašizmom. Aby príspevok priblížil pozadie organizácie, budú použité články “Wolves of the Russian Spring: An Examination of the Night Wolves as a Proxy for the Russian Government” od Matthewa Laudera (2018), ktorá vyšla v časopise Canadian military journal a Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club od Kiry Harris z časopisu Studies in conflict and terrorism. Noční vlci sú podľa Laudera (2018) len časťou rozsiahlej siete mimovládnych organizácií, vojenských združení a a súkromných podnikov, ktoré pracujú na príkaz ruskej vlády. Sú taktiež príkladom tendencií ruskej vlády zadávať neštátnym subjektom činnosti, ktoré tradične vykonávajú štátne spravodajské a obranné jednotky. Medzi tieto externe zabezpečované činnosti patria okrem iného: zhromažďovanie spravodajských informácií, šírenie propagandy, agitácia a provokácie, bojové operácie a násilie šité na mieru, vrátane zastrašovania a cieleného atentátu (Lauder, 2018).

Zmena nastala po tom, čo vedenie Nočných vlkov prevzal začiatkom 90. rokov Alexander Zaldostanov, známy ako „Chirurg“. Skupina počas tohto obdobia prešla počiatočnou transformáciou z anti-systémového motorkárskeho klubu na organizáciu s vlasteneckými sklonmi. V auguste 1991 bránili Noční vlci Kremľ proti pokusu o prevrat komunistami, za čo dostal Zaldostanov medailu od vtedajšieho prezidenta Borisa Jeľcina. Vladimir Putin udelil taktiež

Zaldostanovovi medailu Rád cti za prácu v oblasti patriotického vzdelávania mládeže a za zachovávanie odkazu padlých z Veľkej vlasteneckej vojny. Zaldostanov v rámci propagácie olympiády v Soči 2014 slúžil aj ako jeden z nosičov olympijského ohňa a vlajka Nočných vlkov sa objavila v ruskej časti Medzinárodnej vesmírnej stanice (Lauder, 2018).

Noční vlci taktiež zohrávali malú, ale dôležitú úlohu vo vojenskej operácii Ruskej federácie na Kryme. Pred príchodom Zaldostanova do Simferopolu 28. februára 2014 slúžili členovia miestnej „jednotky“ Nočných vlkov „Sevastopol Night Wolves“ ako podpora ruskej armády. Aktivity počas tohto obdobia zahŕňali zhromažďovanie spravodajských informácií, distribúciu propagandy, organizovanie protestov a jednotiek domobrany a taktiež koordináciu s ruskými špeciálnymi operáciami. Po príchode ruskej armády sa stali Noční vlci oveľa viac zapojenými do vojenských operácii koordináciou blokov ciest a zameraní sa na zastrašovanie miestnych úradníkov. Známe je aj ich zapojenie v následných bojoch na východe Ukrajiny. Je dôležité podotknúť, že Noční vlci boli len jedným z dvoch neštátnych aktérov s povolením vykonávať ozbrojené operácie (Lauder, 2018).

Schopnosť Ruska integrovať Nočných vlkov ako jednu z politických síl demonštruje Putinovu flexibilitu vo vojne spolu s podporou nacionalizmu. Zjednotením sa Nočných vlkov behom ruských útokov na Ukrajinu sa výrazne zvýšila ich domáca popularita a viedla k uznaniu v medzinárodnom meradle. Vayts zdôrazňuje entuziazmus a schopnosť členov Nočných vlkov pôsobiť mimo vládnych štruktúr, čo je kľúčom k ich úspechu pri propagácii ich ideológie. Propagácia Kremľa Nočnými vlkami v kombinácii s ich „hyper-maskulinnou“ identitou a bojovými schopnosťami predstavuje hrozbu pre sovietske štáty. s významnou ruskou populáciou (Harris, 2020).

Klingová (2019) hovorí o Nočných vlkoch v súvislosti s polovojenskými a extrémistickými skupinami. Podľa nej „extrémistické a polovojenské skupiny predstavujú nebezpečenstvo pre stabilitu a bezpečnosť spoločnosti nielen ako priame ohrozenie bezpečnosti a demokratického usporiadania spoločnosti ich protiprávnymi aktivitami, ale aj šírením propagandy a dezinformácií ako dôveryhodný sprostredkovateľ postojov inšpirovaných alebo priamo preberaných od cudzích štátnych aktérov“.

Analytik Daniel Milo z GLOBSEC Nočných vlkov taktiež vidí ako predĺženú ruku Kremľa a vyzýva k obozretnosti, dodáva však, že si nemyslí, že by na Slovensku vznikala základňa s bojovými vozidlami (Denník N, 2018).

4. APLIKÁCIA KONCEPTU HYBRIDNÝCH HROZIEB

Pôvodcom činnosti je štát, prípadne neštátny aktér spolupracujúci so štátnou mocou. Zahraničné analytické práce ohľadne organizácie Noční vlci celkom jednoznačne odpovedali na to, že existuje prepojenie medzi organizáciou a Kremľom. Na druhej strane neexistuje priamy dôkaz toho, že všetky ich aktivity, konkrétne aktivity na území SR Kremľ koordinuje v záujme dosiahnutia svojich vlastných strategických cieľov.

V rámci činnosti vonkajšieho aktéra dochádza k polarizácii spoločnosti a následnému destabilizovaniu usporiadania štátu v štruktúrach NATO a EÚ. Z tohto pohľadu jasne vyplýva, že najvyšší predstavitelia SR nenašli v tomto prípade spoločnú reč a každý z nich reagoval iným spôsobom, čo môže mať neskorší dopad na politickú stabilitu v krajine. Na druhej strane nevidím

v tomto prípade priame následky, ktoré by mali dopad na ukotvenie SR v euroatlantických štruktúrach. Faktom však zostáva, že prehľbovanie aktivít Nočných vlkov vo vzťahu k obyvateľstvu môže mať v dlhodobom časovom horizonte vplyv na verejnú podporu súčasného smerovania zahraničnej politiky. Je jasné, že v tomto bode dochádza aj k polarizácii spoločnosti. Na jednej strane tu máme pohľady bezpečnostných analytikov a tzv. Mainstreamových médií, ktoré považujú pôsobenie Nočných vlkov za bezpečnostnú hrozbu. Na druhej strane je na Slovensku významná skupina obyvateľstva, ktorá inklinuje k proruským myšlienkam, čo podporujú aj prokremeľsky naladené médiá.

Milo (2018) vidí problém aj v nejasnom legislatívnom ukotvení organizácie. Podľa neho „postavenie polovojenských skupín nie je v slovenskom právnom poriadku presne vymedzené a v slovenskej legislatíve neexistuje definícia polovojenskej/paramilitárnej skupiny. Jediné významné obmedzenie a sankcie sa týkajú účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu“ (Milo, 2018).

Prípád pôsobenia Nočných vlkov môžeme analyzovať z pohľadu dvoch indikátorov hybridných hrozieb:

- **Externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;**

Čo sa týka politického nátlaku na predstaviteľov štátu, ten neprišiel priamo od organizácie Noční vlci. Na druhej strane vznikol spolu s touto situáciou po rozsiahlej medializácii prípadu nátlak zo strany verejnosti. Aj napriek pevne ukotvenej zahranično-politickej orientácii SR sa najvyšší štátni predstavitelia vo svojich reakciách nezhodli, v niektorých prípadoch až stáli proti sebe, čo môže prameniť z vnútro politickej polarizácie SR a rozdielnej voličskej základne jednotlivých predstaviteľov.

Ako už bolo povedané, v dlhšom časovom horizonte môže takáto polarizácia spôsobiť oslabenie dôvery v zahranično-politické smerovanie SR a zároveň oslabiť dôveru voči SR zo strany zahraničných partnerov.

- **Informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu“;** Prítomnosť propagandy zo strany Nočných vlkov je zrejmá aj smerom k domácomu obyvateľstvu, kde dominuje nacionalizmus, tak aj k ľuďom v zahraničí prostredníctvom všeslovanskej vzájomnosti, alebo hrdinstva ruského národa pri oslobodzovaní Európy od fašizmu. Noční vlci preukázali svoju schopnosť mobilizovať nacionalistickú náladu v Rusoch, interne aj v zahraničí prostredníctvom propagandy. Zatiaľ čo korene motocyklového klubu sú podobné západným náprotivkom ako Hells Angels MC a Bandidos MC, vyvinuli sa v podnik s ideologickým vplyvom. Známe sú aj ich proruské predstavenia na Kryme, ktoré fungujú ako kampaň mäkkej propagandy s cieľom propagovať protizápadné názory a hlásať myšlienku proruského nacionalizmu (Harris, 2020).

Vyššie už bolo spomenuté, že na Slovensku sú Noční vlci známi z ich ciest po ose Moskva-Berlín, počas ktorej si pripomínajú víťazstvo Ruska nad fašizmom spojeným so šírením proruských myšlienok a myšlienok všeslovanskej vzájomnosti. Spravodajský web Hlavné správy, ktorý je zaradovaný medzi médiá šíriace prokremeľskú propagandu publikoval v

čase riešenia kauzy slovenskej základne niekoľko oslavných reportáží o jazde Nočných vlkov po Bielorusku. V článkoch referoval, ako motorkárov všade vítajú, ako sa s nimi zdravia vojnoví veteráni, aké darčeky preberá ich vodca Alexander „Chirurg“ Zaldostanov (Denník N, 2018). Situácia je neprehľadná, čím sa znižuje schopnosť obete adekvátne zareagovať. Táto otázka v tomto prípade opäť súvisí z neschopnosťou predstaviteľov SR rýchlo a koordinovane reagovať čo i len na spôsob, akým sa má SR k tomuto prípadu postaviť. Koordinovaná a spoločná reakcia je teda v tomto prípade značne obmedzená.

Vzhľadom k obrovskej polarizácii, ako v spoločnosti, tak aj na politickej scéne neexistuje jednotný názor na to, ako na daný prípad reagovať. Rovnako je problémom aj nedostatočná legislatíva, ktorá by upravovala tento prípad.

ZÁVER

Na základe analyzovaných dát pôsobenie organizácie Noční vlci na území SR spĺňa znaky hybridného spôsobu boja a môže byť preto považované za hybridnú hrozbu. Jej intenzita aj naďalej zostáva predmetom diskusie. Faktom však zostáva, že organizácia je úzko napojená na Kremľ, pričom niektorí členovia pôsobili aj vo vojne na východe Ukrajiny. Organizácia je rovnako schopná využívať slabé miesta, ako je polarizovaná spoločnosť, alebo nedostatočná legislatíva. Jej priame zapojenie v podkopávaní zahranično-politickej orientácii SR však nemôžeme s určitosťou potvrdiť, jej činnosť však vykazuje znaky propagandy a šírenia proruského naratívu, čo sa môže prejaviť v dlhodobom časovom horizonte. Vďaka pôsobeniu na zraniteľné miesta v slovenskej bezpečnosti je možnosť reakcie obmedzená.

Zdroje

1. AKTUALITY. 2019. Dankov obdiv ku Kremľu ukázali aj jeho cesty. V Rusku strávil najviac dní. Aktuality.sk, 8.9.2019 [online]. [cit. 20.10.2023] Dostupné na: <https://www.aktuality.sk/clanok/718970/volby2020-danko-cesty-rusko/>.
2. BBC. 2018. Slovakia alarmed by pro-Putin Night Wolves bikers' base. Bbc.com, 31.7.2018 [online]. [cit. 20.10.2023] Dostupné na: <https://www.bbc.com/news/world-europe-45019133>.
3. ČT24. 2018. Noční vlci dostali na Slovensku k dispozíci tanky. Ředitel vojenského ústavu je kvůli tomu mimo službu. Ct24.cz, 31.7.2018 [online]. [cit. 20.10.2023] Dostupné na: (<https://ct24.ceskatelevize.cz/svet/2544958-nocnivlci-dostali-na-slovensku-k-dispozici-tanky-reditel-vojenskehoustavu-je-kvuli>).
4. DENNÍK N. 2016. Štát prvýkrát priznal, že ruská propaganda útočí na prozápadné smerovanie Slovenska. Dennikn.sk, 8.6. 2016 [online]. [cit. 20.10.2023] Dostupné na: <https://dennikn.sk/481082/stat-prvykrat-priznal-ze-ruskapropaganda-utoci-prozapadne-smerovanie-slovenska/>.
5. GROHMANN, J. 2015. Hybridní války podle Valerije Garasimova. [online]. [cit. 12.3.2023] Dostupné na: <https://www.armadninoviny.cz/hybridni-valky-podle-valerije-gerasimova.html?hledat=hybridni+valky>
6. HARRIS, K. 2020. Russia's fifth column: The influence of Night Wolves Motorcycle Club. Studies in Conflict and Terrorism [online]. [cit. 20.10.2023] Dostupné na: https://www.researchgate.net/publication/323948657_Russia's_fifth_column_The_influence_of_Night_Wolves_Motorcycle_Club.

7. KLINGOVÁ, K. 2019. Hybridné hrozby na Slovensku. Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach GLOBSEC. Bratislava. [online]. [cit. 20.10.2023] Dostupné na: <https://www.globsec.org/wpcontent/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnychhrozieb-web.pdf>.
8. KOFMAN, M. – ROJANSKY, M. 2015. A Closer look at Russia's "Hybrid War". [online]. [cit. 20.10.2023] Dostupné na: <https://www.files.ethz.ch/isn/190090/5-kennan%20cable-rojansky%20kofman.pdf>.
9. KONCEPCIA SLOVENSKEJ REPUBLIKY PRE BOJ PROTI HYBRIDNÝM HROZBÁM SCHVÁLENÁ VLÁDOU SR dňa 11. júla 2018 uznesením č. 345/2018, 2018. [online]. [cit. 20.3.2023] Dostupné na: <http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=27668>
10. LAUDER, M. 2018. Wolves of the russian spring - an examination of the night wolves as a proxy for the russian government. Adversarial Intent. [online]. [cit. 20.10.2023] Dostupné na: https://www.researchgate.net/publication/331668105_Wolves_of_the_russian_spring_an_examination_of_the_night_wolves_as_a_proxy_for_the_russian_government_-_2018.
11. LUKÁČOVÁ, A. 2019. Hybridné hrozby a ich vplyv na bezpečnostné prostredie - teória, vývoj, prax. Vojenské reflexie. Liptovský Mikuláš: Akadémia ozbrojených síl M.R. Štefánika. [online]. [cit. 12.3.2023] Dostupné na: http://vr.aos.sk/images/dokumenty/archiv_cisel/2020/vojenske_reflexieXV_1.pdf.
12. MILO, D. 2018. Mapovanie zraniteľnosti SR v oblasti hybridných hrozieb. GLOBSEC. Bratislava. [online]. [cit. 20.10.2023] Dostupné na: <https://www.globsec.org/wpcontent/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnychhrozieb-web.pdf>.
13. MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY. 2016. Biela kniha o obrane Slovenskej republiky. [online]. [cit. 20.3.2023] Dostupné na: http://www.mod.gov.sk/data/BKO2016_LQ.pdf
14. SME. 2018. Slovensko a Rusko si budú uznávať vysokoškolské diplomy. Sme.sk, 13.11.2018. [online]. [cit. 20.10.2023] Dostupné na: <https://domov.sme.sk/c/20695304/slovensko-rusko-duma-parlamentnyvybor-danko-volodin.html>.
15. VEEBEL, V. 2015. Russian propaganda, disinformation and Estonia's experiences. [online]. [cit. 12.3.2023] Dostupné na: https://www.files.ethz.ch/isn/194051/veebel-russian_disinformation.pdf
16. WEBNOVINY. 2018. Kiska označil Nočných vlkov za bezpečnostné riziko pre Slovensko, vyjadril sa aj k únosu Vietnamca. Webnoviny.sk, 31.7.2018 [online]. [cit. 20.10.2023] Dostupné na: <https://www.webnoviny.sk/prezident-andrej-kiska-sa-vyjadri-k-aktualnym-temam/>.

SEMI-AUTOMATED VULNERABILITY ASSESSMENT IN LORAWAN NETWORKS

Pavel Čičák, Katarína Kochanová, Patrik Sabol, Alexander Valach, Ladislav Zemko

Faculty of Informatics and Information Technologies, Slovak University of Technology, pavel.cicak@stuba.sk, xkochanovak@stuba.sk, xsabol@stuba.sk, alexander.valach@stuba.sk, ladislav.zemko@stuba.sk

Abstract: LoRa and LoRaWAN are popular and probably the most successful wireless communication technologies used in the Internet of Things area. With an increasing interest of attackers in Internet of Things devices, it is necessary to perform vulnerability assessments regularly. However, there is currently no suitable tool for the vulnerability assessment of LoRaWAN networks. This paper explains the basics of LoRa modulation and LoRaWAN protocol. It focuses on the security aspects, vulnerabilities, and possible attacks. The paper proposes a solution for semi-automated vulnerability assessment using custom end node firmware and a web application responsible for attack initiation and evaluation.

Keywords: LoRa, LoRaWAN, Security, Vulnerability Assessment.

INTRODUCTION

LoRa and LoRaWAN are emerging wireless communication technologies that have gained significant attention in recent years. They are designed to enable long communication range and low power communication for IoT¹²⁸ applications. This type of network is known as the LPWA¹²⁹ network. However, as with any wireless communication technology, security is a critical concern.

In this paper, we explore the security aspects of LoRa and LoRaWAN, focusing on potential attacks such as Replay Attacks and Eavesdropping. We also conduct a vulnerability assessment of LoRaWAN using a threat modeling approach, analyzing the system's design and identifying potential vulnerabilities that could be exploited by attackers.

The paper is organized as follows. Section 1 provides a brief insight into the LoRa technology and LoRaWAN protocol. Section 2 discusses existing vulnerabilities in LoRaWAN networks. Section 3 focuses on existing solutions and analyses them. Section 4 describes the proposed solution, and Section 5 concludes the paper.

LoRa and LoRaWAN

LoRa is a RF¹³⁰ modulation technology. The name, LoRa, is a refer to the long-range data links this technology enables. Instead of wire, air is used as a transmission medium for transporting LoRa radio waves from an RF transmitter in an IoT device to an RF receiver in a Gateway, and vice versa [1].

¹²⁸ Internet of Things

¹²⁹ Low-power Wide-area

¹³⁰ Radio Frequency

The LoRaWAN is a LPWA networking protocol designed to wirelessly connect battery-operated "things" to the Internet [1]. By the term "things" in the IoT, we usually mean End Nodes, designed to perform one specific function, or they can be also combined. They are most often divided into sensors, which measure physical values from the environment and convert them into digital form, and actuators, which are used to interact with their surroundings, thereby enabling them to perform and manage selected activities [2].

The LoRa networks consist of four basic elements [3]:

- **End nodes.** Sensors or actuators send LoRa-modulated wireless messages to the Gateways or receive messages wirelessly back from the Gateways.
- **Gateways.** Receive messages from End Devices and forward them to the Network Server.
- **Network Server.** Manages the entire network devices, receives uplink messages from all Gateways, and deduplicates them. It also validates the integrity of every message and then forwards it to the appropriate Application Server.
- **Application Server.** Is responsible for securely processing application data received from End Nodes. Application Server can send downlink messages back to End Node via Network Server and Gateways.

End Node Activation

When a device joins the network (this is called a join or activation procedure), an AppSKey¹³¹ and a NwkSKey¹³² are established. The NwkSKey is shared with the network, while the AppSKey is kept private. These session keys are used for the session duration [4].

The NwkSKey is used by the End Node and Network Server to calculate and verify the MIC¹³³ of all data messages to ensure message integrity. It is also used to encrypt and decrypt payloads carrying MAC¹³⁴ commands. The AppSKey is used to encrypt and decrypt application payloads in data messages to ensure message confidentiality [5].

These two session keys (NwkSKey and AppSKey) are unique per device and session. If a device is dynamically activated (OTAA¹³⁵), these keys are re-generated on every activation, e.g. device restart. If a device is activated statically (ABP¹³⁶), these keys stay the same until they are manually changed by the administrator [4].

The End Node activation routine was (before specification v1.1) previously handled by the Network Server. In LoRaWAN specification v1.1, a component called Join Server was introduced primarily for security reasons to separate the entity that stores both AppSKey and NwkSKey. Join Server then distributes AppSKey to appropriate Application Server and NwkSKey to Network Server. As the Network Server does not have AppSKey, it cannot decrypt the application data of any End Node [5].

¹³¹ Application Session Key

¹³² Network Session Key

¹³³ Message Integrity Code

¹³⁴ Medium Access Control

¹³⁵ Over-The-Air Activation

¹³⁶ Activation by Personalization

Attacks in LoRaWAN Network

Due to the wireless nature of communication in the LoRaWAN network, it is possible to perform several attacks, which can cause denial of service, or affect integrity and confidentiality. In this section, we generally describe attacks, which you can perform on LoRaWAN Networks. Examples of common techniques include ACK¹³⁷ spoofing, bit-flipping, jamming, eavesdropping, and replay attacks [6] [7] [8] [9]. In the following section, we will focus on eavesdropping and replay attacks in more depth.

Eavesdropping

LoRaWAN implements channel confidentiality through AES¹³⁸ in CTR¹³⁹ mode. Instead of setting the counter as a nonce, the packet counter value is used as input. As during a reset, this counter value is reset according to the specification while the key remains in place, this means that the block cipher will recreate the same key material. This is the classic textbook case of a key stream reuse [6].

Given two messages encrypted under the same keystream, an adversary could eliminate the secret key as shown in the following equation [6]:

$$\begin{aligned}P_1 \oplus K &= C_1 \\P_2 \oplus K &= C_2 \\C_1 \oplus C_2 &= (P_1 \oplus K) \oplus (P_2 \oplus K) \\C_1 \oplus C_2 &= P_1 \oplus P_2 \oplus (K \oplus K) \\C_1 \oplus C_2 &= P_1 \oplus P_2\end{aligned}$$

This attack exploits that a block cipher in counter mode is not secure if the counter value is allowed to repeat. Specifically, the case of a monotonically increasing counter value is the classic example of how CTR mode can fail in practice given volatile memory [6]. In this attack, a third party gets access to the communication, and thus confidentiality is violated.

Replay Attack

Replay Attack is a type of security attack based on re-sending the valid messages by the attacker. The main purpose is tricking the device by using handshake or previously stored messages. In LoRaWAN it is not possible to decrypt message payload without the AppSKey, since the entire payload is encrypted. The manipulation of data will result in MIC check fail, however the attacker can resend the messages, using the frame counters defined in LoRaWAN specification. Despite the fact that this type of attack can be easily detected and affected messages can be discarded, handling of frame counters is not addressed in the LoRaWAN specification. Instead, it is left up to the specific application and developer. Therefore, networks that do not keep track of the frame counter value can be vulnerable [6].

¹³⁷ Acknowledgment

¹³⁸ Advanced Encryption Standard

¹³⁹ Counter

The ABP-activated end nodes use static keys which are programmed into the device. Moreover, the protocol specification v1.0.2 states: “After a JoinReq - JoinAccept message exchange or a reset for a personalized end node, the frame counters on the end node and the frame counters on the Network Server for that specific device are reset to 0.” [10] Therefore, after reset, an ABP-activated end node will reuse the frame counter value from 0 with the same keys. In this case, an attacker can store messages from the recent session with larger counter values and reuse them in the current session [6].

Related Work

Analysis revealed, there is currently no suitable tool for vulnerability assessment in LoRaWAN networks. However, several papers [6] [9] [8] [7] discuss LoRaWAN vulnerabilities, conduct experiments, perform attacks, and discover the vulnerabilities.

There are several tools for vulnerability assessment, but not specifically for LoRa. We will further discuss 2 of them - OWASP¹⁴⁰ ZAP and Burp Suite. They are capable of scanning vulnerabilities in general.

OWASP ZAP

OWASP ZAP is one of the flagship projects of the OWASP organization, which is an open-source scanner for finding security vulnerabilities in web applications. Detected vulnerabilities are presented along with a description, number, and location of occurrence, and a suggested action. In addition, it generates a detailed report of the performed tests [11].

Burp Suite

Burp Suite is a PortSwigger product for advanced application security testing. There are three editions available: Community, Enterprise, and Professional. An extensive security scanner allows you to adjust the configuration of the tests carried out by the user. For each discovered vulnerability, several parameters are reported, e.g., number and location of occurrence, type of problem, and severity level. After the verification completion, the user can generate a report [11].

Vulnerability Assessment Tool for LoRaWAN Network

To provide a semi-automated vulnerability assessment for the LoRaWAN network, we propose our solution consisting of 2 main complementary components:

- Custom end node firmware capable of performing the attacks,
- Web Application capable of initiation and evaluation of attacks performed.

Solution Architecture

The proposed solution is based on the standard LoRa network. We decided to use an open-source ChirpStack solution, including a Network server and Application server suitable for our use case [12].

¹⁴⁰ Open Worldwide Application Security Project

The architecture is shown in Figure 1. It is possible to connect several Application Servers to a LoRaWAN network. We decided to create a separate Application Server for the attacker and the victim. Our system for vulnerability assessment will be connected to the attacker's Application Server to perform attacks. The connection with the victim's Application Server will only serve the purposes of attack evaluation. Thus, the attack can be performed even without connection with the victim's Application Server. The evaluation itself will be performed by the Web Application, whereas the end node will only provide data necessary for the evaluation.

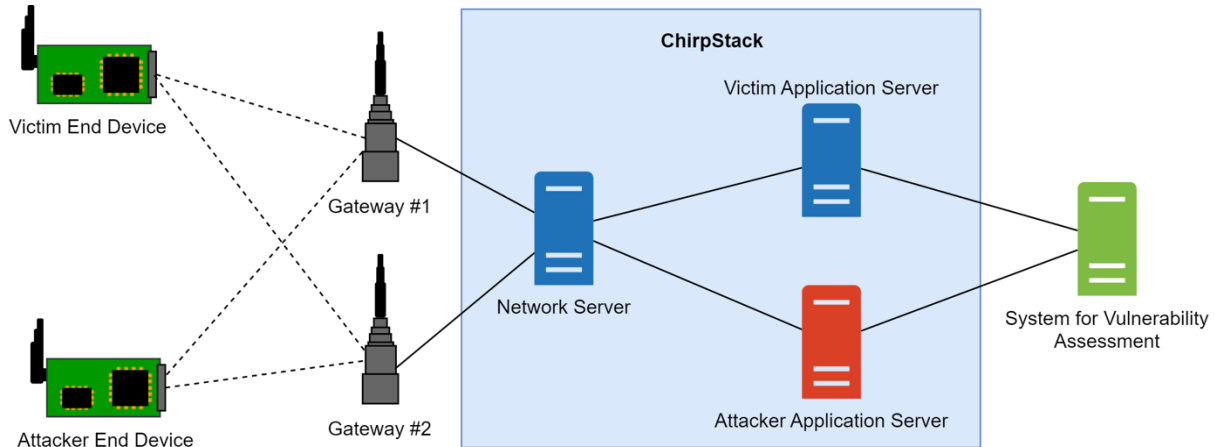


Figure 1 Solution Architecture

Attacks Implementation

Attacks are performed by end nodes. From the hardware perspective, we decided to use LilyGO TTGO LoRa32 T3_V1.6 868MHz, based on the ESP32 microcontroller. Currently, there is a large number of freely available libraries compatible with ESP32, which makes prototyping easier [13].

From the software point of view, the solution is based on the LMIC-node library [14]. It provides a functional and extensible implementation of LoRa frames reception and transmission. It also enables the user to manually set the values necessary for OTAA activation and is compatible with the ChirpStack solution.

To simulate attacks, we need at least two end nodes - one for an attacker and one for a victim. In section 2 several attacks on LoRaWAN networks were described. We decided to implement Eavesdropping, as it is the only attack that threatens confidentiality. Bit-flipping threatens integrity but the attacker would have to hijack the session between Network Server and Application Server or own the malicious Network Server itself. As we decided to use ChirpStack as both an Application and Network Server, it is not possible to implement a Bit-Flipping attack. The rest of the attacks are threatening the availability, so we also selected the Replay Attack as a second representative.

For most applications, the end node is a sensor that digitizes physical conditions and environmental events. Therefore, our victim device simulates the normal operation of the sensor and sends data to its Application Server at regular time intervals (in our case every 30 seconds).

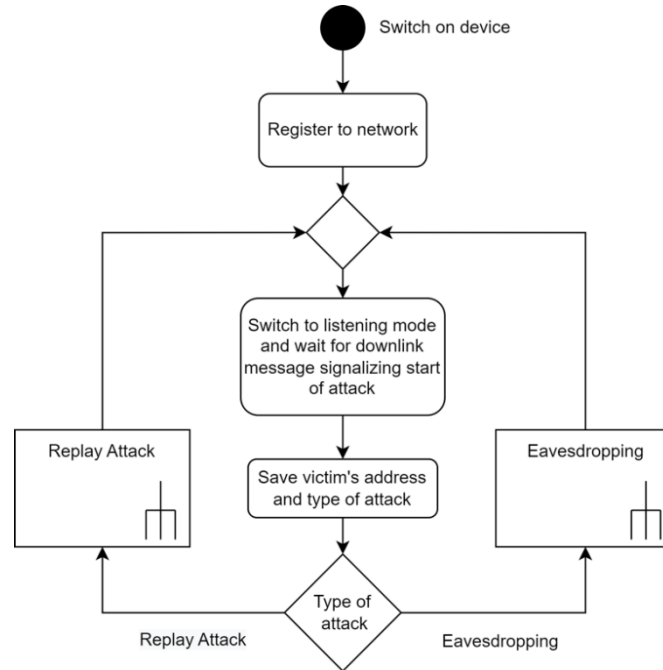


Figure 2 Attacker's End Node Routine

The attacker's device acts as an actuator. The diagram of its routine is shown in Figure 2. After switching on the device and registering it to the network, it switches to listening mode and waits for a downlink message to execute an attack routine. This downlink message contains the address of the victim and the type of attack. The device stores the victim's address in its memory and, based on the type of attack, starts the Replay Attack or Eavesdropping process. After the attack execution, the device returns to the listening state, waiting for a command from the Web Application.

Replay Attack

In a replay attack, the attacker's device captures and stores frames transmitted by the victim. To achieve this, the device first initializes an empty array of frames.

Every message sent by the End Device contains the FCnt¹⁴¹ field in the header, which is incremented with every transmitted message. The Network Server keeps track of the last FCnt value received from the end node. If the difference between the last and current FCnt value is larger than MAX_FCNT_GAP, any subsequent frames are discarded [6].

We defined the variable Gap = 10 000 for the attack, the meaning of which we describe in the following attack example (the value must be less than or equal to the MAX_FCNT_GAP parameter, the value was selected to simplify calculations).

Assume that at the beginning of the attack, the victim's device is sending messages and its current FCnt value is less than 10 000. After a certain time of transmission, the counter of the victim's device reaches 65 535 and resets back to 0. At that very moment, the attacker's device has the victim's frames stored in its frame field with FCnt values of 10 000, 20 000, 30 000, 40 000, 50

¹⁴¹ Frame Counter

000, 60 000, and 65 535. Then, if a well-timed playback of these seven frames takes place, the attacker's device can disable the victim's device, theoretically forever. As soon as the attacker captures a new frame of the victim with FCnt = 0, the next frame can be replayed by the frame with counter value FCnt = 10 000, which at the same time terminates the ongoing attack, because the goal of this scenario was only to disable the victim's end node temporarily, not forever.

If the value of the victim's FCnt counter is at the beginning, for example, 63 000, then after the counter's reset, the attacker's device would have stored frames with FCnt values of 63 000 and 65 535. In this case, in our implementation, the attacker would not be able to disable the device forever, but that is not the goal. After the reset, when a frame with FCnt = 53 000, the attacker would replay a frame with a value of FCnt = 63 000, thereby also achieving a temporary denial of service.

The value Gap = 10 000 is only illustrative for our testing purposes. This value will be set as a parameter, like the attack type and the victims's address, since different networks can have different MAX_FCNT_GAP values.

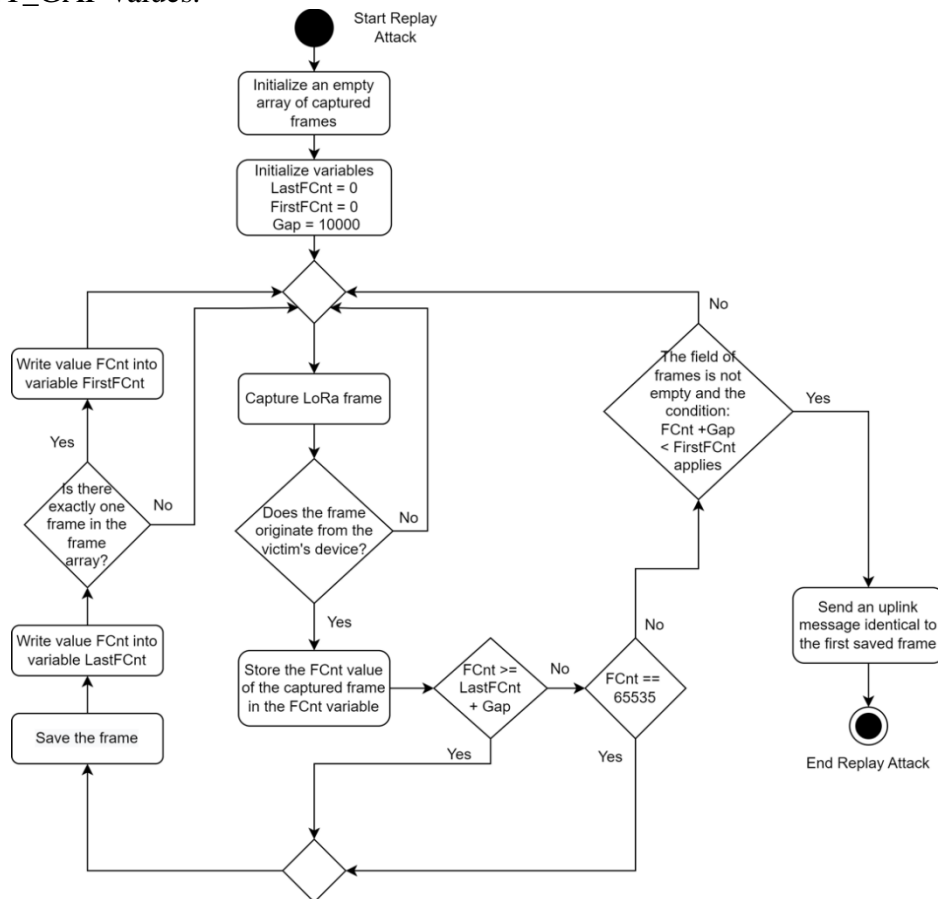


Figure 3 Replay Attack Implementation

This replay attack process is generally described by the diagram in Figure 3. For better readability, the following variables were used:

- **FCnt.** Frame counter value of the currently captured victim frame.
- **FirstFCnt.** FCnt value of the first stored frame.
- **LastFCnt.** FCnt value of the last stored frame.

Eavesdropping

Eavesdropping is a very simple attack. Similarly to the replay attack, the attacker's device needs to intercept all transmitted LoRa frames. If it detects a frame sent by the victim's device, it forwards its data and FCnt value to the appropriate application server, as shown in Figure 4. If the frame is intended for the attacker's device, the attack is terminated.

Unlike the replay attack, the eavesdropping attack can run for an arbitrary length of time and needs to be stopped manually, sending a downlink message. This is because we want to perform eavesdropping to recover the plaintext from the ciphertext via exploiting Key Stream Reuse. The more resets occur, the greater the probability of recovering the original unencrypted message content [6]. Therefore, theoretically, we want to run the attack long enough to increase the chance of recovering the ciphertext.

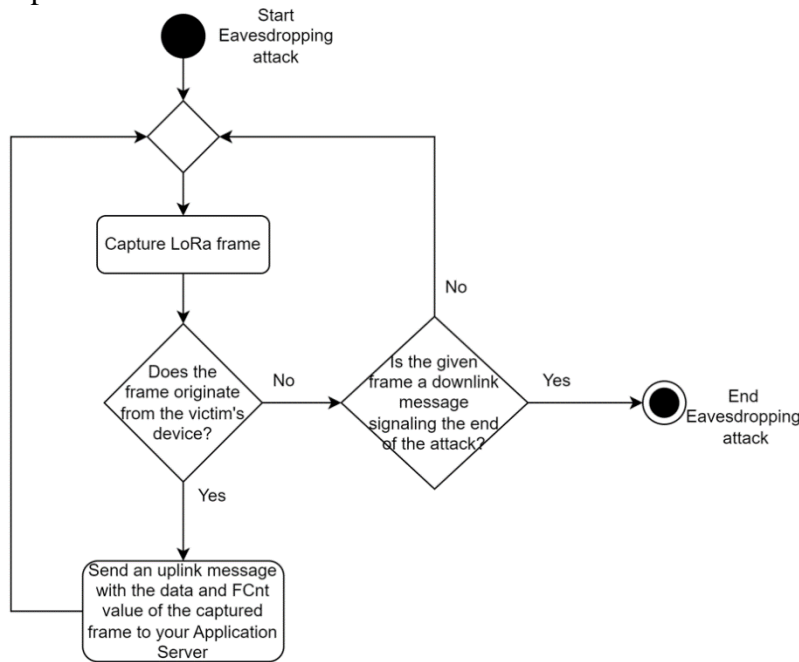


Figure 4 Eavesdropping Attack Implementation

Web Application Extension

The proposed tool extends an existing LoPET¹⁴² [15]. We continued to design the interface according to the already used pattern in the original application.

We used Material-UI components to maintain consistency from a UX¹⁴³ point of view [16]. We added a Security tab to the main navigation bar, as shown in Figure 5, which at the same time serves as a Home Page for Vulnerability Assessment.

¹⁴² LoRa Performance Evaluation Tool

¹⁴³ User Experience

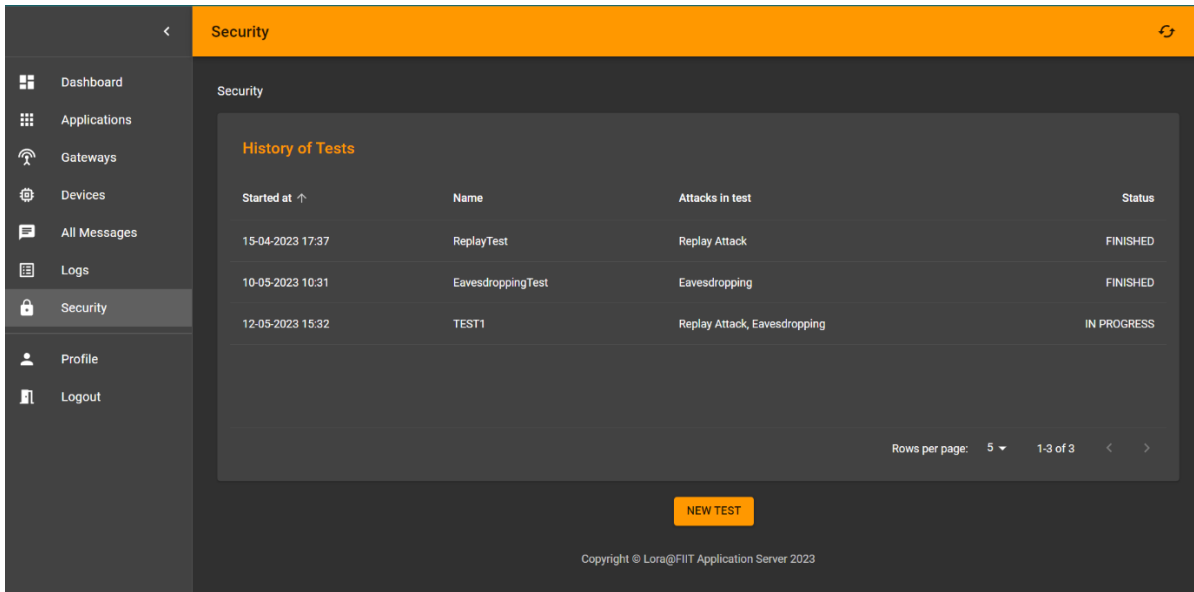


Figure 5 Security Home Page

With a focus on UI¹⁴⁴ and UX, screens for creating new vulnerability assessment scenarios were designed - separately for attacks and evaluation. The screen for creating a new scenario is shown in Figure 6.

The screenshot shows the 'Security / New test' screen. It contains several form fields and options for configuring a new test scenario. The 'Attack with address' section has two radio buttons: 'No Address' and 'Address' (selected). Below this is a text field for 'Victim Device Address *' containing '00fec5a4'. The 'Name of test *' field contains 'TEST'. The 'Counter' section has two radio buttons: '16-bit' (selected) and '32-bit'. The 'Choose attacks for test' section has two checkboxes: 'Replay Attack' and 'Eavesdropping', both of which are checked. To the right of these checkboxes is a 'Gap' text field containing '10000'. The 'Test execution' section has two radio buttons: 'Schedule' (selected) and 'Launch now'. To the right of these is a 'Choose date and time' text field containing '08-05-2023 19:00'. At the bottom right is a 'SAVE' button. The footer shows 'Copyright © Lora@FIIT Application Server 2023'.

Figure 6 Scenario Setup Screen

¹⁴⁴ User Interface

The user chooses whether to attack a device with a specific address or not. The user fills in the name of the test scenario and selects one or more attacks to be performed. In the case of a Replay Attack, the user fills in the mandatory Gap value. In the end, the scenario can be started immediately or scheduled. Screens for Replay Attack and Eavesdropping are also showing the current state of the scenario. The evaluation of the Replay Attack is presented in Figure 7.

Security / Attack detail

Frames

Received at	Data	FCnt ↓	Device address
05-05-2023 00:25:01	41H5WB3XRW	10000	00cc55dd
05-05-2023 00:25:00	X8UYR3MN2E	0	00cc55dd
05-05-2023 00:24:30	C6EMLRHEXL	65535	00cc55dd
05-05-2023 00:24:00	126BDAPN6G	65534	00cc55dd
05-05-2023 00:23:30	6WIWUU2BA6	65533	00cc55dd

Rows per page: 5 1-5 of 55538 < >

Status: FINISHED - PASS

Test name: ReplayTest - Replay Attack

Figure 7: Replay Attack Evaluation Screen

ChirpStack allows developers to generate an API¹⁴⁵ key, which can be used to send downlink messages [12]. We use downlink messages to initiate an attack. Events can be generated by several originators, e.g., uplink or downlink messages. ChirpStack provides HTTP¹⁴⁶ integration which enables sending these events to a user-configured endpoint. This allows us to store uplink and downlink messages in the database.

CONCLUSION

In this paper, the security implications of LoRa and LoRaWAN were discussed. Potential attacks such as Replay Attack and Eavesdropping were examined and vulnerability assessment of LoRaWAN using a threat modeling approach was conducted.

We analyzed the existing solutions and proposed a solution suitable for LoRaWAN networks, consisting of 2 main complementary components: implementation of attacks on end nodes and a web application for attack initiation and evaluation. We thus proposed a LoRaWAN-compatible solution using the ChirpStack as both a Network Server and an Application Server. As End Devices for both the attacker and the victim, we chose LilyGO TTGO LoRa32 T3_V1.6 868 MHz. We decided to implement an Eavesdropping Attack, threatening confidentiality, and a Replay Attack, threatening the availability of an End Device.

¹⁴⁵ Application Programming Interface

¹⁴⁶ Hypertext Transfer Protocol

In future work, we plan to implement scheduling and automated launch of user-defined scenarios, their evaluation, and results PDF export to assist network administrators in discovering vulnerabilities in IoT infrastructure.

Acknowledgment

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

References

1. LoRa Alliance. What is LoRaWAN® Specification. [Online] 2022. <https://loralliance.org/about-lorawan/>.
2. *Survey: Classification of the IoT technologies for better selection to real use*. Kaňuch, Peter, Macko, Dominik and Hudec, Ladislav. 2020. 2020 43rd International Conference on Telecommunications and Signal Processing (TSP). pp. 500 - 505.
3. LoRaWAN Architecture. *The Things Network*. [Online] <https://www.thethingsnetwork.org/docs/lorawan/architecture/>.
4. LoRaWAN Security. *The Things Network*. [Online] <https://www.thethingsnetwork.org/docs/lorawan/security/>.
5. LoRaWAN End Device Activation. *The Things Network*. [Online] <https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/>.
6. *Security Vulnerabilities in LoRaWAN*. Yang, Xueying, et al. 2018. 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). pp. 129 - 140. 10.1109/IoTDI.2018.00022.
7. *Exploring the Security Vulnerabilities of LoRa*. Aras, Emekcan, et al. 2017. Conference: 2017 3rd IEEE International Conference on Cybernetics (CYBCONF). pp. 1 - 6. 10.1109/CYBConf.2017.7985777.
8. *Selective Jamming of LoRaWAN using Commodity Hardware*. Aras, Emekcan, et al. 2017. 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 10.1145/3144457.3144478.
9. *LoRaWAN v1.1 Security: Are We in the Clear Yet?* Philip, Sumesh J., McQuillan, James M. and Adegbite, Oluwatoba. 2020. 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys). pp. 112 - 118. 10.1109/DependSys51298.2020.00025.
10. LoRa Alliance. LoRaWAN® Specification v1.0.2. *LoRa Alliance*. [Online] <https://resources.lora-alliance.org/getting-started-with-lorawan/lorawan-specification-v1-0-2>.
11. Kondraciuk, Aleksandra, Bartos, Aleksandra and Pańczyk, Beata. Comparative analysis of the effectiveness of OWASP ZAP, Burp Suite, Nikto and Skipfish in testing the security of web applications. *Journal of Computer Sciences Institute*. September 2022, 24, pp. 176 - 180.
12. Brocaar, Orne. ChirpStack Network Server. *GitHub*. [Online] <https://github.com/brocaar/chirpstack-network-server>.
13. LilyGO TTGO LoRa32 T3_V1.6 868Mhz 0.96" SMA WiFi Modul. *LaskaKit*. [Online] https://www.laskakit.cz/lilygo-ttgo-lora32-t3_v1-6-868mhz-0-96--sma-wifi-modul/.
14. Parente, Leonel Lopes. LMIC-node. *GitHub*. [Online] 2022. <https://github.com/lnlp/LMIC-node>.

15. *System for Management and Visualization of LoRa Network Components*. Hroš, Daniel and Valach, Alexander. Singapore : Springer Nature Singapore, 2022. Artificial Intelligence and Sustainable Computing. pp. 391 - 404. 978-981-19-1653-3.
16. Google LLC. Material Design. [Online] <https://material.io>.

DEZINFORMÁCIE A PROPAGANDA¹⁴⁷

JUDr. Juraj Drugda, PhD.

Akadémia Policajného zboru v Bratislave, Katedra vyšetrovania; juraj.drugda@akademiapz.sk

Abstrakt: Autor sa vo svojom príspevku venuje priblíženiu základných informácií o problematike dezinformácií a propagandy. Rozpracovaný je systém základných pojmov a východísk, ktorý umožní čitateľovi lepšiu orientáciu v skúmanej problematike. Autor sa ďalej venuje vybraným technikám a cieľom dezinformácií. Špeciálnej analýze sú podrobené negatívne dôsledky šírenia dezinformácií a propagandy v online priestore.

Kľúčové slová: dezinformácie, propaganda, druhy, ciele, negatívne dôsledky, online priestor.

ÚVOD

Dezinformácie a propagandu možno považovať za najvýznamnejší, najviditeľnejší a najčastejšie využívaný druh hybridných hrozieb. Pri zohľadňovaní týchto faktov bol stanovený cieľ tohto príspevku, ako poskytnutie prehľadu o problematike dezinformácií a propagandy vo svetle priblíženia systému základných pojmov a východísk tejto problematiky, oboznámenia čitateľov s druhmi a cieľmi dezinformácií a propagandy a najvýznamnejšími negatívnymi dôsledkami šírenia dezinformácií a propagandy v online priestore.

1. ZÁKLADNÉ POJMY A VÝCHODISKÁ

V nasledujúcej časti príspevku bude priblížený systém základných pojmov a východísk súvisiacich s preberanou problematikou. Vysvetlený bude význam pojmov ako dezinformácia, malinformácia, misinformácia, propaganda, informačné operácie a informačná vojna.

Definícia pojmu dezinformácia

Za dezinformáciu sa považuje overiteľne nepravdivá alebo zavádzajúca informácia, ktorá je vytvorená, prezentovaná a šírená na účely hospodárskeho zisku alebo zámerného zavádzania verejnosti, a môže poškodiť verejný záujem. Poškodenie verejného záujmu zahŕňa ohrozenie demokratických procesov a procesy tvorby politiky, ako aj verejných statkov, ako napr. ochrany zdravia občanov EÚ, životného prostredia alebo bezpečnosti. Medzi dezinformácie nepatria chyby v spravodajstve, satira a paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené.¹⁴⁸

¹⁴⁷ Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

¹⁴⁸ Akčný plán proti dezinformáciám [online]. Európska komisia, 2018 [cit. 2023-10-30]. Dostupné na internete: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52018JC0036&from=SK>

Definícia pojmu malinformácia

Malinformácia – informácia, ktorá je založená na realite, šírená zámerne s cieľom spôsobiť ujmu osobe, organizácii alebo štátu, napr. uniknuté informácie, nenávistné prejavy, obťažovanie.¹⁴⁹

Definícia pojmu misinformácia

Misinformácia – mylná alebo nepravdivá informácia, ktorá sa na rozdiel od dezinformácií šíri nevedome a bez úmyslu poškodiť. Z týchto dôvodov sa nejedná o prvok informačných operácií.¹⁵⁰

Rozdiel medzi dezinformáciou, misinformáciou a malinformáciou

Uvedené pojmy je možné rozlišovať na základe systému znakov. Všetky pojmy majú spoločný znak, a to, že sa jedná o určitý druh informácie. Táto informácia obsahuje ďalší znak, ktorým je charakter informácie. Charakter dezinformácie je, že sa jedná o nepravdivú informáciu, pri malinformácii sa jedná o pravdivú informáciu a pri misinformácii sa jedná o nepravdivú informáciu. Ďalším znakom je existencia/neexistencia určitého subjektu – škodlivého aktéra. Pri dezinformácii tento subjekt existuje, pri malinformácii tento subjekt taktiež existuje a pri misinformácii tento subjekt absentuje. Posledným znakom je existencia motívu/cieľa, ktorý subjekt svojim konaním sleduje. Pri dezinformácii cieľ subjektu existuje, pri malinformácii cieľ subjektu taktiež existuje a pri misinformácii cieľ subjektu, rovnako ako subjekt samotný absentuje.

Definícia pojmu propaganda

Aktivita, ktorá je zameraná na šírenie určitej myšlienky, zdôrazňujúca iba jej pozitívne aspekty, šírená s cieľom presvedčiť publikum o jej správnosti. Má spravidla ideologickú, náboženskú, či politickú konotáciu. Na rozdiel od reklamy či propagácie propaganda nemá komerčný rozmer.¹⁵¹

Vo všeobecnosti môže byť propaganda realizovaná ako oslavná alebo očierňujúca. Oslavná sa sústreďuje na vytváranie pozitívneho dojmu. Takéto úsilie je späté s vyzdvihovaním subjektu, prípadne s glorifikáciou jeho pôsobenia a činnosti. Zároveň, potláča všetko negatívne a nežiaduce. Očierňujúca propaganda cieľi na protivníka v snahe oslabiť či poškodiť jeho povest' alebo pozíciu.

Druhy propagandy

Biela propaganda: Biela propaganda pochádza zo zdroja, ktorý je jednoducho a správne identifikovateľný a obsahuje presné a korektné informácie. Možno ju pokladať za druh propagácie s cieľom zmobilizovania obyvateľstva v podpore určitého spoločného záujmu. Vhodným príkladom môže byť náborová kampaň do americkej armády počas druhej svetovej vojny.

Čierna propaganda: Čierna propaganda pochádza zo zdroja, ktorý sa snaží skrývať svoju identitu. Využíva veľké množstvo skresľujúcich a zavádzajúcich informácií, prípadne úplných klamstiev.

¹⁴⁹ Krátky slovník hybridných hrozieb[online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>

¹⁵⁰ Dezinformácie a informačné operácie [online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html>

¹⁵¹ Krátky slovník hybridných hrozieb[online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>

Šedá propaganda: Šedú propagandu môžeme pokladať za prienik bielej a čiernej propagandy. Presnosť informácií a relevancia ich zdroja je pri šedej propagande častokrát neidentifikovateľná. Rovnako ani identita ich autora, prípadne cieľ, ktoré sa snažil dosiahnuť.¹⁵²

Definícia pojmu informačné operácie

Informačné alebo vplyvové operácie dnes označujú aktivity, ktorými cudzí aktéri alebo ich predstavitelia zbierajú a šíria potenciálne škodlivé informácie o svojom nepriateľovi. V kontexte štátu predstavujú zámerné zasahovanie do vnútorných záležitostí krajiny s cieľom vytvoriť atmosféru nedôvery medzi štátom a jeho občanmi či oslabiť spoločnosť.

Informačné operácie sa môžu vyskytnúť samostatne alebo ako súčasť širšej hybridnej kampane, pri ktorej sa využívajú rôzne metódy naraz. Okrem komunikačných nástrojov možno na ovplyvňovanie spoločnosti použiť všetko - od diplomatických a hospodárskych sankcií až po použitie polovojských skupín.¹⁵³

Definícia pojmu informačná vojna

Koordinované využívanie informácií a dezinformácií orgánmi verejnej moci, ozbrojenými silami alebo inými subjektami s cieľom ovplyvniť myslenie a správanie ľudí s úmyslom dosiahnuť výhodu nad protivníkom.¹⁵⁴

Informačná vojna je koncept zahŕňajúci využívanie riadenia informačných a komunikačných technológií v snahe získať strategickú výhodu nad súperom. Informačná vojna je manipulácia s cieľom dôveryhodnými informáciami, bez jeho vedomia tak, aby cieľ robil rozhodnutia v záujme útočníka. V dôsledku toho nie je jasné, kedy informačná vojna začína, končí a aká je silná alebo deštruktívna.

Informačná vojna môže zahŕňať zhromažďovanie taktických informácií, uisťovanie o správnosti informácií, šírenie propagandy alebo dezinformácií s cieľom demoralizovať alebo manipulovať nepriateľa a verejnosť, spochybňovanie kvality informácií opozičných síl a odopieranie príležitostí na zhromažďovanie informácií nepriateľským silám. Informačná vojna je úzko spojená s psychologickou vojnou.

Informačná vojna môže mať mnoho podôb:

- televízne, internetové a rádiové prenosy môžu byť rušené,
- televízne, internetové a rozhlasové prenosy môžu byť zneužitú na dezinformačnú kampaň,
- deaktivácia logistických sietí,
- používanie dronov a iných sledovacích robotov alebo webových kamier,
- riadenie komunikácie,
- syntetické médiá,

¹⁵² NEUMANN, C.: Propaganda, Uses and Psychology [online]. Espionage encyclopedia, 2023 [cit. 2023-10-30]. Dostupné na internete: <http://www.faqs.org/espionage/Pr-Re/Propaganda-Uses-and-Psychology.html>

¹⁵³ Ako sa brániť proti informačným operáciám? Príručka pre komunikátorov. [online]. GLOBSEC, 2020 [cit. 2023-10-30]. Dostupné na internete: https://www.globsec.org/sites/default/files/2020-02/GLOBSEC_Prirucka-pre-komunikatorov.pdf s. 9

¹⁵⁴ Krátky slovník hybridných hrozieb[online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>

- organizované používanie sociálnych médií a iných platforiem na vytváranie obsahu online, ktoré možno využiť na názorovú manipuláciu medzi masami.

2. TECHNIKY A CIELE DEZINFORMÁCIÍ

2.1 Techniky dezinformácií

Za hlavné techniky dezinformácie sú považované:

- zveličenie (zjednodušenie) udalosti, informácie alebo správy – škodlivý aktér zveličuje udalosti, informácie alebo správy, ktoré zapadajú do jeho dezinformačného naratívu a zjednodušuje alebo bagatelizuje udalosti, informácie alebo správy, ktoré naopak nezapadajú do jeho dezinformačného naratívu,
- zmena povahy alebo okolností (času, miesta) udalosti, informácie alebo správy – škodlivý aktér manipuluje s miestnymi alebo časovými okolnosťami a súvislosťami udalosti, informácie alebo správy tak, aby zapadali do pripravovaného dezinformačného naratívu,
- úplná zmena udalosti, informácie alebo správy na inú – škodlivý aktér kompletne vyfabrikuje, prípadne vynechá určité súčasti udalosti, informácie alebo správy tak, aby zapadali do pripravovaného dezinformačného naratívu.

Najúspešnejšie dezinformácie spravidla:

- vychádzajú z čiastočne alebo úplne pravdivých informácií,
- sú prispôbené kultúrnemu kontextu prijímateľa dezinformácie,
- sú šírené viacerými kanálmi a aktérmi (osobami, profilmi na sociálnych sieťach),
- útočia na negatívne emócie (vyvolanie strachu a hnevu),
- zámerne sa zameriavajú na citlivé otázky spoločnosti.

2.2 Technika 4D

Pre lepšie pochopenie tzv. Techniky 4D odporúčame predstaviť si situáciu, v ktorej dochádza k diskusii v súvislosti so zverejnenou dezinformáciou (v reálnom alebo online priestore). V rámci tejto diskusie prebieha dialóg, ktorý sleduje publikum (reálne alebo publikum zložené z užívateľov online platformy). Vo väčšine prípadov sa v publiku sformujú dva tábory – jeden z nich sa prikláňa k diskutérom, ktorí veria dezinformácii a druhý z nich sa zas prikláňa k diskutérom, ktorí sa túto dezinformáciu snažia vyvrátiť. Technika 4D sú techniky, ktoré frekventovane využívajú aktéri hrozby na to, aby získali podporu pre svoje tvrdenia a naklonili si publikum na svoju stranu. Tieto techniky sú nasledujúce:

Odmietnutie:

Odmietnutie je hlavná a najbežnejšia technika využívaná aktérmi hybridných hrozieb. Aktér hrozby vytvorí urážku, ktorá má zdiskreditovať legitímny zdroj informácie, ako dôvod na to, aby ho prijímatelia prestali považovať za dôveryhodný. Jedná sa o pokus aktéra hrozby o umlčanie vyjadrovania schopnosti subjektu pomocou urážky, ktorá má za účel zasiatie nedôvery v zdroj informácie.

Rozptýlenie pozornosti:

V prípade, že sa aktér hrozby dostane do konverzácie, ktorá mu je nepríjemná alebo pre neho nepriaznivá, tak dochádza k snahám o zmenu predmetu tejto konverzácie. Ďalšou metódou

rozptýlenia pozornosti je napríklad obvinenie oponujúceho, že je vinný z tej istej veci, ktorá nezapadá do naratívu aktéra hrozby. Táto technika umožňuje vzniku falošného porovnávania medzi kritizujúcim a kritizovaným, pričom vznik tejto situácie vytvára priestor na zmenu predmetu konverzácie.

Deformovanie:

Deformácia faktov je jednoducho pochopiteľný koncept. V prípade, že určitý fakt nezapadá do preferovaného naratívu aktéra hrozby dochádza ku vytvoreniu vlastných nových zmanipulovaných faktov za účelom prezentácie naratívu v novom zmanipulovanom svetle.

Vydesenie:

Zmyslom vydesenia je pokus o vystrašenie prijímateľa informácie. Táto technika je bežne využívaná v politických diskusiách. Odsťašujúca rétorika má za cieľ prezentovanie hypotetických katastrofálnych následkov určitého konania v nádeji aktéra hrozby, že jeho oponenti nebudú pokračovať vo svojej pre aktéra hrozby nepohodlnej argumentačnej línii alebo nedosiahnu pre aktéra hrozby nepohodlný cieľ, ktorý mali vopred stanovený.¹⁵⁵

2.3 Ciele dezinformácií

- presvedčanie ľudí, aby verili nesprávnym informáciám,
- podkopávanie správnych informácií,
- vytváranie neistoty,
- podkopávanie dôvery,
- podkopávanie dôveryhodnosti,
- podkopávanie kolektívnej akcie vrátane volieb,
- podkopávanie funkčnej vlády.

3. NEGATÍVNE DÔSLEDKY ŠÍRENIA DEZINFORMÁCIÍ A PROPAGANDY V ONLINE PRIESTORE

Výskumné aktivity o tom, ako sa šíria dezinformácie, zaznamenali prudký nárast. Štúdie ukazujú, že dezinformácie šírené v sociálnych médiách možno rozdeliť do dvoch širokých etáp: seedenie a ozvena. „Seeding“, znamená, že zlomyseľní herci strategicky vkladajú podvody, ako sú falošné správy, do ekosystému sociálnych médií, a „echoing“ nastáva, keď publikum šíri dezinformácie argumentačne ako svoje vlastné názory, často začlenením dezinformácií do konfrontačnej konverzácie. Rozlišujeme nasledujúce negatívne dôsledky personalizovaného online obsahu:

3.1 Informačná bublina

Za informačnú bublinu sa považuje výsledok personalizovaného vyhľadávania, kedy algoritmus webstránky (napr. Facebook, alebo Google Search) selektívne vyberá správy, ktoré sa dostanú k užívateľovi na základe informácií ako lokalizácia, predchádzajúce kliknutia, história vyhľadávania

¹⁵⁵ NIMMO, B.: Combatting Disinformation with the Four D's. [online]. Center for Academic Innovation. University of Michigan, 2022 [cit. 2023-10-30]. Dostupné na internete: <https://ai.umich.edu/blog-posts/spotting-fake-news-ben-nimmo-disinformation-misinformation-fake-news-teach-out/>

apod. Informačná bublina sa považuje za negatívny dopad takto filtrovaných informácií, kedy sa užívateľ stáva izolovaným voči informáciám, ktoré by mohli rozšíriť jeho všeobecný rozhľad, s ktorými by nesúhlasil, alebo by nepodporovali jeho názory. Takto filtrované informácie majú tendenciu utvrdzovať človeka v jeho osobnom presvedčení a uzatvárať každého v jeho vlastných kultúrnych či ideologických bublinách. Riziko informačných bublín spočíva v tom, že takto filtrované informácie nám nedávajú šancu otvoriť sa novým nápadom, témam, názorom či dôležitým správam.¹⁵⁶

3.2 Teória selektívnej expozície

Tento pojem môžeme definovať tak, že jedinci majú tendenciu prijímať informácie, ktoré podporia ich vžitú názory a rozhodnutia a vyhýbajú sa informáciám, ktoré by ich presvedčenie mohli poprieť. Výber takýchto informácií je založený na ich predchádzajúcich skúsenostiach, ich perspektíve, názoroch, viere a iných presvedčeniach. Potenciál médií v šírení informácií je využívaný často na politický marketing, prezentáciu politických strán či osôb a mnoho ďalších názorových prúdov. Ľudia čerpajú informácie z masmédií, ale nemenia svoje vžitú presvedčenie či názory. Tendencia vystavovať ľudí správam, ktoré sú v zhode s ich názormi a vyhýbajú sa nesympatickým informáciám je jedným z dôvodov vzniku informačnej bubliny v prostredí online sociálnych sietí. S príchodom nových médií sa spôsob, akým prijímame informácie výrazne zmenil a stále mení. Algoritmy na sociálnych sieťach, personalizujú náš News Feed a výrazne ovplyvňujú našu expozíciu správam z vonkajšieho sveta. Bežný užívateľ sociálnych sietí si veľa krát neuvedomuje, že väčšina správ, ktoré dostáva, sú takto filtrované a nie sú dostatočne diverzifikované. Okrem algoritmov si každý užívateľ môže sám nastaviť, aké informácie z ktorých zdrojov chce dostávať. V prostredí Twitteru, Facebooku, či ďalších sociálnych sietí, ktoré sú v dnešnej dobe veľa krát zdrojom správ, dostávame len to, čo sa nám páči. Všetko je relevantné našim názorom, záujmom a všetko sa zhoduje s našim pohľadom na svet. Zvyčajne môžeme stráviť celý deň na Twitteri, alebo Facebooku a nedostaneme sa do kontaktu so správami, s ktorými by sme nesúhlasili.¹⁵⁷

3.3 Komnata ozveny

Ľudia majú tendenciu sa uzatvárať do komunit s ľuďmi rovnako zmýšľajúcimi a uzatvárať sa do tzv. komnat ozvien. Komnaty ozvien, anglicky tzv. echo chambers, sú javom, pri ktorých sa ľudia navzájom utvrdzujú vo svojich názoroch a spájajú sa s ľuďmi s rovnakým presvedčením. Takto uzavreté myšlienky, alebo názory sa v daných homogénnych a polarizovaných skupinách odrážajú od opačných argumentov a zosilňujú sa podobne ako ozvena. Taktiež v týchto komunitách sa dezinformácie a konšpirácie zdieľajú medzi priateľmi rýchlejšie, pretože sa s nimi jedinci stotožňujú. Echo chambers majú za následok, že intenzita dezinformácii naberá extrémnejšie podoby v rámci rovnako zmýšľajúcej skupiny.

¹⁵⁶ PARISER, E.: The filter bubble: what the Internet is hiding from you. New York: Penguin Press, 2011.

¹⁵⁷ MORADPOUR, T.: Is Twitter Telling You Only What You Want To Hear? [online]. WordPress, 2010 [cit. 2023-10-30]. Dostupné na internete: <http://tommoradpour.wordpress.com/2010/12/24/is-your-newspaper-telling-you-what-you-want-to-hear>

3.4 Skupinová polarizácia

Skupinovú polarizáciu môžeme definovať, ako výsledok diskusie v skupine, ktorý je extrémnejší, alebo naopak konzervatívnejší, než boli pôvodne názory či postoje jednotlivých členov skupiny. Extrémnou a zároveň rizikovou formou skupinovej polarizácie je, keď sú procesy rozhodovania vysoko súdržnej skupiny podobne zmýšľajúcich ľudí také silné, že je oslabené ich porozumenie reality a môžu byť tak podporené nesprávne, mylné či do konca katastrofálne rozhodnutia. Skupinová polarizácia vo virtuálnych komunitách vedie k omnoho extrémnejším záverom, ako klasická skupinová komunikácia. Jedinci v online komunitách prichádzajú s unikátnejšími a kvalitnejšími nápadmi v porovnaní s tradičnou komunikáciou. Vzájomné utvrdzovanie názorov v rámci jednej skupiny vedie k výraznejšej polarizácii. Užívateľ, ktorý vidí, že ostatní v skupine súhlasia s jeho názormi, sa stáva viac sebavedomejším a tým sa jeho presvedčenie a presvedčovanie ostatných stáva extrémnejším. Príkladom môže byť užívateľ, ktorý si myslí, že klimatické zmeny nie sú pravda. So svojimi vyjadreniami prichádza najprv opatrne, no keď zistí, že s ním súhlasí viac ľudí, tak sa stáva istejším, presvedčenejším o jeho názore a začne pohrdať ľuďmi, ktorí majú opačné názory a iný pohľad na vec. Snahy zmeniť dezinformácie a odhaliť pravdu je väčšinou užívateľmi v polarizovaných skupinách odignorovaná. Práve naopak, ak polarizovaných užívateľov tieto pravdivé či odhalené správy zasiahnu a uveria im, majú tendenciu sa ďalej utvrdzovať už len v ich novom presvedčení.¹⁵⁸

3.5 Deep fake

Deep fake je digitálny obsah, ktorý bol zmanipulovaný. Deep fake technológiu možno využiť na ohováranie, vydieranie a odcudzenie identity. Vďaka nízkym nákladom a efektívnosti môžu byť deep fake-y použité na šírenie dezinformácií rýchlejšie a vo väčšom objeme ako iné druhy dezinformácií. Dezinformačné útočné kampane môžu využívať technológiu Deep fake na generovanie dezinformácií týkajúcich sa ľudí, štátov alebo príbehov. Deep fake technológia môže byť použitá ako zbraň, aby zavádzala publikum a šírila klamlivé a zavádzajúce informácie.

ZÁVER

Dezinformácie a propagandu možno považovať za najvýznamnejší, najviditeľnejší a najčastejšie využívaný druh hybridných hrozieb. Je vysoko pravdepodobné, že sa mnohí členovia spoločnosti a používatelia sociálnych sietí a ostatných internetových portálov s veľkým dosahom a počtom užívateľov už niekedy stretli s určitým druhom dezinformácie a propagandy. Dovolíme si optimisticky predpokladať, že väčšina z nich dokázala na prvý pohľad rozpoznať škodlivú a nepravdivú informáciu od informácie pravdivej a pochádzajúcej z overených zdrojov. Napriek tomu sa však dezinformácie a propaganda naďalej nezastaviteľne šíria v online aj reálnom priestore a ich negatívne dôsledky sa môžu v budúcnosti dotknúť každého z nás. Z tohto, aj mnohých iných dôvodov vznikol tento príspevok, ktorá má čitateľovi napomôcť sa zorientovať v problematike dezinformácií, propagandy a s nimi spojenými najčastejšími škodlivými dôsledkami, ktoré vplývajú na spoločnosť a právny štát.

¹⁵⁸ SUNSTEIN, C.: How Facebook Makes Us Dumber [online]. Bloomberg View, 2016 [cit. 2023-10-30]. Dostupné na internete: <http://www.bloombergvie.com/articles/2016-01-08/how-facebook-makes-us-dumber>

Zdroje

1. Akčný plán proti dezinformáciám [online]. Európska komisia, 2018 [cit. 2023-10-30]. Dostupné na internete: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52018JC0036&from=SK>
2. Ako sa brániť proti informačným operáciám? Príručka pre komunikátorov. [online]. GLOBSEC, 2020 [cit. 2023-10-30]. Dostupné na internete: https://www.globsec.org/sites/default/files/2020-02/GLOBSEC_Prirucka-pre-komunikatorov.pdf s. 68A
3. Dezinformácie a informačné operácie [online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html>
4. Krátky slovník hybridných hrozieb [online]. Národný bezpečnostný úrad, 2023 [cit. 2023-10-30]. Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>
5. MORADPOUR, T.: Is Twitter Telling You Only What You Want To Hear? [online]. WordPress, 2010 [cit. 2023-10-30]. Dostupné na internete: <http://tommoradpour.wordpress.com/2010/12/24/is-your-newspaper-telling-you-what-you-want-to-hear>
6. NEUMANN, C.: Propaganda, Uses and Psychology [online]. Espionage encyclopedia, 2023 [cit. 2023-10-30]. Dostupné na internete: <http://www.faqs.org/espionage/Pr-Re/Propaganda-Uses-and-Psychology.html>
7. NIMMO, B.: Combatting Disinformation with the Four D's. [online]. Center for Academic Innovation. University of Michigan, 2022 [cit. 2023-10-30]. Dostupné na internete: <https://ai.umich.edu/blog-posts/spotting-fake-news-ben-nimmo-disinformation-misinformation-fake-news-teach-out/>
8. PARISER, E.: The filter bubble: what the Internet is hiding from you [online]. New York: Penguin Press, 2011. 294 s. ISBN 978-1-59420-300-8
9. SUNSTEIN, C.: How Facebook Makes Us Dumber [online]. Bloomberg View, 2016 [cit. 2023-10-30]. Dostupné na internete: <http://www.bloombergview.com/articles/2016-01-08/how-facebook-makes-us-dumber>

DIGITÁLNY PRENOS INFORMÁCIÍ A SYSTÉM KRYPTOAKTÍV AKO NÁSTROJE HYBRIDNÉHO KONFLIKTU

por. Mgr. Daniela Gavurová, por. Mgr. Andrej Lipták

Národná kriminálna agentúra Prezídia PZ, Pribinova 2, 812 72 Bratislava, e-mail: daniela.gavurova@minv.sk, daniela.gavurova@akademiapz.sk, Národná centrála osobitných druhov kriminality Prezídia PZ, Pribinova 2, 812 72 Bratislava, e-mail: andrej.liptak@minv.sk, andrej.liptak@akademiapz.sk

Abstrakt: V tomto príspevku sa autori zaoberajú problematikou digitálneho prenosu informácií a využitia systémov kryptoaktív ako nástrojov hybridného konfliktu. V príspevku sa prvkami kvantitatívno-kvalitatívneho skúmania rozoberá systém kryptoaktív a prenos informácií v digitálnom prostredí, ich vplyv na potenciálne narušenie demokratického zriadenia, rozvrat hospodárskej stability a potenciálnu podprahovú manipuláciu obyvateľstva. Predmetom skúmania príspevku je vzťah systému kryptoaktív v zmysle technológie umožňujúcej alternatívny digitálny prenos informácií vrátane ocenených hodnôt, a vzťah informácií nepresného, neúplného, alternatívneho charakteru k hybridným hrozbám. Cieľom príspevku je poskytnúť štruktúrovaný, logicky usporiadaný rámec, ktorý približuje možnosti zneužitia novodobých technológií v ére digitalizácie z pohľadu nekonvenčného hybridného konfliktu.

Kľúčové slová: digitálny prenos, dezinformácie, kryptoaktíva, obchádzanie sankcií, hybridné hrozby.

1. KRYPTOAKTÍVA AKO NÁSTROJ HYBRIDNÉHO KONFLIKTU

Hybridné hrozby narušujú celistvosť demokratického zriadenia, systému orgánov verejnej moci, stabilnú verejnú mienku, hospodárske a ekonomické prostredie štátu, a to atypickým spôsobom. Šírenie dezinformácií, poskytovanie nepresných údajov pri dôležitých strategických rozhodnutiach oprávnených orgánov, podprahové informácie cieliace na vyvolanie nespokojnosti u obyvateľstva, poskytovanie neracionálnych možností, posúvanie hranice morálky, všetky tieto aspekty pracujú v takzvanej šedej zóne. Svojim charakterom nie sú ľahko detekovateľné, pretože operujú na hranici zakázaného, resp. dovoleného, skrývajú sa za princípy a prvky demokracie, slobody, alternatívneho rozmýšľania. Ich snahou je minimalizovať jasne stanovené štruktúry vojny, vojenského konfliktu, označujú agresora, páchatel'a, osobu narušujúcu morálku ako nepochopenú inú stranu, ktorá vo svojej podstate nemusí byť zlá. Na komparovanie podstaty hybridného konfliktu výborne slúži vtipná slovenská anekdota o varení žaby v hrnci.¹⁵⁹

Nástroje hybridného konfliktu sú nebezpečné aj kvôli svojej mnohotvárnosti. Ovplyvňovanie verejnej mienky, oslabovanie hospodárskej stability, kybernetické útoky, znefunkčňovanie strategických objektov, systémov, biologické a chemické ohrozovanie, destabilizácia sociálneho systému sú len počiatkom pri tej početnej variabilite nástrojov hybridného konfliktu. V podstate sa dá povedať, že vzhľadom na dynamický rozvoj v oblasti vedy a výskumu, ktorý aktuálne zažívame najmä na úrovni umelej inteligencie, nie je možné vymenovať všetky nástroje hybridného konfliktu. Nástroje hybridného konfliktu sú veľmi diverzifikované a čo nebolo zneužitie na vojenské účely dnes, môže byť použité zajtra a *vice versa*.

Nástrojmi hybridného konfliktu môžu byť výsledky technologického pokroku, ktoré sú samé o sebe neutrálne, dokonca si dovoľme tvrdiť, že technologický rozvoj je vo väčšine prípadov podmienený pozitívnou motiváciou. Avšak to nemení nič na skutočnosti, že takýto technologický

¹⁵⁹ Posilňovanie odolnosti voči hybridným hrozbám. (online, cit. 07.10.2023). Dostupné na internete: <<https://www.mzv.sk/diplomacia/bezpecnostna-politika/hybridne-hrozby>>

aspekt môže byť zneužitý na účely hybridného konfliktu. Obmedzenie vývoja a výskumu nie je na mieste, pretože úmysel agresora absentovaním nástroja zmenený nebude, agresor si zväčša nájde inú sofistikovanejšiu cestu. Príkladom môžeme uviesť drony, ktoré sú v hybridnom konflikte, jeho konvenčnej časti, využívané po prvý krát. Zákazom alebo obmedzením dronovej techniky by však nedošlo k obmedzeniu sledovania vojensky relevantného priestoru a osôb, hliadkovania na hraniciach vojensky relevantných obvodoch, resp. k vzdušným útokom, ale iba k výmene nástroja, teda dronu za napr. malé lietadlá alebo inú vojenskú techniku. Na mieste je teda vhodná regulácia a s ňou spojené poznanie a detekcia nástrojov hybridného konfliktu, ktoré sú viac podmienené účelom, než ich samotnou podstatou.

Kryptoaktíva sú novodobou technológiou. Predstavujú alternatívu k finančnému systému. Možno ich podstatu prirovnať k medzinárodným bankovým prevodom, resp. ku globálnej sieti, ktorá zabezpečuje prevod ocenených hodnôt alebo vo svojej najväčšej podstate presun informácií medzi subjektami. Systém kryptoaktív nepotrebuje pre svoju funkčnosť centrálnu autoritu, ako je to napríklad pri systéme SWIFT alebo SEPA alebo ACH. Práve táto decentralizácia systému kryptoaktív zabezpečuje stabilitu presunu informácií z pohľadu ich nezameniteľnosti. Veď ako si jeden môže byť istý, že presun informácií skrz pôvodne vojensky relevantnú sieť Tor nebol ovplyvnený neoprávnenou osobou, ktorá nezanechala digitálne stopy? Ako si v priestore internetu jeden môže byť istý, že odoslaná informácia z jedného uzla siete je tá istá, neovplyvnená než prijatá informácia iným uzlom siete? Určitým spôsobom uvedené rieši asymetrická kryptografia a pre ňu typický systém privátnych a verejných kľúčov. Ak však je potrebné informácie zdieľať s viacerými strategickými entitami je bezpečnosť informácií negatívne ovplyvnená počtom entít. Kryptoaktíva uvedené riešia transparentnosťou blockchainu, ktorú si však netreba myliť s dostupnosťou dát. Systém kryptoaktív zabezpečuje, aby si každý uzol siete mohol s istotou overiť pravdivosť informácie. Tieto pravidlá a použité technológie však nie sú v systéme kryptoaktív unifikované. Relevantný je však napríklad systém Zero-Knowledge proof¹⁶⁰, ktorý zabezpečuje overenie validity informácii bez toho, aby bola informácia zverejnená buď jemu alebo inej entite v sieti. Ďalšou skutočnosťou, ktorú zaisťuje systém kryptoaktív je celistvosť informácií. To znamená, že akákoľvek informácia umiestnená do distribuovanej databázy transakcií systému kryptoaktív ostáva nezmeniteľná, vzhľadom na výpočtovú náročnosť, ktorú by musel neoprávnený útočník na jej zmenu vynaložiť. Medzinárodný prevod finančných prostriedkov, resp. presun informácií skrz centralizovane zabezpečené siete nevytvára také možnosti na dynamický rozvoj ako vytvára systém kryptoaktív. Ak hovoríme o presune informácií a o ich celistvosti a nezmeniteľnosti v rámci systému kryptoaktív, prečo neumiestniť do distribuovanej databázy transakcií určitý program, ktorý vzhľadom na znaky systému kryptoaktív bude realizovať činnosti bez toho, aby ho bolo možné ovplyvniť. Smart kontrakty¹⁶¹ alebo programy bežiacie v rámci systému kryptoaktív existujú, no ich funkčnosť je podmienená ich stupňom vývoja. Protokoly, na základe ktorých sú vytvárané smart kontrakty sú na počiatku svojho vývoja, aktuálne obsahujú množstvo chýb využiteľných agresorom vo svoj prospech. Za dôležité však považujeme poukázať na potenciál systému kryptoaktív aj v tejto oblasti. Vytvorenie decentralizovaných bánk, zmenární, úschov, systémy na určovanie vlastníctva a iných finančných inštitúcií akoto programov bez centrálnej autority, bez možnosti ich absolútneho zákazu, spojením s bezpečným presunom informácií, ktorý

160 Awesome zero knowledge proofs. (online, cit. 07.10.2023.) Dostupné na internete: <<https://github.com/matter-labs/awesome-zero-knowledge-proofs>>

161 Introduction to smart contracts. (online, cit. 07.10.2023). Dostupné na internete: <<https://ethereum.org/en/smart-contracts/>>

môže mať charakter prevodu oceníteľných hodnôt založených na dôvere (ako tomu je aj v aktuálnom finančnom systéme), vykazuje znaky značného technologického pokroku. Na jednej strane systém kryptoaktív môže priniesť množstvo dobra, ako je reštartovanie finančného systému zbankrotovanej krajiny v priebehu niekoľkých dní s minimálnymi nákladmi, no na druhej strane môže takýto systém pôsobiť ako nástroj hybridného konfliktu.¹⁶²

Rusko ako nespochybniteľný iniciátor aktuálneho rusko-ukrajinského konfliktu bolo za svoje počínanie ohodnotené rôznymi sankciami. Sankcie z pôdy Európskej únie¹⁶³ alebo z pôdy americkej finančnej spravodajskej jednotky OFAC sú reštriktívnymi opatreniami, ktoré sú reakciou na ruské konanie narušajúce zvrchovanosť a nezávislosť Ukrajiny. Odpojenie vybraných ruských bánk už zo spomínaného systému SWIFT a obmedzenie medzinárodného obchodu okrem iného zapríčinilo hospodársky úpadok Ruska, oslabenie ruskej meny a nutnej orientácie ruského hospodárstva smerom k autoritatívnym a diktátorským režimom. Kryptoaktíva v tomto ponímaní môžu byť vzhľadom na svoj fundament spolu s kybernetickými útokmi priamym nástrojom hybridného konfliktu alebo nástrojom na obchádzanie uvalených sankcií. Vedeckovýskumný inštitút v USA, Congressional Research Service vo svojich výstupoch poukazuje na metódy a techniky, akým spôsobom môžu byť kryptoaktíva použité najmä na obchádzanie sankcií. Vylúčenie Ruska ako hospodárskeho partnera znamená prerušenie transakčného toku medzi Ruskom a ostatnými krajinami. Najmä v prípade SWIFT, celosvetovo použíwanej transakčnej siete, ktorej funkčnosť zaisťuje centrálny orgán so sídlom v Belgicku, možno hovoriť o úspešnom obmedzení transakčného toku Ruska. Kryptoaktíva však nie sú riadené centrálnym orgánom, a preto predstavujú jednu z potenciálnych možností, ako môže Rusko obísť takéto obmedzenie transakčného toku.¹⁶⁴

Transparentnosť systému kryptoaktív však dáva oprávneným orgánom do rúk moc pozorovať všetky transakcie vykonané jednotlivými uzlami siete kryptoaktív. To znamená, že aj keď je systém kryptoaktív a jeho transakčný tok neovplyviteľný, možno tento transakčný tok kryptoaktív pozorovať, odhaľovať pokusy o zneužitie tohto transakčného toku a na základe uvedeného sankcionovať jednotlivé entity. Týmito entitami môžu byť poskytovatelia služieb kryptoaktív reprezentovanými verejnými adresami prijímajúcimi a odosielať kryptoaktíva, resp. môže byť uvalený zákaz prijímania alebo odosielať kryptoaktív v súvislosti so zakázanými verejnými adresami. V tomto ponímaní poukazujeme na finančnú spravodajskú jednotku OFAC a jej sankčný list, v ktorom sú uvedené aj odhalené verejné adresy sankcionovaných entít, ktoré boli použité alebo mali byť použité na obchádzanie sankcií alebo na realizáciu inej trestnej činnosti. Najčastejšie legalizovania výnosov z trestnej činnosti. Za zmienku stojí napríklad sankcionovaná entita TASK FORCE RUSICH (program RUSSIA-EO14024) a identifikované a priradené sankcionované verejné adresy kryptoaktíva Bitcoin bc1q2lpjnt348pfvxhfy33ehmdzy3gmx8w4052z6, kryptoaktíva Ethereum bc1q17dlyh8xz6tpqk92vztrhgh88dmjvcwrmsemrm, 0x3AD9dB589d201A710Ed237c829c7860Ba86510Fc, 0xc2a3829F459B3Edd87791c74cD45402BA0a20Be3 alebo kryptoaktíva USDT, ktoré kopíruje

162 ŠANTA, J., ŠANTA, I.: Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty. Praha: Leges, 2023. 15-20 strán. ISBN: 978-80-7502-668-2

163 EU restrictive measures against Russia over Ukraine (since 2014). (online, cit. 07.10.2023). Dostupné na internete: <<https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/>>

164 Potential Sanctions Evasion with Cryptocurrency. (online, cit. 2023). Dostupné na internete: <<https://crsreports.congress.gov/product/pdf/IN/IN11920>>

hodnotu amerického dolára TX5GV4DyfxNB3rPkzZJhmqZ1efVmL4rEqG. Prípadne poskytovateľ služby kryptoaktív aktívny v Rusku GARANTEX EUROPE OU, známy zapojením do legalizácie výnosov z trestnej činnosti rôznych hackerských skupín ako je napríklad severokórejská skupina Lazarus Group, a jej sankcionované verejné adresy kryptoaktíva Bitcoin 3Lpoy53K625zVeE47ZasiG5jGkAxJ27kh1, alebo kryptoaktíva Ethereum 0x7FF9cFad3877F21d41Da833E2F775dB0569eE3D9.¹⁶⁵ Identifikácia verejných adries a ich priradenie nie je jednoduchý proces. No na jeho realizáciu možno použiť metódy analýzy distribuovanej databázy transakcií, trasovania a vykonávania prvkov súčinnosti a spolupráce s poskytovateľmi služby kryptoaktív a finančnými spravodajskými jednotkami jednotlivých štátov.

Kvantitatívne tieto skutočnosti potvrdzujú aj výsledky výskumnej činnosti spoločností, ktoré realizujú skúmanie systému kryptoaktív. Od začiatku rusko-ukrajinského hybridného konfliktu bolo len do marca 2022 vykonaných transakcií kryptoaktív v hodnote prevyšujúcej 62 miliónov amerických dolárov z identifikovaných ruských verejných adries. Väčšina týchto transakcií bola určená vysoko rizikovým pôvodom a skrz formu OTC obchodov. Forma OTC transakcií je rizikovejšou formou, než je forma nákupu alebo predaja kryptoaktíva priamo s poskytovateľom služby kryptoaktív. Ten vie určiť pôvod svojich kryptoaktív. Avšak pri OTC transakciách dochádza zo strany poskytovateľa služby kryptoaktív len k sprostredkovaniu transakcie medzi jednotlivými subjektmi s neznámym pôvodom kryptoaktív. Niektorí autori subsumujú pod OTC formu obchodu aj P2P formu obchodu alebo tzv. vextl kryptoaktív. Podľa indexu Cambridge Bitcoin Electricity Consumption, ktorý hodnotí koľko elektrickej energie sa globálne využíva na zabezpečenie funkčnosti systému kryptoaktíva Bitcoin bolo Rusko koncom Augusta 2021 umiestnené na treťom mieste v mňaní množstva elektrickej energie na zabezpečovanie funkčnosti kryptoaktíva Bitcoin. Táto skutočnosť bezpochyby súvisí s prílevom kapitálu do krajiny, čo je opäť forma, ako sa vyhnúť sankciám, keďže presun hodnoty medzinárodného obchodu bol Rusku obmedzený skrz zablokovanie prístupu do medzinárodného transakčného toku SWIFT. Prísun kapitálu do krajiny si Rusko v súvislosti s kryptoaktívami zaisťuje aj skrz činnosť hackerských skupín využívajúcich metódy hackerských útokov na decentralizované financie, smart kontrakty alebo hackerských útokov známych ako ransomware útoky, resp. prostredníctvom poskytovania služieb výmeny kryptoaktív, pri ktorých nie sú dodržiavané AML opatrenia.¹⁶⁶

Systém kryptoaktív tak ako akákoľvek digitálna technológia môže byť zneužitá na účely hybridného konfliktu. Jej zrušenie alebo *en bloc* zákaz neprichádza do úvahy. Je preto vhodné venovať sa erudícii v tejto oblasti, pochopiť systém kryptoaktív a využívať dostupné metódy, ako je analýza distribuovanej databázy transakcií, trasovanie kryptoaktív a identifikácia verejných adries za účelom regulovania tejto technológie. Zvolenie efektívneho prístupu k tejto technológii bude mať za následok udržanie etického a morálneho rozvoja systému kryptoaktív.¹⁶⁷

165OFAC sanction list search. (online, cit. 07.10.2023). Dostupné na internete: <<https://sanctionsearch.ofac.treas.gov/>>

¹⁶⁶ ŠANTA, J., ŠANTA, I.: K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami In: Justičná revue. – Roč. 75, Vydanie 5/2023, s. 640 – 643

¹⁶⁷ Cryptocurrency Brings Millions in Aid to Ukraine, But Could It Also Be Used For Russian Sanctions Evasion? (online, cit. 07.10.2023). Dostupné na internete: <<https://www.chainalysis.com/blog/cryptocurrency-ukraine-russia-sanctions/>>

2. DIGITÁLNY PRENOS INFORMÁCIÍ AKO HYBRIDNÁ HROZBA

V súčasnej dobe žijeme vo svete, kde digitálny prenos informácií zohráva kľúčovú úlohu v našom každodennom živote. Internet, sociálne siete a elektronická komunikácia sa stali neodmysliteľnou súčasťou našej existencie. Zároveň sa však stáva zrejším, že digitálny prenos informácií môže byť použitý ako nástroj na dosiahnutie rôznych cieľov, vrátane tých nekalých. Hybridná hrozba spočíva v tom, že zahrňuje kombináciu tradičných a **digitálnych techník** na dosiahnutie politických, ekonomických alebo vojenských cieľov, a predstavuje novú výzvu pre bezpečnosť a ochranu nášho spoločenstva.¹⁶⁸

Digitálny prenos informácií ako nástroj hybridnej hrozby sa stáva stále sofistikovanejším. Často sa začína v online prostredí, kde môžu byť dezinformácie, propagandistické kampane a kybernetické útoky ľahko šírené. Tieto digitálne nástroje môžu slúžiť rôznym cieľom, vrátane oslabenia dôvery verejnosti voči inštitúciám, destabilizácie politických systémov a dokonca vyvolania konfliktov.¹⁶⁹

Jedným z príkladov hybridnej hrozby, ktorá využíva digitálny prenos informácií, sú dezinformačné kampane. Agentúry alebo štátne inštitúcie môžu vytvoriť falošné správy, ktoré majú ovplyvniť verejnú mienku. Tieto správy môžu byť následne šírené cez sociálne siete a online médiá, čím sa dostanú k veľkému množstvu ľudí. Týmto spôsobom môže byť verejná mienka zmanipulovaná, a to bez použitia vojenských síl.

2.1 Dezinformácie ako hybridné hrozby

V oblasti spoločenských vied nachádzame poznatky o mnohých faktoroch, ktoré sú úzko prepojené s vierou v pravdivosť dezinformácií. Môžeme hovoriť o faktoroch, ktoré sa dotýkajú napríklad osobnosti človeka, spôsobu akým zvykne uvažovať nad vecami vo svojom okolí, ale aj toho, z akého prostredia pochádza.¹⁷⁰ Vzhľadom k tomu, koľko dezinformácií sa dnes vyskytuje v našom okolí, je takmer nemožné, aby ktokoľvek z nás nikdy žiadnej „nenaletel“. Dezinformácie sú vo svojej podstate vytvorené tak, aby boli pre ľudí prirodzene pútavé, pritiahli ľudskú pozornosť a aby intuitívne dávali zmysel a nútili ľudí pýtať sa, či všetko náhodou nie je úplne inak, ako sme si doposiaľ mysleli. V súčasnosti existujú tri najznámejšie psychologické mechanizmy, ktoré sú spojené s vyššou náchylnosťou k rôznym typom dezinformácií.¹⁷¹

Prvý mechanizmus súvisí s **prínosom kvanta informácií**, ktoré na jedinca pôsobia zo všetkých strán. Je prirodzené, že nie všetky informácie dokáže človek správne vyhodnotiť. V mnohých prípadoch sa stáva, že napríklad v časovej tiesni, pod váhou emócií alebo pod vplyvom názorov ľudí z blízkeho okolia človek podľa neho skratkovitému uvažovaniu a uverí aj niečomu, čomu by bežne neuveril. Dôležitou súčasťou skratkovitého uvažovania je to, že človek si automaticky predstavuje súvislosti aj medzi úplne náhodnými udalosťami. Veľmi dobrým príkladom v tejto oblasti boli dezinformácie šírené s ochorením COVID-19. Ľudia si v súvislosti s týmto ochorením často spájali rôzne iné nesúvisiace informácie, ako napríklad to, keď človek zomrel na uvedenú

¹⁶⁸ Hybridné hrozby na SR. (online, cit. 13.10.2023). Dostupné na internete: <https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf>

¹⁶⁹ Nástroje hybridných hrozieb. (online, cit. 13.10.2023). Dostupné na internete: <<https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/>>

¹⁷⁰ S Brotherton R.: Suspicious minds: Why we believe conspiracy theories, Bloomsbury Publishing, 2015

¹⁷¹ Uscinski J. E.: Conspiracy theories and the people who believe them, Oxford University Press 2018

chorobu, tak sa zaujímali či bol zaočkovaný alebo nie, koľko mal očkovacích dávok a pod. Takéto vzájomné prepájanie udalostí je veľmi bežnou súčasťou skratkovitého uvažovania. V mnohých prípadoch sa stáva, že človek v rýchlosti vyvodí nejaký mylný záver a až následne, keď sa nad ním hlbšie zamyslí, zistí, že existuje aj iné, jednoduchšie a pravdepodobnejšie vysvetlenie. Takéto skratkovité uvažovanie v značnej miere pomáha šíriteľom dezinformácií, ktorí sa často snažia k niečomu ľuďi dotlačiť, napr. „zdieľajte, kým to nezmažú“. Vyvolávanie pocitu, že človek musí konať rýchlo ho navedú k tomu, že prezdieľa alebo dokonca aj uverí takým tvrdeniam, nad ktorými sa poriadne nezamyslí.¹⁷²

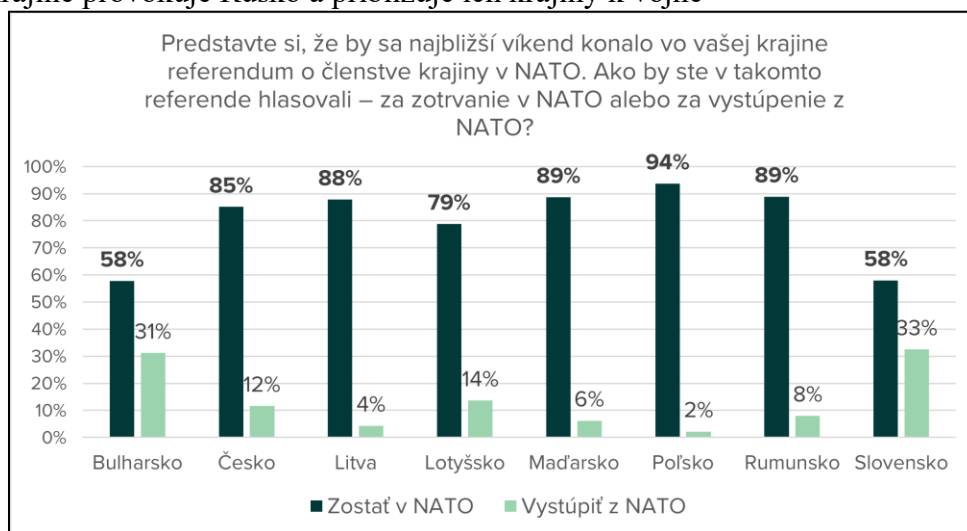
Druhým častým prvkom pri šírení dezinformácií je **náznak ohrozenia**, ktorý vplýva na myšlienkovú a aj emocionálnu stránku jedinca. Pod váhou emócií dokáže človek ľahšie podľahnúť skratkovitému uvažovaniu. Niektoré pocity dokážu byť natoľko nepríjemné, že sa ich človek snaží najskôr vytlačiť preč. Preto ľahšie uverí takým tvrdeniam, ktoré napomáhajú pocit úzkosti, či bezmocnosti dostať pod kontrolu bez toho, aby sa človek dokázal lepšie zamyslieť nad ich pravdivosťou. Mnoho ľudí počas pandémie COVID-19 na Slovensku uverilo dezinformácii, že ochorenie COVID-19 v skutočnosti neexistuje a celá pandémia je iba hoax. Ak zvážime koľko rôznych politikov, lekárov, či vedcov by sa muselo po celom svete potajme dohodnúť, aby vzbudili dojem celosvetovej pandémie, zrejme si uvedomíme, že tento názor je vysoko nepravdepodobný. Aj napriek tomu, mnohí ľudia tejto možnosti aspoň na istý čas uverili. Takéto presvedčenie im mohlo dočasne pomôcť zbaviť sa veľkého náporu strachu o seba, svojich blízkych. Vyvolávanie pocitu ohrozenia a tiež prípadné poskytovanie úniku pred strachom je účinným mechanizmom využívaným pri šírení dezinformácií.

S vyvolaním strachu a nenávisti súvisí aj tretí prvok šírenia dezinformácií, ktorý vyvoláva **pocit strachu z niečoho alebo pocit nenávisti voči vonkajšiemu nepriateľovi**, ktorý zdanlivo ohrozuje našu vlastnú skupinu. V tomto prípade nemusí ísť o skutočnú hrozbu, môže to byť aj hrozba domnelá. Typickým príkladom pre tento prvok, bola migračná kríza v Európe, pri ktorej sa niektorým skupinám ľudí podarilo vyvolať na Slovensku obrovský strach z prichádzajúcich migrantov. Takéto vyvolávanie strachu a nenávisti z údajných vonkajších nepriateľov je známou taktikou na odpútanie pozornosti ľudí od iných, skutočných a závažnejších problémov.

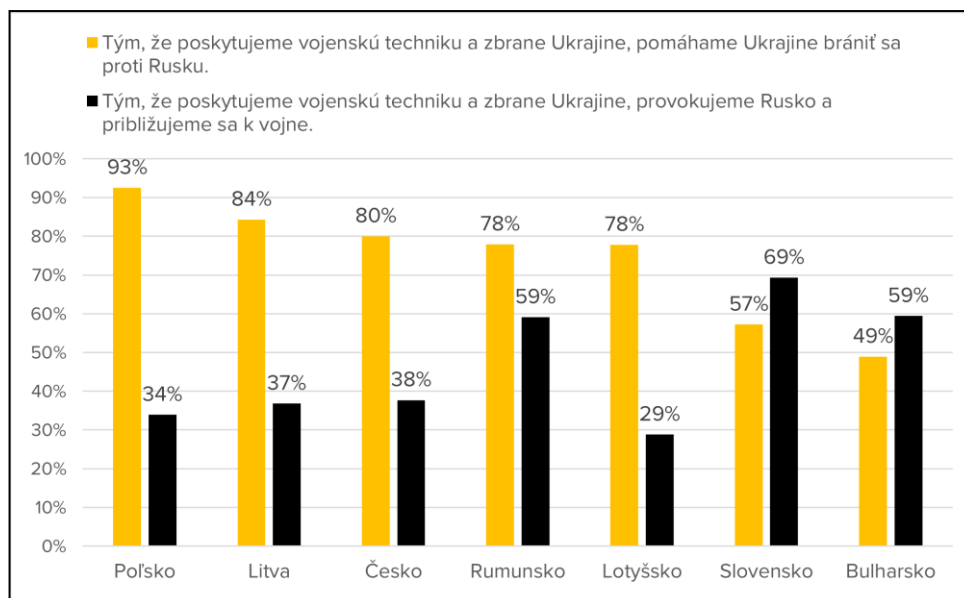
Z prieskumov GLOBSEC – mimovládnej organizácie, dlhodobo vyplýva, že Slovensko v hoaxových rebríčkoch obsadzuje dlhodobo nelichotivé miesta. Aj keď sú hoaxy považované za celosvetový problém, napriek tomu existujú v tejto oblasti regionálne rozdiely. Výsledky uvedených prieskumov poukazujú na to, že Slováci sú najviac náchylní uveriť konšpiračným teóriám z krajín Vyšehradskej štvorky, tzv. V4. Či už ide o dezinformácie o pandémii COVID-19, migračnej kríze, či vojne na Ukrajine, mnohé rezonujú medzi tretinou až polovicou obyvateľov, a to bez ohľadu na vzdelanie, vekové skupiny či bydlisko. Naprieč všeobecne vysokej popularite dezinformácií vieme v krajine definovať typy, ktoré sú náchylnejšie veriť manipulatívnym informáciám. Sú to prevažne starší ľudia, ľudia s nižším vzdelaním a tí, ktorí neveria médiám a nie sú spokojní s demokraciou. Najnovší prieskum verejnej mienky, ktorý GLOBSEC uskutočnil v ôsmich krajinách strednej a východnej Európy (Bulharsko, Česko, Maďarsko, Lotyšsko, Litva, Poľsko, Rumunsko a Slovensko) skúma postoje regiónu ku kľúčovým naratívom – pravdivým aj manipulatívnym.

¹⁷² Risen, J. L.: Believing what we do not believe: Acquiescence to superstitious beliefs and other powerful intuitions, *Psychological Review*, 2016, 123(2), 182.

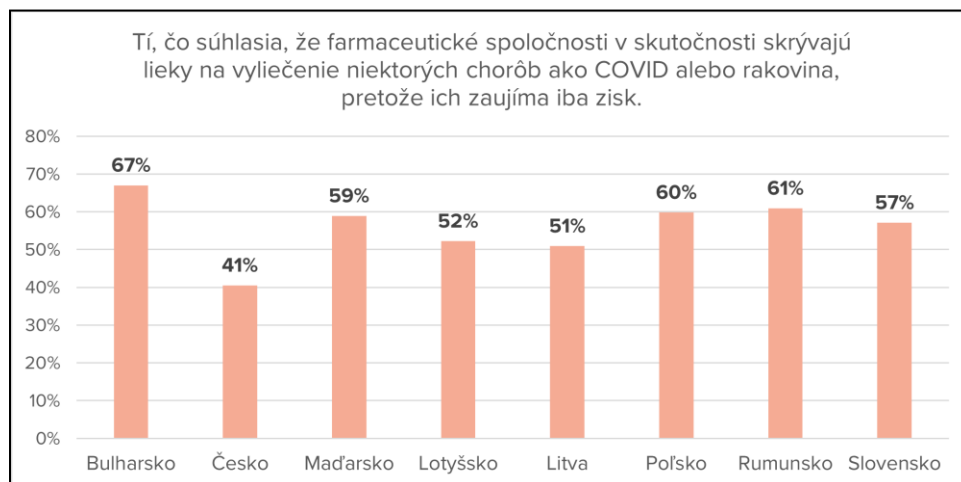
Priemerná podpora členstva v NATO v regióne je 79 %, ale údaje sa v jednotlivých krajinách výrazne líšia. Na jednej strane členstvo podporuje 94 % Poliakov a na druhej strane 58 % Slovákov a Bulharov. Podobne v priemere 74 % respondentov uznáva, že vojenská podpora Ukrajine jej pomáha brániť sa proti Rusku, ale na Slovensku a v Bulharsku si viac ľudí myslí, že vojenská pomoc Ukrajine provokuje Rusko a približuje ich krajiny k vojne



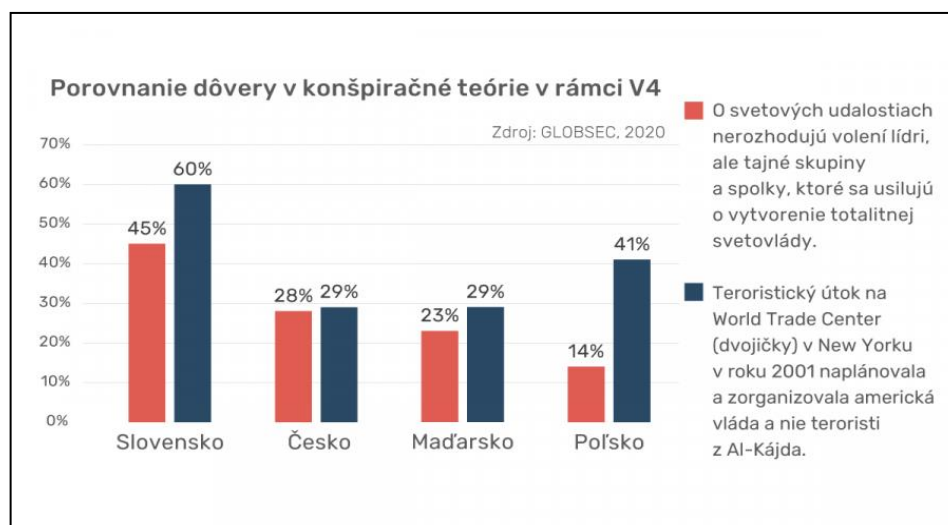
"Slovensko je príkladom toho, čo sa môže stať, keď skombinujeme nedôveru v inštitúcie, spoločnosť s náchylnosťou veriť dezinformáciám a silných politických aktérov, ktorí vedia využiť frustrácie a obavy spoločnosti vo svoj prospech. Sme poznačení politickým chaosom a zmätkami spôsobenými vládnuťou koalíciou v rokoch 2020 až 2023. Aktuálne máme na Slovensku historicky najnižšiu mieru dôvery v inštitúcie, kedy vláde dôveruje len 18 % respondentov. Tento nedostatok dôvery vytvoril živnú pôdu pre časť opozičných strán na kampaň obviňujúcu Západ z vojny a podkopávanie podpory Ukrajine, ktorá našla odozvu u značnej časti obyvateľstva," vysvetlila Katarína Klingová, senior analytička GLOBSECu.



GLOBSEC Trends tento rok poukazuje aj na to, ako vplyv dezinformácií týkajúcich sa zdravia, ktoré sa šírili počas pandémie COVID-19, prispeli k nedôvere voči farmaceutickým spoločnostiam, zdravotníckym organizáciám a očkovaníu. Približne 37 % obyvateľov regiónu strednej a východnej Európy sa domnieva, že vakcíny proti COVID-19 zvyšujú riziko predčasných úmrtí, a 56 % podozrieva farmaceutické spoločnosti, že z dôvodu zisku zatajujú účinné spôsoby liečby chorôb, ako je COVID-19 a rakovina. „Tieto nálady rezonujú aj v spoločnostiach, ktoré vykazujú väčšiu odolnosť voči geopolitickým dezinformáciám, ako sú Česko a Poľsko. Ak chceme byť lepšie pripravení na budúce zdravotné krízy by sme túto nedôveru mali riešiť teraz, keď zdravie nie je témou číslo jedna politickej agendy,“ dodala D. Hajdu.¹⁷³



Dezinformačné šírenie rôznymi aktérmi na Slovensku, od politikov cez širokú sieť webstránok a facebookových skupín v online priestore vytvára rôzne názorové bubliny, ktoré dokážu utvrdiť každého v jeho vlastných domnienkach a tým zatvárajú prístup do svetov iných. Početné množstvo ľudí sa uchýľuje ku konšpiračným teóriám s cieľom zjednodušiť si odôvodnenie vecí, ktorým dnes nie ľahké porozumieť. Svet sa rýchlo mení a je plný zložitých javov, preto uveriť konšpiračným



¹⁷³Nový prieskum GLOBSEC-u. (online, cit. 13.10.2023). Dostupné na internete: <<https://www.globsec.org/what-we-do/press-releases/novy-prieskum-globsec-u-slovensko-zaznamenalo-vyrazny-prepad-v/>>

teóriám predstavuje spôsob, ako si v živote nájsť nové istoty. Takýmto konaním môže človek pocítiť výnimočnosť, že patrí k „vyvolenej“ skupine, ktorá pozná „ozajstnú pravdu“.¹⁷⁴

2.2. Kritické myslenie a mediálna gramotnosť

Kritické myslenie a mediálna gramotnosť patria medzi základné prvky, ktoré sú nevyhnutné pre analýzu a následnú interpretáciu moderných informácií. Rýchle šírenie chybných informácií a dezinformácií sa v posledných rokoch, práve vďaka rozvoju a zvyšovaniu dostupnosti internetu stalo masovým fenoménom. Dezinformácie využívajú klamstvá a podvody s cieľom zmanipulovať jedinca spôsobom vyhovujúcim ich tvorcom. Občas dokonca tvorcovia dezinformácií využívajú pravdivé, faktami podložené informácie, ktoré prekrúčia vytrhnutím z kontextu alebo zmenou rámca. Ako najefektívnejšie dezinformácie môžeme považovať tie, ktoré sú akousi zmesou pravdivých a nepravdivých informácií.¹⁷⁵

Za najúčinnjší spôsob ako bojovať proti dezinformáciám, je využitie analytických schopností, ktorých pomocou dokážeme preskúmať čo čítame, sledujeme, či počujeme a to racionálnym, logickým a nezaujatým spôsobom. Tento spôsob umožňuje lepšie identifikovanie jednotlivých faktami podložených informácií a odlíšiť ich od nepravdivých a klamlivých informácií. Pri analýze je z hľadiska dôveryhodnosti užitočné zaoberať sa otázkami ako: „Kto je autorom – šíriteľom danej informácie?, Aký jazyk a gramatiku príspevok používa a aké pocity vyvoláva?, Z ktorého obdobia informácia pochádza? Sú používané údaje stále relevantné?“¹⁷⁶

Vedomosť kto je autorom a distribútorom konkrétnej informácie, môže pomôcť pri odpovedi na otázku, či ide o spoľahlivé spravodajstvo. Tento údaj môže byť užitočným ukazovateľom práve toho, kedy treba byť opatrný. Ak chce človek zistiť kto je producentom konkrétneho média, zväčša stačí len jednoduché vyhľadanie na internete. Zároveň je potrebné overiť si vierohodnosť toho daného zdroja informácií aj prostredníctvom rôznych webstránok overovačov faktov tzv. „*fact-checkers*“. V prípade slovenských zdrojov je nápomocný portál konšpiratori.sk, ktorý zverejňuje zoznam konšpiračných teórií, dezinformačných médií či webov. V prípade jazyka a gramatiky je hovorový, vulgárny alebo emotívny jazyk varovným signálom, že to, čo si človek prezerá alebo číta, môže byť dezinformácia. Samotné dezinformácie svojou povahou manipulujú, a preto sú presýtené emotívnym jazykom a obrazmi. Kvalitné médiá len zriedkavo využívajú veľké písmená na zdôraznenie svojho názoru. Titulky plné veľkých písmen a výkričníkov spravidla znamenajú, že ide o šírenie novej dezinformácie. Dezinformácie sa šíria aj formou klikacích návodov tzv. „*clickbaitových článkov*“, ktoré využívajú práve tento typ jazyka s prvkami dôverného a hovorového tónu. V mnohých prípadoch sa stáva, že sú články, videá alebo obrázky „recyklované“. Dezinformačné kampane využívajú aj niekoľko rokov staré obrázky a videá práve pre aktuálne príbehy. Cieľom je použiť emocionálne šokujúce alebo násilné obrázky na vyvolanie strachu. Účinnými nástrojmi v boji proti dezinformáciám, ktoré pomôžu nestratiť sa v kvante

¹⁷⁴ Slováci veria hoaxom viac ako iné národy, prečo je to tak. (online, cit. 13.10.2023). Dostupné na internete: <<https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/>>

¹⁷⁵ Stengel, R.: Information Wars. 2019, New York: Atlantic Monthly Press, str. 290

¹⁷⁶ Cillizza, C. (2019, February 19). Why our politics can't handle Jussie Smollett. CNN Politics. (online, cit. 13.10.2023). Dostupné na internete: <<https://edition.cnn.com/2019/02/18/politics/jussie-smollett-politics/index.html/>>

informácií môžu byť aj stránky: Hoaxy a podvody – Polícia SR, Hoax.sk, Demagog.sk, Pouzimerozum.sk, či Argumentuj.sk.¹⁷⁷

Vyvolanie pocitu dôvery a začlenenia sa do spoločnosti predstavujú kľúčovú rolu pre fungujúcu demokraciu. Boj s korupciou a klientelizmom, ktoré bránia uprednostňovaniu určitých skupín obyvateľstva pred inými, ako aj reforma vzdelávania, v ktorej sa bude práve poukazovať na dôležitosť kritického myslenia a vysvetlenie fungovania demokracie i života v nej, sú primárnymi prvkami štrukturálnych zmien, ktoré sa v spoločnosti musia odohrať. V individuálnej rovine sa síce môže každý snažiť filtrovať čas strávený na sociálnych sieťach, ktoré sú dnes hlavným ohniskom konšpiračných teórií a dezinformácií, ale je dôležité byť aktívnejším užívateľom namiesto pasívneho konzumovania a viac komunikovať mimo virtuálnej reality. Ak sa človek už rozhodne zapájať do konverzácií nie len v offline ale aj v online priestore, je dôležité dbať o slušnú komunikáciu a overiť si informácie predtým ako sa ich rozhodne zdieľať v informačnom priestore.¹⁷⁸

Zdroje

1. ŠANTA, J., ŠANTA, I.: K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami In: Justičná revue. – Roč. 75, Vydanie 5/2023, s. 636 – 650
2. ŠANTA, J., ŠANTA, I.: Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty. Praha: Leges, 2023. 199 strán. ISBN: 978-80-7502-668-2
3. Awesome zero knowledge proofs. (online, cit. 07.10.2023.) Dostupné na internete: <<https://github.com/matter-labs/awesome-zero-knowledge-proofs>>
4. Introduction to smart contracts. (online, cit. 07.10.2023). Dostupné na internete: <<https://ethereum.org/en/smart-contracts/>>
5. Posilňovanie odolnosti voči hybridným hrozbám. (online, cit. 07.10.2023). Dostupné na internete: <<https://www.mzv.sk/diplomacia/bezpecnostna-politika/hybridne-hrozby>>
6. Cryptocurrency Brings Millions in Aid to Ukraine, But Could It Also Be Used For Russian Sanctions Evasion? (online, cit. 07.10.2023). Dostupné na internete: <<https://www.chainalysis.com/blog/cryptocurrency-ukraine-russia-sanctions/>>
7. EU restrictive measures against Russia over Ukraine (since 2014). (online, cit. 07.10.2023). Dostupné na internete: <<https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/>>
8. OFAC sanction list search. (online, cit. 07.10.2023). Dostupné na internete: <<https://sanctionssearch.ofac.treas.gov/>>
9. Potential Sanctions Evasion with Cryptocurrency. (online, cit. 2023). Dostupné na internete: <<https://crsreports.congress.gov/product/pdf/IN/IN11920/>>
10. Hybridné hrozby na SR. (online, cit. 13.10.2023). Dostupné na internete: <https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickich-oblasti.pdf>
11. Nástroje hybridných hrozieb. (online, cit. 13.10.2023). Dostupné na internete: <<https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/>>

¹⁷⁷ Každý druhý Slovak verí konšpiráciám. (online, cit. 13.10.2023). Dostupné na internete: <<https://eduworld.sk/cd/janka-horniakova/8510/kazdy-druhy-slovak-veri-konspiraciám/>>

¹⁷⁸ Slováci veria hoaxom viac ako iné národy. (online, cit. 13.10.2023). Dostupné na internete: <<https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/>>

12. S Brotherton R. :Suspicious minds: Why we believe conspiracy theories. Bloomsbury Publishing, 2015.298 strán. ISBN 978-1-4729-1564-1
13. Uscinski J. E.: Conspiracy theories and the people who believe them. Oxford University Press 2018. 560 strán. ISBN 978-0-1908-4408-0
14. Risen, J. L. (2016). Believing what we do not believe: Acquiescence to superstitious beliefs and other powerful intuitions. *Psychological Review*, 123(2), 182–207
15. Hybridné hrozby na SR. (online, cit. 13.10.2023). Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickyh-oblasti.pdf/>
16. Nástroje hybridných hrozieb. (online, cit. 13.10.2023). Dostupné na internete: <<https://www.hybridnehrozby.sk/1648/nastroje-hybridnych-hrozieb/>>
17. Stengel, R.: Information Wars. 2019, New York: Atlantic Monthly Press, 384 strán. ISBN 978-0-8021-4799-8
18. Cillizza, C. (2019, February 19). Why our politics can't handle Jussie Smollett. CNN Politics. (online, cit. 13.10.2023). Dostupné na internete: <<https://edition.cnn.com/2019/02/18/politics/jussie-smollett-politics/index.html/>>
19. Cillizza, C. (2019, February 19). Why our politics can't handle Jussie Smollett. CNN Politics. (online, cit. 13.10.2023). Dostupné na internete: <<https://edition.cnn.com/2019/02/18/politics/jussie-smollett-politics/index.html/>>
20. Každý druhý Slovák verí konšpiráciám. (online, cit. 13.10.2023). Dostupné na internete: <<https://eduworld.sk/cd/janka-horniakova/8510/kazdy-druhy-slovak-veri-konspiraciam/>>
21. Slováci veria hoaxom viac ako iné národy. (online, cit. 13.10.2023). Dostupné na internete: <<https://vedanadosah.cvtisr.sk/ludia/sociologia/slovaci-veria-hoaxom-viac-ako-ine-narody-preco-je-to-tak/>>

HOAX, JEHO PODSTATA A VNÍMANIE

doc. Ing. Miroslav Gombár, PhD., prof. Ing. Antonín Korauš, PhD., MBA, LL.M., prof. RNDr. Šárka Mayerová, Ph.D., doc. PaedDr. Alena Vagaská, PhD.

Prešovská univerzita v Prešove, Fakulta manažmentu, ekonomiky a obchodu, miroslav.gombar@unipo.sk; Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu, antonin.koraus@akademiapz.sk; Univerzita obrany v Brně, Fakulta vojenských technológií, sarka.mayerova@unob.cz; Technická univerzita v Košiciach, Fakulta výrobných technológií, alena.vagaska@tuke.sk

Abstrakt Výskum zameraný na porozumenie vnímaniu a schopnosti identifikovať hoax zo strany rôznych vekových kategórií na Slovensku priniesol veľmi zaujímavé výsledky. Analýzy ukázali signifikantný vzťah medzi vekom respondenta a jeho presvedčením o tom, že rozumie pojmu hoax a dokáže ho identifikovať, s konkrétnymi odchýlkami v názoroch a sebavedomí medzi rôznymi vekovými skupinami. Mladšie skupiny, napriek vysokému percentu tvrdení, že rozumejú pojmu a dokážu identifikovať hoax, predstavujú zaujímavý priestor na ďalší výskum vzhľadom na to, či ich sebavedomie odráža reálnu kompetenciu. Stredné vekové kategórie sa zdali byť sebavedomé vo svojich schopnostiach detekcie hoaxu, avšak otázky ostávajú o vplyve životných skúseností a kontextu na ich presvedčenia. Staršie generácie ukázali úplný nesúhlas s neschopnosťou identifikovať hoax, čo otvára debatu o možných kultúrnych alebo sociálnych faktoroch ovplyvňujúcich ich odpovede. Na záver, významné množstvo respondentov vníma hoax ako vážny problém pre Slovensko, pričom existuje signifikantný vzťah medzi vekom a touto perspektívou. Tieto zistenia otvárajú cestu pre ďalšiu diskusiu a analýzu o tom, ako sebavedomie a vnímanie hrozieb hoaxu sa prejavujú naprieč generáciami a ako tieto postoje môžu byť ovplyvnené osobnými a sociálnymi faktormi..

Kľúčové slová: hoax, vnímanie, identifikácia, problém.

ÚVOD

Hoax možno definovať ako zámerne vymyslenú alebo klamlivú nepravdu, ktorá sa často šíri s úmyslom oklamať alebo zavádzať ostatných. Hoaxy môžu mať rôzne podoby vrátane písaných textov, obrázkov, videí alebo dokonca napodobňovania identity. Prístupy k definovaniu hoaxu sa líšia v závislosti od kontextu a zámeru podvodu. Niektorí výskumníci napríklad definujú hoax ako text „zámerne napísaný s cieľom zavádzať spotrebiteľov“. Iní zdôrazňujú úlohu mocenských vzťahov a tvrdia, že hoax zahŕňa výkon moci nad oklamanými. Jedným z prístupov k definovaniu hoaxu je jeho odlíšenie od falošných správ. Falošné správy, podobne ako hoax, zahŕňajú šírenie nepravdivých informácií. To, čo však hoax odlišuje od falošných správ, je zámer, ktorý sa za ním skrýva. Hoax je zámerne vytvorený s cieľom klamať alebo zavádzať ostatných, zatiaľ čo falošné správy môžu obsahovať nepravdivé informácie bez výslovného zámeru klamať. Powell túto definíciu dopĺňa tvrdením, že nespravodlivé mocenské vzťahy sú ústredným bodom hoaxov, pretože podvodník vykonáva moc nad oklamanými tým, že ich úmyselne zavádza (Finneman & Thomas, 2018). Okrem toho sa hoaxy môžu považovať za pokusy o podvod, ktorých cieľom je manipulovať vnímanie verejnosti, narušovať dôveru v určité entity alebo informačné zdroje a vykonávať kontrolu nad presvedčením a konaním spoločnosti (Nihayah & Adila, 2020). Navyše, hoaxy možno vnímať ako pokus o oklamanie čitateľov a poslucháčov falošných správ, aj keď si tvorcovia hoaxu uvedomujú, že informácie sú nepravdivé.

Prístupy k definovaniu hoaxu možno kategorizovať do niekoľkých perspektív. Jednou z perspektív je náboženská perspektíva, ako sa uvádza v článku Selly „The Qur'anic Views of the reality of hoaxes“. V tejto perspektíve sa hoaxy chápu ako ohováranie alebo falošné obvinenia s cieľom

poraziť protivníkov alebo nepriateľov. Hoaxy sú tiež vnímané ako rýchlo sa šíriace správy, ktoré majú schopnosť ovplyvňovať ostatných. Ďalšou perspektívou je perspektíva gramotnosti, o ktorej hovorila Lina Meilita Rahayu vo svojom spise „Pochopenie textu boja proti fenoménu hoaxov“. Podľa tejto perspektívy sú hoaxy definované ako zámerné nepravdy šírené prostredníctvom písaných textov a iných foriem médií s cieľom oklamať alebo zavádzať publikum. Jedným z navrhovaných riešení boja proti hoaxom je zlepšiť kultúru gramotnosti prostredníctvom vzdelávania a podpory zručností kritického myslenia.

Ďalším prístupom k definovaniu hoaxov je hermeneutická perspektíva, ktorú skúmal Syaiful Ilham vo svojej štúdii „Fenomén podvodu: Kritická perspektíva“. Podľa tejto perspektívy sú hoaxy vnímané ako diskurzívne praktiky, ktoré formujú významy a interpretácie udalostí alebo javov. Nie sú to len nepravdivé informácie, ale skôr strategické a zámerné konštrukcie zamerané na manipuláciu vnímania verejnosti. Tretím prístupom k definovaniu hoaxov je právna perspektíva, o ktorej hovorili Quintanilla et al. vo svojom článku „Právne pohľady na hoaxy a falošné správy“. Podľa tejto perspektívy možno hoaxy definovať ako zámerne nepravdivé informácie alebo klamlivé praktiky, ktoré sú určené na klamanie a zavádzanie iných na rôzne účely. Tieto účely môžu siahať od spôsobenia škody jednotlivcom alebo inštitúciám, šírenia dezinformácií pre osobný prospech alebo manipulácie verejnej mienky z politických alebo sociálnych dôvodov. Z týchto rôznych uhlov pohľadu je evidentné, že hoaxy sú zámerne klamlivé praktiky, ktorých cieľom je šíriť nepravdivé informácie a manipulovať s vnímaním publika. Hoaxy možno kategorizovať do rôznych perspektív, ktoré pomáhajú definovať ich povahu a dopad. Celkovo možno hoax definovať ako úmyselne nepravdivé informácie alebo klamlivé praktiky, ktoré sa šíria s cieľom oklamať a zavádzať ostatných. V dnešnom rýchlo sa meniacom svete nemožno význam presných informácií preceňovať. V dnešnom rýchlo sa meniacom svete nemožno význam presných informácií preceňovať. Hoaxy majú niekoľko negatívnych dopadov, ako je poškodenie dôveryhodnosti a integrity organizátorov a politikov, ktorí súperia vo všeobecných voľbách, spôsobujú nepokoje alebo rozruch v spoločnosti a rozdeľujú národnú jednotu (Rohmah & Kusromaniah, 2021). Hoaxy majú tiež potenciál ovplyvniť politické voľby, majú škodlivé účinky na zdravie jednotlivcov a vytvárajú javy nenávisti a diskriminácie. Preto je kľúčové vyvinúť prístupy, ktoré môžu ľuďom pomôcť posúdiť dôveryhodnosť informácií a kriticky myslieť (Benamara et al., 2018). Hoaxy, ako ich definujú rôzne perspektívy, zahŕňajú zámerné šírenie nepravdivých informácií alebo zapájanie sa do podvodných praktík s cieľom o klamaní a zavádzaní iných. Tieto hoaxy môžu mať rôzne formy, vrátane falošných správ, dezinformácií alebo strategických manipulácií s udalosťami alebo javmi (Jannana et al., 2021).

Hoax je teda možné definovať v troch základných rovinách:

1. Všeobecná definícia: Hoax sa zvyčajne chápe ako zámerne vymyslená lož, ktorá sa vydáva za pravdu. Od podvodu sa líši v tom, že podvodník sa často snaží oklamať obeť, aby uverila nepravdivému tvrdeniu bez toho, aby nevyhnutne hľadala nejaký materiálny zisk (Boese, 2002).
2. Psychologická/sociálna definícia: Niektorá literatúra sa ponorí do psychologických aspektov hoaxov a nedefinuje ich len ako jednoduché podvody, ale aj ako podvody, ktoré využívajú ľudské predsudky, sociálne správanie a kolektívne systémy viery. Hoaxy sa v tomto svetle považujú za sociálne alebo psychologické javy, ktoré skúmajú kolektívne systémy viery a spoločenské obavy (Bartholomew, 2006).
3. Médiá a digitálne podvody: S príchodom digitálnych médií sa podvody vyvinuli tak, aby využívali rýchle šírenie informácií online. Internetové hoaxy a falošné správy sa môžu šíriť

virálne a ich cieľom je často vytvárať príjmy z reklamy, manipulovať s vnímaním verejnosti alebo jednoducho žartovať verejnosť. Definícia v tejto oblasti často zdôrazňuje použité médium (t. j. digitálne kanály) a rýchlosť a jednoduchosť šírenia (Tandoc, 2018).

Na základe vyššie uvedených skutočností a základných prístupov k pojmu hoax môžeme hoaxy klasifikovať podľa diferentných kritérií ako:

1. Klasifikácia podľa účelu (Sobieraj, 2010):

- Pre zisk: Hoaxy, ktorých cieľom je získať finančný zisk, pričom často využívajú strach alebo presvedčenie ľudí.
- Pre pozornosť: Niektoré hoaxy sú vytvorené jednoducho s cieľom získať pozornosť alebo trollovať verejnosť bez akéhokoľvek základného zámeru alebo úmyslu ublížiť.
- Škodlivý alebo škodlivý: Hoaxy, ktorých cieľom je vyvolať paniku, narušiť spoločenský mier alebo poškodiť povest' jednotlivcov alebo subjektov.

2. Klasifikácia podľa obsahu (Helling, 2017):

- Vedecké podvody: Falzifikácie v oblasti vedeckého výskumu a objavov, ako napríklad Piltdown Man.
- Umelecké podvody: Vytváranie alebo pripisovanie umeleckých diel, ktorých cieľom je oklamať odborníkov a verejnosť, ako je to v prípade Vermeerových falzifikátov.
- legendy: Široko šírené príbehy, ktorým verejnosť verí, ale nemajú overiteľný základ, ako napríklad aligátory v kanalizačnom systéme v New Yorku.

3. Klasifikácia podľa kanála (Zollmann, 2016):

- Tradičné mediálne podvody: Využívanie novín, rádia alebo televízie na šírenie nepravdivých informácií.
- Digitálne hoaxy: Používanie internetových platforiem, sociálnych médií a e-mailu na šírenie falošných príbehov.

4. Klasifikácia podľa závažnosti a vplyvu (Evans, 2013):

- Harmless/Prank Hoaxes: Jednoduché žarty bez väčších negatívnych dopadov.
- Škodlivé hoaxy: Tie, ktoré majú zásadný negatívny vplyv, prípadne ovplyvňujú akciové trhy, politické situácie alebo sociálnu stabilitu.

1. VÝSKUMNÁ VZORKA

Výskum zameraný na vnímanie rizika Kybernetickej bezpečnosti, ako jednej z hybridných hrozieb, sa realizoval od 02/2023 do 07/2023 pomocou autorského výskumného nástroja. Výskumný nástroj bol distribuovaný respondentom (študenti vybraných vysokých škôl) v elektronickej forme a realizoval sa na základe dostupnosti. Výskumný súbor predstavuje celkovo $N=964$ respondentov.

Z hľadiska štruktúry je výskumný súbor tvorený 521 (54.046 %) mužmi a 443 (45.954 %) ženami z dvoch krajín. Respondentov zo Slovenskej republiky bolo celkovo 580 (60.166 %) a z Českej republiky 384 (39.834 %). Priemerný vek respondenta je 26.03 ± 0.51 roka so smerodajnou odchýlkou na úrovni 8.145 roka. Minimálny vek respondenta je 19 rokov a maximálny 63 rokov. Vek respondenta sa analyzoval aj ako ordinálna premenná, pričom respondentov mladších ako 25 rokov bolo celkovo 669 (69.398 %), respondentov vo veku 26 – 35 rokov bolo celkovo 156 (16.183

%), respondentov vo veku 36 – 45 rokov bolo 95 (9.855 %), respondentov vo veku 46 až 55 rokov bolo 41 (4.253 %) a respondenti starší ako 55 rokov boli traja (0.311 %). Z celkového počtu 964 respondentov študuje 321 (33.299 %) na bakalárskom stupni štúdia, 591 (61.307 %) na magisterskom stupni štúdia, 52 (5.394 %) na doktorandskom stupni štúdia a to v dennej forme 592 respondentov (61.411 %) a v externej forme 372 (38.589 %) respondentov. Detailnejšie členenie výskumnej vzorky z hľadiska krajiny, rodu a veku môžeme vidieť v Tab. 1.

Tab. 1 Základný popis výskumnej vzorky z hľadiska krajiny, rodu a veku respondenta

N=964	COUNT	GEN	AGE1 < 25 years	AGE1 26 - 35 years	AGE1 36 - 45 years	AGE1 46 - 55 years	AGE1 > 55 years	Row Totals
Count			135	60	34	4	0	233
Column Percent	SK	male	34.62%	54.05%	54.84%	23.53%		
Row Percent			57.94%	25.75%	14.59%	1.72%	0.00%	
Table Percent			23.28%	10.34%	5.86%	0.69%	0.00%	40.17%
Count			255	51	28	13	0	347
Column Percent	SK	femal e	65.38%	45.95%	45.16%	76.47%		
Row Percent			73.49%	14.70%	8.07%	3.75%	0.00%	
Table Percent			43.97%	8.79%	4.83%	2.24%	0.00%	59.83%
Count	Total		390	111	62	17	0	580
Table Percent			67,24%	19.14%	10.69%	2.93%	0.00%	100.00 %
Count			213	39	24	12	0	288
Column Percent	CZ	male	76.34%	86.67%	72.73%	50.00%	0.00%	
Row Percent			73.96%	13.54%	8.33%	4.17%	0.00%	
Table Percent			55.47%	10.16%	6.25%	3.13%	0.00%	75.00%
Count			66	6	9	12	3	96
Column Percent	CZ	femal e	23.66%	13.33%	27.27%	50.00%	100.00%	
Row Percent			68.75%	6.25%	9.38%	12.50%	3.13%	
Table Percent			17.19%	1.56%	2.34%	3.13%	0.78%	25.00%
Count	Total		279	45	33	24	3	384
Table Percent			72,66%	11.72%	8.59%	6.25%	0.78%	100.00 %

COUNT – krajina, GEN – rod, AGE1 – vek

2. VÝSLEDKY A DISKUSIA

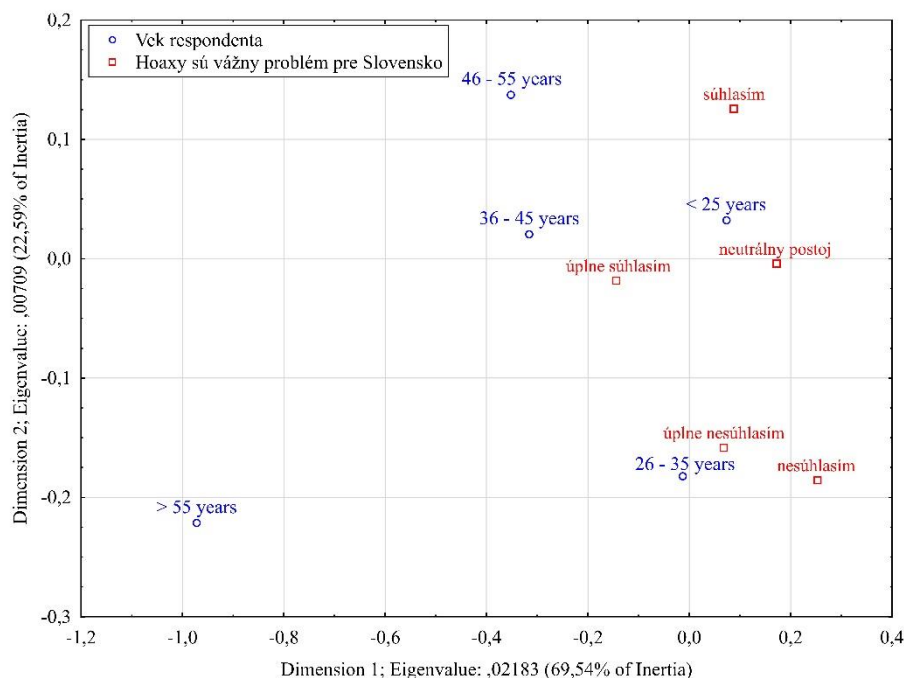
Ak sme si v úvodnej časti definovali pojem hoax z rôznych uhlov, vo výskumnej časti sme sa v prvom rade zamerali na otázku, či respondenti si myslia, že vedia čo je hoax. Základným kritériom pre hodnotenie názoru je vek respondentov. Z výskumu vyplynulo, že existuje signifikantný vzťah medzi vekom respondenta a jeho názorom, že vedia čo hoax je ako taký ($p < 0.000$). Dalším zistením je, že respondenti mladší ako 25 rokov zastávajú názor, že určite vedia čo je hoax (69.955 %), že vedia čo je hoax (10.613 %), k definícii hoaxu má indiferentný postoj 5.531 % respondentov, pojem hoax nedokáže vysvetliť 9.417 % a určite ho nedokáže vysvetliť 4.484 % respondentov. Vo vekovej kategórii 26 až 35 ročných respondentov je 78.846 % tých, ktorí určite vedia čo hoax je, 3.846 % tých, ktorí vedia definovať pojem hoax, 2.564 % tých, ktorí nie sú si istý, či by hoax vedeli definovať, 10.256 % tých, ktorí hoax nevedia definovať a 4.487 % respondentov hoax určite definovať nevie. Vo vekovej kategórii 36 až 45 rokov si až 80.000 % respondentov myslí, že určite vedia čo hoax je, 6.316 % si myslí, že by vie čo je hoax, 5.263 % respondentov nevie, či by hoax dokázali definovať a 8.421 % hoax nedokáže definovať. Vo vekovej kategórii 46 až 55 ročných respondentov 68.293 % si myslí, že hoax určite a 7.317 % respondentov vie hoax definovať. Súčasne až 17.073 % respondentov tejto vekovej kategórie nevie, či by hoax vedeli definovať a 7.317 % by ho definovať nevedeli. V poslednej vekovej kategórii teda respondentov starších ako 55 rokov všetci (100.000 %) uvádzajú, že nevedia, či pojem hoax vlastne znamená. Ak teda pridáme k záveru, že väčšina respondentov (s výnimkou respondentov starších ako 55 rokov) určite vie, alebo vie čo hoax znamená, bolo potrebné zistiť, či podľa názoru respondentov, by ho aj dokázali identifikovať, pričom otázka bola položená ako zápor (Nedokážem hoax identifikovať) aby sme si overili, že respondenti nevypĺňajú dotazník mechanicky ale nad položenými otázkami sa aj zamýšľajú. V rámci analýzy sme rovnako dospeli k záveru, že existuje signifikantný vzťah medzi vekom respondentov a ich názorom, že dokážu hoax identifikovať ($p = 0.007$). Vo vekovej kategórii respondentov mladších ako 25 rokov vysoký stupeň nesúhlasu (72.496 %) ukazuje, že väčšina ľudí v tejto vekovej skupine si myslí, že sú schopní identifikovať hoax a súčasne 11.361 % súhlasí s tvrdením, že nedokážu identifikovať hoax. Vo vekovej kategórii 26 až 35 rokov je nesúhlas je ešte vyšší (82.692 %), čo opäť naznačuje, že väčšina v tejto vekovej skupine si myslí, že dokáže identifikovať hoax. Len 3.846 % súhlasí s tvrdením, že nedokážu identifikovať hoax. Ďalšia veková kategória respondentov a to vo veku 36 až 45 rokov v 80.000 % nesúhlasí s položenou otázkou, čo ukazuje na istú sebadôveru v schopnosti identifikovať hoax. Súčasne 5.263 % vyjadrilo súhlas, a teda ,že nedokážu identifikovať hoax. Vo vekovej skupine 46 až 55 ročných respondentov je nesúhlas s tvrdením opäť vysoký (82.927 %). Súčasne 4,878 % súhlasí s tvrdením, že nedokážu hoax ako taký identifikovať nedokážu. Detailnejšie výsledky prinášame v rámci tab.2.

Tab. 2 Názor respondentov, že Nedokážu identifikovať hoax

	úplne nesúhlasím	nesúhlasím	neutrálny postoj	súhlasím	úplne súhlasím
< 25 years	47,384 %	25,112 %	16,143 %	6,428 %	4,933 %
26 - 35 years	47,436 %	35,256 %	13,462 %	1,923 %	1,923 %
36 - 45 years	44,211 %	35,789 %	14,737 %	5,263 %	0,000 %
46 - 55 years	70,732 %	12,195 %	12,195 %	4,878 %	0,000 %
> 55 years	100,000 %	0,000 %	0,000 %	0,000 %	0,000 %

V prípade skupiny mladších ako 25 rokov, kde väčšina respondentov nesúhlasí s tvrdením "Nedokážem identifikovať hoax," je dôležité zamyslieť sa nad tým, či táto sebaistota pramení zo skutočnej kompetencie alebo z nadmerného sebavedomia. Technologická gramotnosť a pohodlnosť s digitálnymi médiami môže prispievať k tomuto postoji. Mladí ľudia sú často obklopení technológiami a médiami, čo by teoreticky mohlo zvyšovať ich schopnosť rozpoznávať hoaxy. Otázka znie, či táto sebavedomosť korešponduje s reálnou schopnosťou identifikovať falošné správy a hoaxy. Pre stredné vekové skupiny (26 - 55 rokov) vznikajú zaujímavé otázky ohľadom stability v ich odpovediach. Pomerne vysoký stupeň nesúhlasu s tvrdením "Nedokážem identifikovať hoax" sústreďuje diskusiu na to, či táto skupina verí, že má dostatočné skúsenosti a znalosti na rozlíšenie skutočných informácií od klamlivých. Zdá sa, že sú toľko sebavedomí ako najmladšia skupina. Je tu však potenciál na skúmanie, či skúsenosti a životný kontext prispievajú k tejto sebavedomosti viac ako v prípade mladších respondentov. Skupina starších ako 55 rokov predstavuje fascinujúci prípad, kde 100% respondentov nesúhlasí s tvrdením. Je možné, že táto úplná neochota priznať neschopnosť identifikovať hoaxy je odrazom generačných postojov ku kredibilita a sebavedomiu? Mohli by byť títo jednotlivci socializovaní v kultúre, ktorá hodnotí sebaistotu a určitú formu expertízy? Alternatívne, môže tu byť aj jav, kedy staršie generácie môžu byť menej ochotné priznať nevedomosť alebo neistotu v prieskume. Celkovo, vysoká miera nesúhlasu v každej vekovej kategórii vyvoláva dôležité otázky o tom, či sebavedomie v schopnosti identifikovať hoaxy skutočne odráža reálnu kompetenciu. Bolo by zaujímavé skúmať, ako sa tieto postoje prejavujú v reálnom svete, keď sú títo jednotlivci vystavení možným hoaxom a dezinformáciám.

Ak teda poznáme odpovede respondentov na to, či poznajú význam slova hoax, či hoax vedia identifikovať ďalšou logickou otázkou je, či hoax je vážnym problémom pre Slovensko. Na základe výsledkov korešpondenčnej analýzy ($\chi^2=30.256$, $df=16$) je možné prijať záver, že existuje signifikantný vzťah ($p=0.0168$) medzi vekom respondenta a názorom, že hoaxy sú vážny problém pre Slovensko na zvolenej hladine významnosti $\alpha=0.05$. Ak budeme detailnejšie sledovať názor respondentov na položenú otázku z hľadiska vekovej kategórie respondentov, tak v kategórii mladších ako 25 rokov 3.438 % určite nesúhlasí a 7.474 % nesúhlasí s tvrdením, že hoaxy sú nebezpečné. V tejto vekovej kategórii 18.348 % zaujíma k hoaxom neutrálny postoj a súčasne 24.963 % súhlasí a až 45.292 % určite súhlasí s položenou otázkou o nebezpečenstve hoaxov. Vo vekovej kategórii 26 až 35 ročných respondentov, nepovažuje hoaxy za nebezpečné celkovo 14.103 % respondentov (určite nesúhlasí 4.487 %, nesúhlasí 9.615 %). Rovnako v tejto vekovej kategórii považuje 17.949 % respondentov, nebezpečenstvo vyplývajúce z hoaxov za indiferentné a za vážny problém hoaxy považuje 67.949 % respondentov. Vo vekovej kategórii 36 až 45 ročných nepovažuje hoax za nebezpečenstvo pre Slovensko 7.368 % (úplne nesúhlasím 4.211 %, nesúhlasím 3.158 %) a 8.421 % respondentov má k hoaxu ako nebezpečenstvu neutrálny postoj. Na druhej strane 84.211 % respondentov vo veku 36 až 45 rokov považuje hoax za vážny problém Slovenska (súhlasím 21.053 %, úplne súhlasím 63.158 %). Vo vekovej kategórii 46 až 55 ročných respondentov sme neidentifikovali ani jedného respondenta, ktorý by hoax nepovažoval za vážny problém. Neutrálny postoj k hoaxu ako nebezpečenstvu zaujalo 14.634 % respondentov a až 85.366 % respondentov ho za problém považuje. V poslednej vekovej kategórii a to respondentov starších ako 55 rokov všetci považujú hoax za vážny problém Slovenska.



Obr. 1 Miera súhlasu respondentov s tvrdením že hoaxy sú vážnym problémom pre Slovensko

Na základe prezentovaných výsledkov je teda možné, na základe obr.1 prijať záver, že respondenti vo veku menej ako 25 rokov zaujímajú k vnímaniu hoaxu ako nebezpečenstvu neutrálny postoj, respondenti vo veku 26 až 35 rokov úplne nesúhlasia resp. nesúhlasia s tvrdením, že hoax predstavuje pre Slovensko nebezpečenstvo, 36 až 45 roční respondenti úplne súhlasia a 46 až 55 roční respondenti súhlasia, že hoax nebezpečenstvom pre Slovensko je.

Podľa zistených údajov prostredníctvom autorského výskumného nástroja vidíme, že vnímanie hoaxov ako problému pre Slovensko stúpa s vekom respondentov. Zatiaľ čo mladší ľudia vykazujú nižšiu úroveň úplného súhlasu, na druhej strane, u starších ľudí pozorujeme takmer univerzálny úplný súhlas s tvrdením. Mladšie vekové skupiny, hoci stále vo veľkej miere súhlasia s tým, že hoaxy predstavujú problém, vykazujú o niečo vyššiu mieru nesúhlasu alebo neutrálneho postoj. Môže to súvisieť s ich väčšou expozíciou a obratnosťou v digitálnom svete a potenciálne s väčšou schopnosťou filtrovať a identifikovať falošné informácie. Taktiež môže ich mladosť a možná menšia politická angažovanosť ovplyvňovať mieru, do akej považujú dezinformácie za vážny spoločenský problém. Staršie generácie vykazujú vysoký až univerzálny súhlas s tým, že hoaxy predstavujú problém. Je možné, že vnímajú svet, v ktorom žijú, ako viac neistý a zmätený v dôsledku falošných informácií. Taktiež môže ísť o obavy z toho, ako dezinformácie ovplyvňujú mladšie generácie a spoločnosť ako celok. Rovnako, staršie generácie, ktoré nie sú tak digitálne pohotové, môžu cítiť, že sú viac ohrozené a že spoločnosť je viac ohrozená v dôsledku šírenia hoaxov. Celkovo je zjavné, že v celom spektre vekových skupín je vnímaný významný problém v oblasti hoaxov a dezinformácií. Z tohto pohľadu je dôležité, aby sa realizovali vzdelávacie programy zamerané na mediálnu gramotnosť a kritické myslenie, ktoré by zohľadňovali potreby a osobitosti jednotlivých vekových kategórií. Táto diskusia by mohla byť aj platformou pre ďalší výskum týkajúci sa efektivity rôznych stratégií boja proti dezinformáciám voči rôznym vekovým skupinám.

ZÁVER

V rámci predloženého príspevku autori analyzovali základné aspekty hoaxu na základe realizovaného prieskumu, ktorého sa zúčastnilo celkovo 964 študentov z Českej a Slovenskej republiky zo 4 vysokých škôl. Základným problémom je otázka, či vôbec pojmu hoax laická spoločnosť alebo rovnako aj vedecká komunita rozumie do dôsledkov. S pribúdajúcou frekvenciou využívania pojmu „hoax“ vo všetkých oblastiach spoločenského života vzniká a reálne aj existuje veľké nebezpečenstvo, že pojmom hoax sa označuje všetko, s čím nesúhlasíme, čo nepoznáme a čomu nerozumieme, resp. čo je v rozpore s názorom väčšiny. Tu narážame na prvý problém, čo teda za hoax reálne označiť môžeme. Hoax má v zmysle svojej definície jasný význam a to v prvej časti, že hoax je zámerne vymyslená alebo klamlivá nepravda. Ak sa sústredíme na túto prvú časť definície hoax, mal by spĺňať podmienku zámernosti, teda musí byť vytvorený vedome za účelom oklamania alebo zavádzania. Ak prijeme tento predpoklad ako nutnú podmienku na vzniku hoaxu otvára sa diskutovaný problém neuváženeho označovania každého názoru s ktorým nesúhlasíme, iného názoru za hoax. Ak z definície hoaxu vyberieme ďalšiu jeho dôležitú vlastnosť a to, že hoax je nepravda znova stojíme pred závažným problémom, ako túto nepravdu vyvrátiť, resp. kto definuje čo pravda je. Všeobecný pojem „pravda“ a jeho opozitum „nepravda“ sú veľmi zložité filozofické konštrukty, ktorých význam je nutné chápať z pohľadu rôznych kontextov (filozofický, vedecký, eticko-morálny, sociálno-kultúrny, právny, náboženský ap.). Vo všeobecnosti môžeme pravdivosť určitého záveru potvrdiť iba na základe dôkazov. A tu znova narážame na problém, čo vlastne dôkaz je, ako s dôkazom pracovať, vyhodnocovať ho a na základe neho prijať relevantné závery. Pri hlbšej úvahe toho čo dôkaz je, prideme nevyhnutne k záveru, že existuje iba veľmi malý a obmedzený počet vedných odborov, kde dôkaz je definitívny a nevyvrátený a naopak v ostatnej väčšine sa dôkaz stáva synonymum slova názor. Čím hlbšie budeme skúmať základ a podstatu hoaxu a s ním spojený pojem dezinformácia, tým na zložitejšie otázky budeme musieť nájsť odpovede. Súčasne však musíme upriamiť pozornosť aj na spomenuté označovanie pojmom hoax všetkého s čím nesúhlasíme, nerozumieme alebo nepoznáme a závery na javy okolo nás si vytvárame iba základe subjektívneho konceptu vnímania sveta. S tým je spojené označovanie pojmom „hoax“ všetkého čo je v rozpore s všeobecne definovanou „pravdou“ resp. všeobecne prijímaným „správnym názorom“. Takýto prístup k používaniu pojmu hoax je veľmi nesprávny a možno tvrdiť, že až škodlivý. Celkový rozvoj spoločnosti ako celku je možný iba v prostredí, kde sú prijímané a akceptované rôznorodé názory, teda v prostredí so širokou názorovou pluralitou a v prostredí kde sa akceptuje pochybnosť. Práve pochybnosť a schopnosť akceptovať rôznorodé názory vedú k vedeckému pokroku a progresu v rozvoji spoločnosti. Hoax ako taký vykazuje určitú mieru škodlivosti, máme však za to, že väčším problémom je nesprávne používanie tohto pojmu. Aby sme ale minimalizovali škodlivé dopady hoaxov (v ich skutočnom chápaní) na spoločnosť, existuje iba jedna jediná cesta. A to je, aby spoločnosť bola dostatočne vzdelaná a súčasne bola tolerantná v akceptovaní iných pohľadov na existujúce javy. Ak spoločnosť, v chápaní jednotlivých jej členov bude dostatočne vzdelaná, nebude musieť mať obavy vyplývajúce z plurality názorov a v konečnom dôsledku príde k záveru, že o „pravde“ sa musí vždy a za každých okolností diskutovať, aby bolo možné rozšíriť úroveň poznania. Príspevok je teda možné uzavrieť výrokom Francois Maria Aroueta, známeho francúzskeho osvietenského filozofa „*Nesúhlasím s vaším názorom, ale dal by som svoj život za to, aby ste ho mohli slobodne povedať.*“

Zdroje

1. Bartholomew, R. E., & Hassall, B. (2006). Psi wars: TED, Wikipedia and the battle for the Internet. *Journal of the Society for Psychical Research*, 70(885).
2. Benamara, F., Bosco, C., Fersini, E., Pasi, G., Patti, V., & Viviani, M. (2018, October 1). SeCredISData 2018: Special Session on Sentiment, Emotion, and Credibility of Information in Social Data. <https://scite.ai/reports/10.1109/dsaa.2018.00082>.
3. Boese, A. (2002). *The Museum of Hoaxes*. E.P. Dutton.
4. Evans, A. D., & Lee, K. (2013). Emergence of Lying in Very Young Children. *Developmental Psychology*, 49(10), 1958-1963.
5. Finneman, T., & Thomas, R J. (2018, September 1). A family of falsehoods: Deception, media hoaxes and fake news. <https://scite.ai/reports/10.1177/0739532918796228>.
6. Helling, J. (2017). *Anatomy of a Hoax: The Underlying Logic of Hoaxes and Scams*. McFarland.
7. Jannana, N S., Prabowo, T T., & Istriyani, R. (2021, June 3). Identifying Fake News: A Lesson from Library Science Students. <https://scite.ai/reports/10.24252/v9i1a5>.
8. Nihayah, Z., & Adila, I. (2020, January 1). Hoax: The Dispute among Information Disruption or Social Psychological Aggression. <https://scite.ai/reports/10.4108/eai.18-9-2019.2293464>.
9. Rohmah, M., & Kusromaniah, S. (2021, January 1). Development of Critical Thinking Skills Measurement in Socio-Political Context. <https://scite.ai/reports/10.2991/assehr.k.210423.055>.
10. Sobieraj, S. (2010). Reporting Conventions: Journalists, Activists, and the Thorny Struggle for Political Visibility. *Critical Studies in Media Communication*, 27(4), 331-350.
11. Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). Defining “Fake News”: A typology of scholarly definitions. *Digital Journalism*, 6(2), 137-153.
12. Zollmann, A. (2016). Corporate media coverage of the role of corporations in global health. *Critical Sociology*, 44(4-5), 709-728.
13. Yusri, Y., Rivai, M., & Anwar, M. (2022, August 27). The COVID-19 Hoax News in Indonesia Context: Looking Beyond the Essence Using Content Analysis. <https://scite.ai/reports/10.31849/reila.v4i2.9216>.

FUNKCE A VLASTNOSTI KOMPOZITNÍCH INDIKÁTORŮ VNÍMÁNÍ ZÁVAŽNOSTI HYBRIDNÍCH HROZEB

doc. Ing. Miroslav Gombár, PhD., prof. Ing. Antonín Korauš, PhD., MBA, LL.M., prof. RNDr. Šárka Mayerová, Ph.D., doc. PaedDr. Alena Vagaská, PhD., PhDr. Pavlína Račková, Ph.D.

Prešovská univerzita v Prešove, Fakulta manažmentu, ekonomiky a obchodu, miroslav.gombar@unipo.sk; Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu, antonin.koraus@akademiapz.sk; Univerzita obrany v Brně, Fakulta vojenských technologií, sarka.mayerova@unob.cz; Technická univerzita v Košiciach, Fakulta výrobných technológií, alena.vagaska@tuke.sk; Univerzita obrany v Brně, Fakulta vojenských technologií, pavlina.rackova@unob.cz

Abstrakt: Kybernetická bezpečnost je neoddeliteľnou súčasťou odolnosti každého štátu voči hybridným hrozbám. Nejedná sa však len o vlastné hrozby ako také, ale veľké nebezpečenstvo je skryté už vo vlastnom vnímaní týchto hrozieb jednotlivými občanmi, pretože chyba jednotlivca môže mať dalekosáhlé dôsledky. Preto je nevyhnutná výchova občanov k zodpovednému chovaniu na internete. Aby mohla byť táto výchova účinne aplikovaná, musí každý štát najprv vedieť, ako k jednotlivým hrozbám občania pristupujú, ako vnímajú ich nebezpečenstvo. Autoři článku zaměřili svou pozornost právě na vnímání rizika ohrožené štátu skrz Kybernetickou bezpečnosť. Vytvorili rozsáhlý výskumný dotazník, jehož cieľom bolo zistiť a analyzovať vnímanie závažnosti ohrozenia štátu prostredníctvom jednotlivých pilierov Kybernetickej bezpečnosti. Vnímanie rizika bude popísané pomocou agregatívnej funkcie, ktorej konštrukcia bude vychádzať z obecných platných vlastností kompozitných indikátorov, ktoré však budú aplikované na konkrétnu problematiku.

Kľúčové slová: hybridní hrozby, kybernetická bezpečnosť, korešpondenčná analýza, výskumný súbor.

ÚVOD

Problematika členení hybridnému pôsobeniu a hybridným hrozbám či v súčasnej dobe stále aktuálnejšia oblasť hybridného válčenia je veľmi rozsiahla. Oblasť členení hybridnému pôsobeniu a súvisiacim hrozbám nabýva postupne na významu, a to nielen na úrovni jednotlivých štátov, ale aj na úrovni spoločenstiev typu Európskej únie a NATO. Ruku v ruku s týmto vývojom sa tak zvyšujú i nároky na zlepšovanie a zvyšovanie odolnosti jednotlivých štátov voči hybridným hrozbám tak majú narastajúcu tendenciu ako celosvetovo [1], tak i v rámci jednotlivých členských krajín Európskej únie [2]. Oblasť kybernetickej bezpečnosti je veľmi dôležitý problém [3], ktorému sa venuje v súčasnej dobe odpoviadajúca pozornosť a medzi odborníkmi sa vedú bohaté diskusie k tomuto tématu [4-6].

Jak uvádza autor článku [7]: *Problematika členení hybridnému pôsobeniu generuje niekoľko základných variantov možného prístupu. Za najvhodnejší lze považovať komplexní systémový přístup, označovaný v zahraniční literatuře jako tzv. Comprehensive Approach, který řeší všechny podstatné záležitosti související s problematikou členení hybridnému pôsobeniu a hybridným hrozbám. Tento přístup popisuje spoločné využitie všetkých dostupných nástrojov a politik z celého existujúceho spektra moci, a to s cieľom čeliť hybridnému pôsobeniu, aktivitám a hrozbám najrôznejších aktérov. Lze zmieniť zejména nástroje diplomacie, bezpečnosti, obrany, ekonomiky apod. [8] Je zásadné chápať propojenie všetkých oblastí fungovania štátu a spoločnosti, rovnako ako nástroje hybridného pôsobenia. K zajištění bezpečnosti je z toho důvodu potřeba přistoupit z pohledu celé společnosti (tzv. Whole Society Approach) a reflektovat toto vzájemné provázání. Komplexní přístup lze považovat za*

nejvhodnější, ačkoliv je poměrně zdrojově náročný a vyžaduje značnou fundovanost i záběr participantů.

Česká republika se k řešení otázky hybridních hrozeb poprvé postavila formulací strategického dokumentu *Audit národní bezpečnosti* z roku 2016, kde do širšího spektra nejvýznamnějších aktuálních hrozeb pro Českou republiku byly zakomponovány konkrétně i hybridní hrozby a jejich vliv na bezpečnost občanů České republiky. Zde byly hybridní hrozby vůči České republice rozděleny do tří klíčových oblastí, které zahrnují: působení proti soudržnosti a ideově-hodnotovému zakotvení společnosti; působení proti fungující ekonomice; působení proti bezpečnosti státu a občanů.

Tento dokument sám o sobě však nijak nezaručí disponibilitu schopnostmi čelit samotnému praktickému hybridnímu působení. Jak uvádí Havlík v [7] cituji: „*Je nutná pravidelná aktualizace a evaluace veškerých souvisejících procesů na základě nepřetržitého monitorování všech zásadních faktorů. Praktické implementaci specifických přístupů v rámci České republiky, jak čelit hybridním hrozbám a hybridnímu působení, předchází odpovídající Národní strategie pro čelení hybridnímu působení, na kterou navazuje konkrétní akční plán determinující specifické úkoly a opatření. Komplexní národní systém čelení hybridním hrozbám by měl zahrnovat všechny národní zpravodajské služby, silová a další ministerstva i další relevantní subjekty, včetně soukromého sektoru či akademické obce. Nepopíratelnou úlohu v boji proti hybridním hrozbám hraje také vzájemná součinnost s dalšími subjekty, aktéry a partnery mimo Českou republiku. Zdůraznění zaslouží především členství České republiky v NATO a Evropské unii. Důležitá potřeba nadnárodní spolupráce a koordinace je umocněna charakteristikou hybridních hrozeb, které mají často nadnárodní rozměr a svým charakterem potvrzují vzájemné prolínání vnější i vnitřní dimenze bezpečnosti.*“

Tento příspěvek má za cíl seznámit s problematikou tvorby agregační funkce, která by byla schopna modelovat význam jednotlivých pilířů. Každému pilíři musí být totiž přiřazena váha, která co nejlépe vystihuje roli daného pilíře v rámci celé agregační funkce. Metod stanovení vah existuje velké množství, přičemž není možné jednoznačně říci, kterou je potřeba zvolit. Záleží vždy na dané studované problematice, ale i na zvoleném přístupu výzkumníka. Ten musí potom uživatele seznámit v klady i nevýhodami zvoleného postupu.

Také v tomto výzkumu předpokládáme využití několika pohledů a několika způsobů výpočtů vah zvolených pilířů a následné verifikaci a diskuzi získaných výsledků.

Je třeba zdůraznit, že na danou problematiku se autoři dívají očima respondentů – tj. studentů vybraných vysokých škol zejména policejního a armádního typu ve Slovenské a České republice. V Sekci 2 popíšeme základní vlastnosti výzkumného souboru. V Sekci 3 se zmíníme o výzkumném dotazníku, sekce 4 bude věnovaná vlastnostem kompozitních indikátorů. V poslední závěrečné sekci shrneme doposud získané výsledky.

1. POPIS VÝZKUMNÉHO SOUBORU

Výzkum zaměřený na vnímání rizika Kybernetické bezpečnosti, jako jedné z hybridních hrozeb, se realizoval od 02/2023 do 07/2023 mimo jiné pomocí jedinečného dotazníku, který byl vytvořen speciálně pro tento výzkum. Hlavními autory dotazníku jsou spoluautoři článku doc. Gombár

a prof. Korauš. Dotazník byl distribuován studentům a akademickým pracovníkům vybraných vysokých škol, kteří byli respondenty, v elektronické formě a realizoval se na základě souhlasu zodpovědných osob v každé škole a dobrovolného souhlasu každého studenta či akademického pracovníka. Od studentů autoři obdrželi celkem 964 plně vyplněných dotazníků, tedy výzkumný soubor představuje celkem $N=964$ respondentů.

Jak již bylo uvedeno i v článku [9] genderové rozložení respondentů je 521 (54,046 %) muži a 443 (45,954 %) ženy ze Slovenské republiky a České republiky. Respondentů ze Slovenské republiky bylo celkem 580 (60,166 %), z České republiky odpovědělo 384 (39,834 %). Průměrný věk respondenta je 26.03 ± 0.51 roku se směrodatnou odchylkou na úrovni 8.145 roku. Minimální věk respondenta je 19 let a maximální 63 let.

Věk respondenta byl analyzován také jako ordinální proměnná, přičemž respondentů mladších 25 let bylo celkem 669 (69,398 %), respondentů ve věku 26–35 let bylo celkem 156 (16,183 %), respondentů ve věku 36–45 let bylo 95 (9,855%), respondentů ve věku 46 až 55 let bylo 41 (4,253 %) a respondenti starší 55 let byli tři (0,311 %). Z celkového počtu 964 respondentů studuje 321 (33,299 %) na bakalářském stupni studia, 591 (61,307 %) na magisterském stupni studia, 52 (5,394 %) na doktorském stupni studia a to v denní formě 1 1 492 respondentů. (38,589 %) respondentů.

Detailnější členění výzkumného vzorku z hlediska země, rodu a věku můžeme vidět v Tab. 1.

Tab. 3 Základní popis datového souboru z pohledu země, rodu a věku respondenta

<i>N=964</i>	<i>Země</i>	<i>GEN</i>	<i>Věk</i> <i>< 25 let</i>	<i>Věk</i> <i>26 - 35 let</i>	<i>Věk</i> <i>36 - 45 let</i>	<i>Věk</i> <i>46 - 55 let</i>	<i>Věk</i> <i>> 55 let</i>	<i>Řádek</i> <i>Celkem</i>
Počet			135	60	34	4	0	233
Column Percent	SK	muž	34.62%	54.05%	54.84%	23.53%		
Řádek procenta			57.94%	25.75%	14.59%	1.72%	0.00%	
Table procenta			23.28%	10.34%	5.86%	0.69%	0.00%	40.17%
Počet			255	51	28	13	0	347
Column procenta	SK	žena	65.38%	45.95%	45.16%	76.47%		
Řádek procenta			73.49%	14.70%	8.07%	3.75%	0.00%	
Table procenta			43.97%	8.79%	4.83%	2.24%	0.00%	59.83%
Počet	Celkem		390	111	62	17	0	580
Table procenta			67,24%	19.14%	10.69%	2.93%	0.00%	100.00%
Počet			213	39	24	12	0	288
Column procenta	CZ	muž	76.34%	86.67%	72.73%	50.00%	0.00%	
Řádek procenta			73.96%	13.54%	8.33%	4.17%	0.00%	
Table procenta			55.47%	10.16%	6.25%	3.13%	0.00%	75.00%
Počet			66	6	9	12	3	96
Column Percent	CZ	žena	23.66%	13.33%	27.27%	50.00%	100.00%	
Řádek procenta			68.75%	6.25%	9.38%	12.50%	3.13%	
Table procenta			17.19%	1.56%	2.34%	3.13%	0.78%	25.00%
Počet	Celkem		279	45	33	24	3	384
Table procenta			72,66%	11.72%	8.59%	6.25%	0.78%	100.00%

vek (v ordinálnej škále)

2. POPIS VÝZKUMNÉHO NÁSTROJE

V rámci realizovaného výzkumu zaměřeného na vnímání stupně závažnosti Kybernetické bezpečnosti ve vztahu k ohrožení státu jako jednoho z pilířů hybridních hrozeb byl využit výše popsáný autorský dotazník, který se skládal z 5 základních položek.

Měření je založeno na subjektivním vnímání stupně závažnosti ohrožení státu, přičemž respondenti si vybírali odpovědi z 5 stupňové Likertovy škály: 1 – nezávažné, 2 – málo závažné, 3 – středně závažné, 4 – závažné, 5 – vysoce závažné.

Samotný výzkumný nástroj byl rozdělen do pěti základních oblastí, pilířů Kybernetické bezpečnosti:

1. Kybernetická špionáž
2. Narušení nebo snížení odolnosti IT infrastruktury
3. Nepřátelské kampaně
4. Narušení nebo snížení bezpečnosti eGoverementu
5. Kyberterorismus

Každému z pěti vyjmenovaných pilířů Kybernetické bezpečnosti byly věnované výroky, u kterých respondenti vyjadřovali své subjektivní vnímání míry rizika od „nezávažné“ až po „vysoce závažné“.

Již prvotní analýza ukázala velmi zajímavé výsledky a možná i do jisté míry nečekané rozdíly mezi vnímáním hrozeb v jednotlivých zemích.

Spolehlivost celého výzkumného nástroje byla posuzovaná pomocí Kronbachova koeficientu alfa a dosáhla hodnoty 0,83883. To ukazuje na relativně nízkou chybovou složku rozptylu měření a jednotlivé dílčí položky výzkumného nástroje jsou tudíž vnitřně konzistentní. To tedy vlastně znamená, že existuje vysoká míra shody položek výzkumného nástroje v tom smyslu, že stejně dobře objasňují stejný jev, tedy kybernetickou bezpečnost. Podrobnosti k této části výzkumu lze nalézt v článku [9].

Pro čtenářovo pohodlí považujeme za nezbytné ještě zopakovat formulaci základních výzkumných otázek, kterými v rámci popisované studie jsou [9]:

1. „*Jaký je vztah mezi základními definovanými pilíři Kybernetické bezpečnosti a základními demografickými ukazateli výzkumného vzorku?*“
2. „*Existují ve vnímání závažnosti ohrožení státu difference mezi jednotlivými skupinami respondentů?*“

K zodpovězení definovaných výzkumných otázek byla použita korespondenční analýza, tedy statistická metoda pro analýzu vztahů mezi kategoriemi dvou nebo více proměnných uspořádaných v kontingenční tabulce [10]. Tento typ analýzy umožňuje zkoumat asociaci kategoriálních proměnných a získat přehledné grafické zobrazení souvislostí ve dvourozměrném, resp.

vícerozměrném prostoru. Cílem je posoudit vzájemný vztah mezi proměnnými a vysvětlit strukturu zkoumané závislosti.

Následující obrázek pro ilustraci ukazuje příklad jedné položky dotazníku věnované vybraným aspektům hybridních hrozeb.

Obr. 4 Příklad jedné položky dotazníku věnované vybraným aspektům hybridních hrozeb.

Táto časť dotazníka sa dotýka vybraných aspektov hybridných hrozieb. V nasledujúcich dvoch otázkach si vyberte iba jednu možnosť (tú, ktorá najviac vystihuje Vaše vnímanie problematiky hybridnej hrozby)

Ako rozumiete pojmu Hybridné hrozby? *

- ☐ Nezaregistroval som takýto problém.
- ☐ Ide najmä o koordinovanú politickú virtuálnu aktivitu, ktorej cieľom je destabilizovať politický systém v inej krajine.
- ☐ Ide najmä o koordinovanú aktivitu, ktorej cieľom je destabilizovať demokraciu v inej krajine.
- ☐ Ide najmä o rôznorodé aktivity využívajúce dezinformácie a falošné správy s cieľom vyvolať paniku v inej krajine.
- ☐ Ide najmä o koordinovanú vojenskú aktivitu, ktorej cieľom je narušenie politického systému inej krajiny.
- ☐ Ide najmä o koordinovanú dezinformačnú kampaň, ktorej cieľom je podkopanie dôvery k politickým elitám inej krajiny.
- ☐ Ide najmä o koordinovanú ekonomickú aktivitu, ktorej cieľom je destabilizácia ekonomického systému inej krajiny.

3. ZÁKLADNÍ VLASTNOSTI KOMPOZITNÍCH INDIKÁTORŮ

V této kapitole zmíníme některé základní poznatky, které musejí být vzaty do úvahy při tvorbě výše zmíněné agregační funkce. Vycházíme přitom z poznatků o kompozitních indikátorech publikovaných v [11]. Zde uvedené metody tvorby a vlastnosti budou muset být modifikovány na náš konkrétní výzkum.

3.1 Výhody a nevýhody kompozitních indikátorů

Indikátorem rozumíme kvantitativní nebo kvalitativní měřítko odvozené ze série pozorovaných skutečností, které může odhalit relativní pozice v dané oblasti. Při vyhodnocování v pravidelných intervalech může indikátor ukazovat směr změny napříč různými jednotkami a časem. Složené indikátory jsou velmi podobné matematickým nebo výpočtovým modelům. Jejich konstrukce jako taková vděčí spíše řemeslné zručnosti tvůrce než všeobecně uznávaným vědeckým pravidlům pro tvorbu. Pokud jde o modely, opodstatnění pro složený indikátor spočívá v jeho vhodnosti pro zamýšlený účel a v akceptaci ze strany kolegů [12].

Výhody:

- Schopnost shrnout složité, vícerozměrné skutečnosti s cílem podpořit rozhodnutí tvůrce (rozhodovatele).

- Snadnější interpretovatelnost než množina mnoha samostatných ukazatelů.
- Schopnost posoudit pokrok v průběhu času.
- Redukují velikost sady indikátorů, aniž by došlo ke ztrátě či vypuštění základních informací.
- Umožňují výzkumníkovi srovnat efektivně porovnávat komplexní dimenze.

Nevýhody:

- Může poskytnout zavádějící informace, pokud jsou špatně konstruované nebo špatně interpretované.
- Může vést ke zjednodušeným závěrům.
- Možnost zneužití, manipulace (tj. tvorba výsledku „na objednávku“), pokud proces není transparentní a/nebo postrádá zdravé statistické nebo koncepční principy.
- Výběr ukazatelů a vah by mohl být předmětem sporu.
- Může zamaskovat vážné nedostatky v některých dimenzích a zvýšit obtížnost identifikace správného nápravného opatření, pokud proces výstavby není transparentní.
- Může vést k nevhodným zásadám, pokud jsou ignorovány dimenze, které je obtížné měřit.

Při tvorbě indikátorů by měl být dodrženy následující kroky:

1. **Určit teoretický rámec** - Poskytuje základ pro výběr a kombinaci proměnných do smysluplného složeného ukazatele v rámci vhodnosti pro daný účel
2. **Výběr dat**- Mělo by být založeno na analytické spolehlivosti, měřitelnosti a relevance ukazatelů pro měřený jev a jejich vzájemné vztahy.
3. **Dopočet chybějících dat** – k dispozici musí být kompletní datová sada. Pokud není, aplikuje se jednoduchá nebo vícenásobná imputace. Tj.
 - Odhadnout chybějící hodnoty.
 - Poskytnout míru spolehlivosti každé doplněné hodnoty,
 - Diskutovat o přítomnosti odlehlých hodnot v datové sadě.
4. **Vícerozměrná analýza** - Měla by být použita ke studiu celkové struktury datového souboru, posouzení jeho vhodnosti a být vodítkem pro následné metodologické volby (např. vážení nebo agregace).
5. **Normalizace** - měla by být provedena, aby byly zajištěny, že jednotlivé proměnné jsou srovnatelné.
6. **Určení vah a agregace** – použít takové agregační procedury, které respektují jak teoretické rámce, tak vlastnosti dat.
7. **Analýza nejistoty a citlivosti** -pro posouzení robustnosti kompozitního indikátore
8. **Další kontrola dat** - zkontrolovat korelace a kauzalita (pokud je to možné).
9. **Vazby na další ukazatele** – provedení korelace
10. **Vizualizace výsledků** – vhodná vizualizace může ovlivnit (nebo pomoci zlepšit) interpretovatelnost výsledků

3.2 Tvorba vah

Pro stanovení vah existuje řada technik. Naším úkolem bude vybrat tu nejvhodnější nebo vytvořit modifikaci přesně pro naši problematiku. Některé z technik používaných pro stanovení vah ukazatelů jsou odvozeny ze statistických modelů, jako je faktorová analýza, analýza obalů dat a

modely nepozorovaných složek (UCM), nebo z participativních metod, jako jsou procesy přidělování rozpočtu (BAP), procesy analytické hierarchie (AHP) a conjoin analýza (CA). Bez ohledu na to, která metoda je použita, váhy jsou v podstatě hodnotové úsudky. Zatímco někteří analytici si mohou vybrat váhy pouze na základě statistické metody, jiní mohou při tvorbě vaz „odměňovat“ (nebo „trestat“) složky, které jsou považovány za více (nebo méně) vlivné, v závislosti na názoru odborníků, aby lépe odrážely např. politické priority nebo teoretické faktory.

ZÁVĚR

Jedním z cílů článku bylo ukázat komplexnost problematiky a také nutnost jejího studia. Autoři jsou nyní ve fázi zpracování získaných dat a hledání nejvhodnějších způsobů jak modelovat a interpretovat vazby, které se mezi jednotlivými pilíři, ale i skupinami respondentů objevili. Veríme, že odhalení těchto vazeb povede k lepšímu a přesnějšímu pohledu do problematiky, k zlepšení práce se studenty, k jejich větší informovanosti ohledně hybridních hrozeb a v důsledku i ke zvýšení odolnosti celého státu k těmto hrozbám.

Pod'akovanie

Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Acknowledgement

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

Zdroje

1. Granholm, F., Tin, D., Ciottone, G. R. (2022) Not war, not terrorism, the impact of hybrid warfare on emergency medicine, *The American Journal of Emergency Medicine*, Volume 62, 2022, pp. 96-100, ISSN 0735-6757, <https://doi.org/10.1016/j.ajem.2022.10.021>
2. Procházka, J., Vinkler, P., Jojart, K., Szenes, Z., Gruszczak, A., Kandrik, M. (2023) One threat – multiple responses. Countering Hybrid Threats in V4 countries/Jedna hrozba – více způsobů reakce. Čelení hybridnímu působení v zemích V4. *Obrana a strategie (Defence and Strategy)*, 23, p. 049-073. doi: 10.3849/1802-7199.23.2023.01.049-073
3. Eberle, J., Daniel, J. (2022) Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety, *Political Geography*, Vol. 92, 2022, 102502, ISSN 0962-6298, <https://doi.org/10.1016/j.polgeo.2021.102502>.
4. Qin, X., Jiang, F., Cen, M., Doss, R. (2023) Hybrid cyber defense strategies using Honey-X: A survey, *Computer Networks*, Vol. 230, 2023, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2023.109776>
5. Hausken, K. (2020) Cyber resilience in firms, organizations and societies, *Internet of Things*, Vol. 11, 2020, 100204, ISSN 2542-6605, <https://doi.org/10.1016/j.iot.2020.100204>
6. Mekala, S.H., Baig, Z., Anwar, A., Zeadally, S. (2022) Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions, *Computer Communications*, Vol. 208, 2023, p. 294-320, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2023.06.020>

7. Havlík M. (2022) Aktuální přístupy České republiky, EU a NATO k hybridním hrozbám. *Vojenské rozhledy*. 2022, 31 (2), 003-016. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.
8. Bauerová, H., Hlaváčková, H., Vošta, M. (2018) Vnitřní a vnější dimenze bezpečnosti Evropské unie. Nakladatelství Libri, Praha, 2018. ISBN 978-80-7277-576-7. Str. 31.
9. Gombár, M., Korauš, A., Mayerová, Š., Vagaská, A. (2023) Kybernetická bezpečnosť a jej piliere v analýze vnímania závažnosti ohrozenia štátu, sborník konference „Zvýšenie odolnosti Slovenska voči hybridným hrozbám“, 5. – 6. 10. 2023, Častá – Papiernička, 8 str.
10. Fávero, L.P., Belfiore, P., de Freitas Souza, R. (2023) Chapter 13 - Simple and multiple correspondence analysis, Editor(s): Luiz Paulo Fávero, Patrícia Belfiore, Rafael de Freitas Souza, Data Science, Analytics and Machine Learning with R, Academic Press, 2023, p. 215-234, ISBN 9780128242711, <https://doi.org/10.1016/B978-0-12-824271-1.00013-5>
11. OECD (2008), Handbook on Constructing Composite Indicators METHODOLOGY AND USER GUIDE, JRC European Commission, <https://doi.org/10.1787/9789264043466-e>, ISBN 978-92-64-04345-9.
12. Rosen R. (1991), Life Itself: A Comprehensive Inquiry into Nature, Origin, and Fabrication of Life. Columbia University Press

KYBERNETICKÁ BEZPEČNOSŤ A JEJ PILIERE V ANALÝZE VNÍMANIA ZÁVAŽNOSTI OHROZENIA ŠTÁTU

doc. Ing. Miroslav Gombár, PhD., prof. Ing. Antonín Korauš, PhD., MBA, LL.M., prof. RNDr. Šárka Mayerová, Ph.D., doc. PaedDr. Alena Vagaská, PhD.

Prešovská univerzita v Prešove, Fakulta manažmentu, ekonomiky a obchodu, miroslav.gombar@unipo.sk; Akadémia Policajného zboru v Bratislave, Katedra informatiky a manažmentu, antonin.koraus@akademiapz.sk; Univerzita obrany v Brně, Fakulta vojenských technológií, sarka.mayerova@unob.cz; Technická univerzita v Košiciach, Fakulta výrobných technológií, alena.vagaska@tuke.sk

Abstrakt: Neoddeliteľnou súčasťou odolnosti štátu voči hybridným hrozbám je aj jeho kybernetická bezpečnosť, ktorej prípadné narušenie má ďalekosiahle dopady na chod krajiny. V rámci článku sa zameriavame práve na vnímanie rizika ohrozenia štátu cez Kybernetickú bezpečnosť. Prezentujeme výskumné otázky a výsledky štatistickej analýzy dát získaných pomocou implementácie skonštruovaného výskumného nástroja na vzorke $N=964$ respondentov zo SR a ČR. Analýza vnímania závažnosti ohrozenia štátu cez jednotlivé piliere Kybernetickej bezpečnosti priniesla zaujímavé výsledky vo vzťahu k demografickým ukazovateľom výskumnej vzorky.

Kľúčové slová: hybridné hrozby, kybernetická bezpečnosť, korešpondenčná analýza, výskumný súbor.

ÚVOD

Nároky na zvyšovanie odolnosti štátu voči hybridným hrozbám majú v súčasnosti narastajúci trend ako celosvetovo [1], tak aj v rámci jednotlivých krajín Európskej únie [2], keďže hybridné hrozby majú potenciál spôsobiť ničivé následky v rôznych oblastiach fungovania štátu. EÚ podniká dôležité kroky na zlepšenie svojej schopnosti čeliť hybridným hrozbám a na posilnenie odolnosti EÚ a prijíma opatrenia, medzi inými aj v oblasti kybernetickej bezpečnosti – uvádzajú autori v [2] kde sa zameriavajú hlavne na krajiny V4. Tejto téme sa venuje vysoká pozornosť v odbornej literatúre, keďže ide o vysoko relevantný problém [3], vedú sa bohaté diskusie medzi zúčastnenými aktérmi.

Často diskutovanou je Kybernetická bezpečnosť [4], keďže je jedným z pilierov na ktorých sa aktuálne stavia odolnosť krajiny voči hybridným hrozbám a útokom. Rozvoj a prijatie sieťových technológií totiž pretvára každodenný život ako jednotlivca, tak aj štátu, čím sa zvyšuje riziko kybernetických hrozieb a útokov. V súčasnosti sa aktívne vyvíjajú nové stratégie na detekciu kybernetických bezpečnostných hrozieb [5], tejto problematike sa venuje pozornosť z viacerých zorných uhlov [6].

V rámci predkladaného článku sa uvedenej problematike venujeme z pohľadu vnímania rizika ohrozenia Kybernetickej bezpečnosti štátu. Konkrétne cez optiku respondentov zapojených do výskumu, v tomto prípade ide o študentov vybraných vysokých škôl policajného a armádneho typu v Slovenskej republike a Českej republike, berúc do úvahy spoločnú minulosť týchto dvoch štátov. V článku uvádzame popis výskumného súboru (v sekcii 2), v sekcii 3 formulujeme výskumné otázky a prinášame riešenia a diskusiu výsledkov získaných na základe štatistickej analýzy dát. Vďaka korešpondenčnej analýze dát sme získali zaujímavé výsledky, najpodstatnejšie z nich sú zhrnuté v Závere článku.

1. POPIS VÝSKUMNÉHO SÚBORU

Výskum zameraný na vnímanie rizika Kybernetickej bezpečnosti, ako jednej z hybridných hrozieb, sa realizoval od 02/2023 do 07/2023 pomocou autorského výskumného nástroja. Výskumný nástroj bol distribuovaný respondentom (študenti vybraných vysokých škôl) v elektronickej forme a realizoval sa na základe dostupnosti. Výskumný súbor predstavuje celkovo $N=964$ respondentov.

Z hľadiska štruktúry je výskumný súbor tvorený 521 (54.046 %) mužmi a 443 (45.954 %) ženami z dvoch krajín. Respondentov zo Slovenskej republiky bolo celkovo 580 (60.166 %) a z Českej republiky 384 (39.834 %). Priemerný vek respondenta je 26.03 ± 0.51 roka so smerodajnou odchýlkou na úrovni 8.145 roka. Minimálny vek respondenta je 19 rokov a maximálny 63 rokov. Vek respondenta sa analyzoval aj ako ordinálna premenná, pričom respondentov mladších ako 25 rokov bolo celkovo 669 (69.398 %), respondentov vo veku 26 – 35 rokov bolo celkovo 156 (16.183 %), respondentov vo veku 36 – 45 rokov bolo 95 (9.855 %), respondentov vo veku 46 až 55 rokov bolo 41 (4.253 %) a respondenti starší ako 55 rokov boli traja (0.311 %). Z celkového počtu 964 respondentov študuje 321 (33.299 %) na bakalárskom stupni štúdia, 591 (61.307 %) na magisterskom stupni štúdia, 52 (5.394 %) na doktorandskom stupni štúdia a to v dennej forme 592 respondentov (61.411 %) a v externej forme 372 (38.589 %) respondentov. Detailnejšie členenie výskumnej vzorky z hľadiska krajiny, rodu a veku môžeme vidieť v Tab. 1.

Tab. 5 Základný popis výskumnej vzorky z hľadiska krajiny, rodu a veku respondenta

$N=964$	$COUNTRY$	GEN	$AGE1 < 25$ years	$AGE1 26 - 35$ years	$AGE1 36 - 45$ years	$AGE1 46 - 55$ years	$AGE1 > 55$ years	Row Totals
Count			135	60	34	4	0	233
Column Percent	SK	male	34.62%	54.05%	54.84%	23.53%		
Row Percent			57.94%	25.75%	14.59%	1.72%	0.00%	
Table Percent			23.28%	10.34%	5.86%	0.69%	0.00%	40.17%
Count			255	51	28	13	0	347
Column Percent	SK	female	65.38%	45.95%	45.16%	76.47%		
Row Percent			73.49%	14.70%	8.07%	3.75%	0.00%	
Table Percent			43.97%	8.79%	4.83%	2.24%	0.00%	59.83%
Count			390	111	62	17	0	580
Table Percent	Total		67,24%	19.14%	10.69%	2.93%	0.00%	100.00 %
Count			213	39	24	12	0	288
Column Percent	CZ	male	76.34%	86.67%	72.73%	50.00%	0.00%	
Row Percent			73.96%	13.54%	8.33%	4.17%	0.00%	
Table Percent			55.47%	10.16%	6.25%	3.13%	0.00%	75.00%

Count			66	6	9	12	3	96
Column Percent	CZ	femal e	23.66%	13.33%	27.27%	50.00%	100.00%	
Row Percent			68.75%	6.25%	9.38%	12.50%	3.13%	
Table Percent			17.19%	1.56%	2.34%	3.13%	0.78%	25.00%
Count			279	45	33	24	3	384
Table Percent	Total		72,66%	11.72%	8.59%	6.25%	0.78%	100.00%

COUNT – krajina, *GEN* – rod, *AGE1* – vek (v ordinálnej škále)

2. VÝSLEDKY A DISKUSIA

V rámci realizovaného výskumu zameraného na vnímanie stupňa závažnosti Kybernetickej bezpečnosti vo vzťahu k ohrozeniu Slovenskej republiky ako jedného z pilierov hybridných hrozieb sa využil autorský dotazník, ktorý pozostával z 5 základných položiek. Meranie je založené na subjektívnom vnímaní stupňa závažnosti ohrozenia štátu, pričom respondenti si vybrali odpovede z 5 stupňovej Likertovej škály: 1 – nezávažné, 2 – málo závažné, 3 – stredne závažné, 4 – závažné, 5 – vysoko závažné. Samotný výskumný nástroj bol rozdelený do piatich základných oblastí, pilierov Kybernetickej bezpečnosti:

1. Kybernetická špionáž (*CYBSPY*)
2. Narušenie alebo zníženie odolnosti IT infraštruktúry (*DISRIT*)
3. Nepriateľské kampane (*ENECAM*)
4. Narušenie alebo zníženie bezpečnosti eGoverementu (*DISREG*)
5. Kyberterorizmus (*CYBTER*)

Reliabilita celého výskumného nástroja, definovaná pomocou Cronbachovho koeficientu alfa, dosahuje hodnotu 0.83883 čo preukazuje, že chybová zložka rozptylu meraní je relatívne nízka a dlhšie položky výskumného nástroja sú vnútorne konzistentné. To znamená, že existuje vysoký stupeň zhody položiek výskumného nástroja v tom zmysle, že rovnako dobre odrážajú ten istý jav, v našom prípade Kybernetickú bezpečnosť.

Základnou výskumnou otázkou v rámci štúdie je „Aký je vzťah medzi základnými definovanými piliermi Kybernetickej bezpečnosti a základnými demografickými ukazovateľmi výskumnej vzorky?“ a súčasne „Existujú vo vnímaní závažnosti ohrozenia štátu diferencie medzi jednotlivými skupinami respondentov?“ Na zodpovedanie definovaných výskumných otázok bola použitá korešpondenčná analýza. Korešpondenčná analýza je štatistická metóda na analýzu vzťahov medzi kategóriami dvoch alebo viacerých premenných usporiadaných v kontingenčnej tabuľke [7]. Umožňuje skúmať asociáciu kategoriálnych premenných a získať prehľadné grafické zobrazenie súvislostí v dvojrozmernom, resp. viacrozmernom priestore. Cieľom je posúdiť vzájomný vzťah medzi premennými a vysvetliť štruktúru skúmanej závislosti.

Vstupnými premennými môžu byť akékoľvek kategoriálne premenné, ktoré sa dajú vyjadriť vo forme početností (absolútnych alebo relatívnych). Môžeme použiť nominálne, ordinálne alebo kvantitatívne diskkrétne premenné. Ak chceme pracovať s kvantitatívnymi spojitými premennými, musíme ich hodnoty rozdeliť do kategórií. Najdôležitejším výstupom analýzy je

multidimenzionálna mapa, ktorú nazývame korešpondenčná mapa. V nej sú prehľadne zobrazené výsledky analýzy, zaznačením vzťahov medzi kategóriami v priestore v rovnakých dimenziách. Umožní nám posúdiť kategórie danej premennej, ich vzájomnú podobnosť a rozdiely medzi nimi, prípadne asociácie s kategóriami iných premenných. Táto metóda je obzvlášť vhodná pri analýze kontingenčných tabuliek s veľkým počtom stĺpcov a riadkov, kde grafické zobrazenie môže byť omnoho prehľadnejšie ako tabuľkové výstupy. Korešpondenčná analýza je analógiou metódy hlavných komponentov a faktorovej analýzy v prípade kategoriálnych premenných. Pomocou nej hľadáme latentné skryté faktory, ktoré predstavujú osi korešpondenčnej mapy. Aplikáciou metódy získame ordinačné osi (dimenzie) s klesajúcim stupňom dôležitosti. Snažíme sa nájsť také riešenie, v ktorom je možné zakresliť hlavnú informáciu z pôvodnej tabuľky do podpriestoru s nižším počtom dimenzií, pri čo najmenšej strate informácií. Najčastejšie využívame dvojrozmerný priestor. V Tab. 2 uvádzame výsledky štatistickej analýzy dát získaných výskumným nástrojom.

Tab. 6 Analýza základných vzťahov medzi piliermi kybernetickej bezpečnosti a demografickými skupinami respondentov

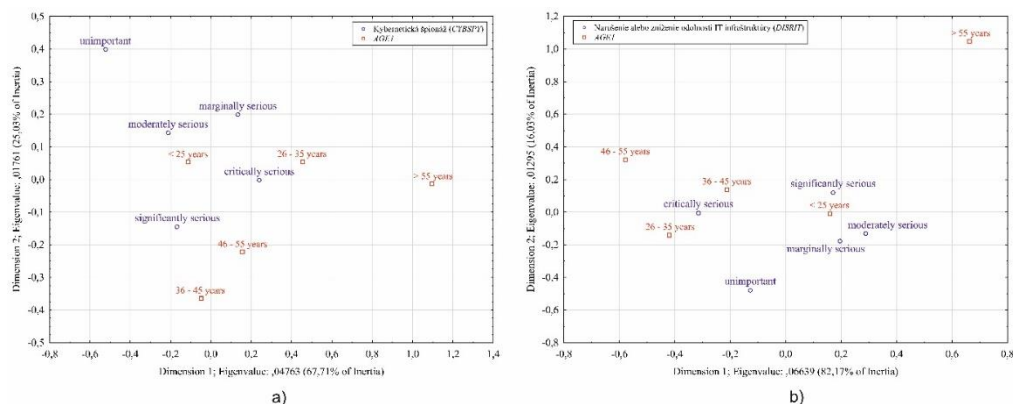
	<i>CYBSPY</i>	<i>DISRIT</i>	<i>ENECAM</i>	<i>DISREG</i>	<i>CYBTER</i>
<i>GEN</i>	$\chi^2=27.5093, df=4$ $p<0.0000^*$	$\chi^2=14.1700, df=4$ $p=0.0068^*$	$\chi^2=7.4798, df=4$ $p=0.1126$	$\chi^2=4.0842, df=4$ $p=0.3995$	$\chi^2=26.1286, df=4$ $p<0.0000^*$
<i>AGE1</i>	$\chi^2=67.8039, df=16$ $p<0.0000^*$	$\chi^2=77.8852, df=16$ $p<0.0000^*$	$\chi^2=63.5888, df=16$ $p<0.0000^*$	$\chi^2=53.3568, df=16$ $p<0.0000^*$	$\chi^2=43.7858, df=16$ $p=0.0002^*$
<i>GEDS</i>	$\chi^2=34.4236, df=8$ $p<0.0000^*$	$\chi^2=28.1860, df=8$ $p=0.0004^*$	$\chi^2=6.8043, df=8$ $p=0.5579$	$\chi^2=6.7789, df=8$ $p=0.5607$	$\chi^2=34.2927, df=8$ $p<0.0000^*$
<i>FORMS</i>	$\chi^2=15.5900, df=4$ $p=0.0036^*$	$\chi^2=31.2358, df=4$ $p<0.0000^*$	$\chi^2=41.6442, df=4$ $p<0.0000^*$	$\chi^2=17.2158, df=4$ $p=0.0018^*$	$\chi^2=12.0708, df=4$ $p=0.0168^*$
<i>PRAC2</i>	$\chi^2=13.9787, df=12$ $p=0.3015$	$\chi^2=29.5077, df=12$ $p=0.0033^*$	$\chi^2=33.8134, df=12$ $p=0.0007^*$	$\chi^2=12.1233, df=12$ $p=0.0267^*$	$\chi^2=18.6952, df=12$ $p=0.0962$
<i>COUNT</i>	$\chi^2=59.0466, df=4$ $p<0.0000^*$	$\chi^2=60.3971, df=4$ $p<0.0000^*$	$\chi^2=24.8875, df=4$ $p=0.0001^*$	$\chi^2=14.6885, df=4$ $p=0.0054^*$	$\chi^2=53.5031, df=4$ $p<0.0000^*$
<i>FAC</i>	$\chi^2=89.0235, df=12$ $p<0.0000^*$	$\chi^2=79.0140, df=12$ $p<0.0000^*$	$\chi^2=45.5495, df=12$ $p<0.0000^*$	$\chi^2=32.0480, df=12$ $p=0.0014^*$	$\chi^2=63.0897, df=12$ $p<0.0000^*$

CYBSY – kybernetická špionáž, *DISRIT* - Narušenie alebo zníženie odolnosti IT infraštruktúry, *ENECAM* - Nepriateľské kampane, *DISREG* - Narušenie alebo zníženie bezpečnosti eGoverementu, *CYBTER* – Kyberterorizmus, *GEN* – rod respondenta, *AGE1* – vek respondenta, *GEDS* – stupeň štúdia, *FORMS* – forma štúdia, *PRAC2* – dĺžka praxe, *COUNT* – krajina, *FAC* – fakulta, * - signifikantné na hladine významnosti $\alpha = 0.05$.

Z Tab. 2 vyplýva, že medzi jednotlivými piliermi kybernetickej bezpečnosti a demografickými údajmi respondentov existuje množstvo štatisticky významných väzieb. V predloženom príspevku sa zameriame iba niektoré z nich. Bude to predovšetkým väzba medzi rodom respondenta, vekom respondenta a jednotlivými piliermi kybernetickej bezpečnosti.

V prvom rade, na základe Tab.2 existuje štatisticky významný vzťah medzi rodom respondenta a vnímaním stupňa závažnosti Kybernetickej špionáže (*CYBSPY*). V prvom rade je potrebné spomenúť, že z celkového počtu 964 respondentov je v rámci výskumného súboru 443 žien a 521 mužov. Z analýzy vyplýva, že celkovo 1.129 % žien vníma kybernetickú špionáž ako nezávažné, 10.158 % ako málo závažné, 21.219 % ako stredne závažné, 33.634 % ako závažné a 33.860 % ako vysoko závažné ohrozenie. Naproti tomu 3.647 % mužov vníma kybernetickú špionáž ako nezávažné, 6.334 % ako málo závažné, 12.476 % ako stredne závažné, 33.781 % ako závažné a až 43.762 % ako vysoko závažné ohrozenie štátu. Vo všeobecnosti je tak možné prijať záver, že ženy vnímajú kybernetickú špionáž ako málo a stredne závažné ohrozenie štátu a naopak muži vnímajú skúmaný pilier kybernetickej bezpečnosti *CYBSPY* ako závažné a vysoko závažné ohrozenie. Druhý pilier kybernetickej bezpečnosti a to Narušenie alebo zníženie odolnosti IT infraštruktúry (*DISRIT*) vníma 1.129 % žien ako nezávažné, 6.772 % ako málo závažné, 22.348 % ako stredne závažné, 33.860 % ako závažné a 35.892 % ako vysoko závažné ohrozenie. Z pohľadu druhej skupiny respondentov a to mužov, tak 1.344 % mužov vníma Narušenie alebo zníženie odolnosti IT infraštruktúry ako nezávažné, 5.950 % ako málo závažné, 13.436 % ako stredne závažné, 37.620 % ako závažné a 41.651 % ako vysoko závažné ohrozenie štátu. Ďalším záverom, ktorý vyplýva z Tab.2 je skutočnosť, že medzi rodom a dvoma piliermi kybernetickej bezpečnosti, menovite Nepriateľské kampane (*ENECAM*) a Narušenie alebo zníženie bezpečnosti eGoverementu (*DISREG*), nie je signifikantný vzťah. Je teda možné povedať, že tieto dva piliere vnímajú muži aj ženy rovnako. Ďalšiu signifikantnú väzbu (Tab.2) nachádzame medzi rodom respondenta a vnímaním stupňa závažnosti piliera Kyberterorizmu (*CYBTER*). V rámci odpovedí ani jedna žena nepovažuje kyberterorizmus za nezávažné hrozenie. Ako málo závažné ohrozenie vníma kyberterorizmus 8.578 % žien, ako stredne závažné 16.479 %, ako závažné 35.666 % a ako vysoko závažné ohrozenie štátu 39.278 %. Naopak, muži za nezávažné ohrozenie považujú kyberterorizmus celkovo v 2.303 % prípadoch, ako málo závažné 2.879 %, ako stredne závažné 16.891 %, ako závažné 33.589 % a ako vysoko závažné ohrozenie považuje kyberterorizmus až 44.338 % mužov.

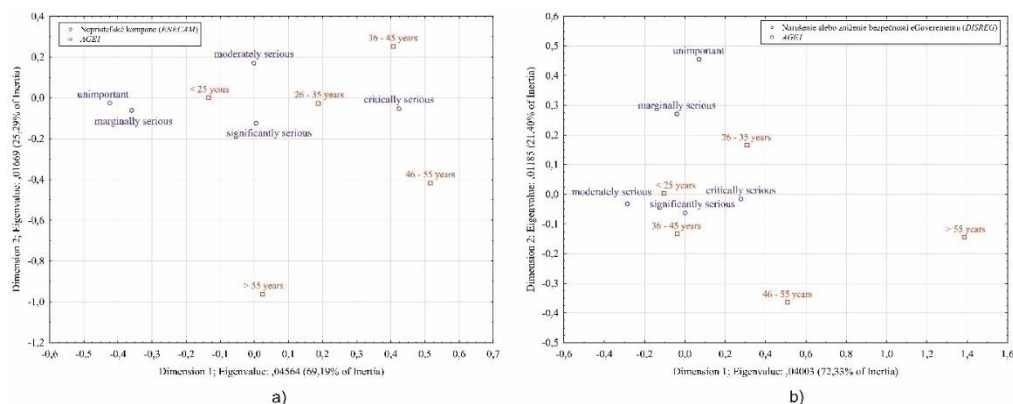
Vzťah veku respondentov a prvého piliera kybernetickej bezpečnosti a to kybernetickej špionáže (*CYBSPY*) vo forme korešpondenčnej mapy je uvedený na Obr. 1a. Z uvedeného obrázka vyplýva, že respondenti vo veku menej ako 25 rokov vnímajú kybernetickú špionáž ako stredne závažné ohrozenie, respondenti vo veku 26 až 35 rokov ako kritické ohrozenie a respondenti vo veku 36 až 55 rokov ako závažné ohrozenie štátu. Zaujímavosťou je aj skutočnosť, že kybernetickú špionáž považuje za nezávažné ohrozenie iba 3.587 % respondentov vo veku menej ako 25 rokov. Na druhej strane všetci respondenti starší ako 55 rokov považujú kybernetickú špionáž za vysoko závažné ohrozenie.



Obr. 2 Korešpondenčná mapa vzťahu Kybernetickej špionáže (a) a Narušenia alebo zníženia odolnosti IT infraštruktúry (b) a veku respondenta

Vzťah druhého piliera kybernetickej bezpečnosti a to Narušenie alebo zníženie odolnosti IT infraštruktúry (*DISRIT*) a veku respondenta je uvedený na Obr.1b. Z uvedeného vzťahu vo forme korešpondenčnej mapy vyplýva, že respondenti vo veku 26 až 45 rokov vnímajú skúmaný pilier (*DISRIT*) kybernetickej bezpečnosti ako vysoko závažné ohrozenie a respondenti vo veku nižšom ako 25 rokov ako stredne závažné, resp. závažné ohrozenie. Z detailnejšej analýzy odpovedí respondentov ďalej vyplýva, že všetci respondenti starší ako 55 rokov vnímajú pilier *DISRIT* ako závažné riziko a súčasne 34.146 % respondentov vo veku 46 až 55 rokov vnímajú Narušenie alebo zníženie odolnosti IT infraštruktúry ako závažné a 65.854 % respondentov v tejto vekovej skupine ako vysoko závažné ohrozenie.

Vzťah piliera kybernetickej bezpečnosti, ktorý sa definoval ako Nepriateľské kampane (*ENECAM*) a veku respondenta je uvedený na Obr. 2a. Z korešpondenčnej mapy vyplýva, že respondenti vo veku 25 až 35 rokov vnímajú tento pilier ako stredne závažné resp. závažné ohrozenie a respondenti vo veku 36 až 55 rokov ako vysoko závažné ohrozenie štátu. Za nezávažné ohrozenie považuje nepriateľské kampane iba 1.943 % respondentov vo veku nižšom ako 25 rokov a 1.282 % respondentov vo veku 26 až 35 rokov. Ostatné kategórie respondentov z pohľadu veku nepovažujú nepriateľské kampane za nezávažné. Na druhej strane všetci respondenti vo veku vyššom ako 55 rokov považujú tento pilier za vysoko závažné ohrozenie štátu.



Obr. 3 Korešpondenčná mapa vzťahu Nepriateľských kampaní (a) a Narušenia alebo zníženia bezpečnosti eGovernmentu (b) a veku respondenta

V poradí štvrtý pilier kybernetickej bezpečnosti a to Narušenie alebo zníženie bezpečnosti eGoverementu (*DISREG*) považujú respondenti vo veku nižšom ako 25 rokov za stredne závažné ohrozenie, respondenti vo veku 26 až 35 rokov za málo závažné a respondenti vo veku 36 – 45 rokov za závažné resp. vysoko závažné ohrozenie štátu (Obr. 2b). Za nezávažné považuje pilier kybernetickej bezpečnosti *DISREG* iba 0.747 % respondentov vo veku nižšom ako 25 rokov a iba 1.281 % respondentov vo veku 26 až 35 rokov. Na druhej strane 48.781 % respondentov vo veku 46 – 55 rokov považuje pilier *DISREG* za závažné a 43.902 % respondentov tejto vekovej skupiny ako vysoko závažné ohrozenie. Súčasne všetci respondenti vo veku vyššom ako 55 rokov považujú tento skúmaný pilier kybernetickej bezpečnosti ako vysoko závažné ohrozenie bezpečnosti štátu.

Posledný pilier kybernetickej bezpečnosti a to kyberterorizmus (*CYBTER*) považujú respondenti vo veku nižšom ako 25 rokov za málo závažné resp. stredne závažné, respondenti vo veku 26 až 35 rokov za závažné, respondenti vo veku 36 až 45 rokov za nezávažné a respondenti vo veku 46 až 55 rokov za vysoko závažné ohrozenie bezpečnosti štátu. Tu je nutné podotknúť, že za nezávažné ohrozenie považuje kyberterorizmus 1.046 % respondentov vo veku nižšom ako 25 rokov, 1.282 % respondentov vo veku 26 – 35 rokov a 3.158 % respondentov vo veku 36 – 45 rokov. Rovnako ako v predchádzajúcich prípadoch, všetci respondenti vnímajú kyberterorizmus ako vysoko závažné ohrozenie štátu.

ZÁVER

Pred hrozbami v kybernetickom priestore nie je v dnešnej dobe úplne chránený žiadny štát. Zhoršujúca sa bezpečnostná situácia nie je iba v oblastiach, ktoré bezprostredne susedia s členskými štátmi NATO, EU umocňuje zvyšujúce sa nároky na schopnosti krajín samostatne reagovať na bezpečnostné hrozby v kybernetickom priestore [2]. Je možné pozorovať rastúce snahy štátnych aj neštátnych aktérov v budovaní a používaní kybernetických ofenzívnych prostriedkov [8], ktorých cieľom je predovšetkým kritická infraštruktúra, resp. jej časť vystavená v kybernetickom priestore – kritická informačná infraštruktúra a významné informačné systémy. Práve tie totiž predstavujú kľúčový systém prvkov, ktorých narušenie alebo nefunkčnosť by malo závažný dopad na bezpečnosť štátu, na zabezpečenie základných životných potrieb obyvateľstva v rôznych oblastiach, alebo na ekonomickú situáciu.

V rámci predloženej štúdie sme sa zamerali na analýzu názorov a postojov k hodnoteniu rizík jednej zo základných súčastí hybridnej hrozby a to Kybernetickej bezpečnosti na základe štatistickej analýzy dát získaných pomocou autorského výskumného nástroja. Ten bol implementovaný na vzorke ($N=964$) študentov Slovenskej a Českej republiky, ktorí študujú na vysokých školách policajného a armádne typu štúdia. Voľba cieľovej skupiny respondentov bola motivovaná skutočnosťou, že práve táto skupina respondentov bude v budúcnosti predstavovať prvú líniu boja proti hybridným hrozbám. Výskumný nástroj ako taký vychádza z oficiálnych dokumentov Slovenskej a Českej republiky v oblasti bezpečnosti.

V rámci realizovanej matematicko-štatistickej analýzy dát je možné konštatovať, že existujú významné väzby medzi jednotlivými definovanými piliermi kybernetickej bezpečnosti a demografickými znakmi respondentov. Vo vzťahu k rodu respondenta môžeme prijať záver, že v prípade štatisticky významných väzieb (*CYBSPY*, *DISRIT* a *CYBTER*) ženy vo všeobecnosti vnímajú jednotlivé piliere ako málo závažné resp. stredne závažné a muži ako závažné resp.

vysoko závažné ohrozenie bezpečnosti štátu. Všeobecným záverom analýzy vzťahu veku respondentov a štatisticky významných pilierov kybernetickej bezpečnosti (*CYBSPY*, *DISRIT*, *ENECAM*, *DISREG* a *CYBTER*) je, že so zvyšujúcim sa vekom respondenta sa zvyšuje vnímanie stupňa ohrozenia bezpečnosti štátu.

Predložený príspevok predstavuje základnú analýzu vzťahov medzi definovanými piliermi kybernetickej bezpečnosti a základnými demografickými znakmi respondentov (rod a vek). Určite by bolo zaujímavé detailne rozobrať aj ostatné významné vzťahy uvedené v Tab. 2, čo však rozsah príspevku neumožňuje. Okrem tejto hybridnej hrozby (Kybernetická bezpečnosť) je potrebné venovať pozornosť aj iným hybridným hrozbám, ako je napr. energetická a priemyselná bezpečnosť, strategická komunikácia, pôsobenie cudzej moci, organizovaný zločin a strategická korupcia, extrémizmus, environmentálna bezpečnosť a umelá inteligencia, z pohľadu vnímania rizika jednotlivých hybridných hrozieb respondentami ako aj analýze vzťahu medzi jednotlivými hybridnými hrozbami. Týmto otázkam sa autorský kolektív v súčasnosti intenzívne venuje.

Podakovanie

Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Acknowledgement

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

Zdroje

1. Granholm, F., Tin, D., Ciottone, G. R. (2022) Not war, not terrorism, the impact of hybrid warfare on emergency medicine, *The American Journal of Emergency Medicine*, Volume 62, 2022, pp. 96-100, ISSN 0735-6757, <https://doi.org/10.1016/j.ajem.2022.10.021>
2. Procházka, J., Vinkler, P., Jojart, K., Szenes, Z., Gruszczak, A., Kandrik, M. (2023) One threat – multiple responses. Countering Hybrid Threats in V4 countries/Jedna hrozba – více způsobů reakce. Čelení hybridnímu působení v zemích V4. Obrana a strategie (Defence and Strategy), 23, p. 049-073. doi: 10.3849/1802-7199.23.2023.01.049-073
3. Eberle, J., Daniel, J. (2022) Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety, *Political Geography*, Vol. 92, 2022, 102502, ISSN 0962-6298, <https://doi.org/10.1016/j.polgeo.2021.102502>.
4. Mekala, S.H., Baig, Z., Anwar, A., Zeadally, S. (2022) Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions, *Computer Communications*, Vol. 208, 2023, p. 294-320, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2023.06.020>
5. Qin, X., Jiang, F., Cen, M., Doss, R. (2023) Hybrid cyber defense strategies using Honey-X: A survey, *Computer Networks*, Vol. 230, 2023, ISSN 1389-1286, <https://doi.org/10.1016/j.comnet.2023.109776>
6. Hausken, K. (2020) Cyber resilience in firms, organizations and societies, *Internet of Things*, Vol. 11, 2020, 100204, ISSN 2542-6605, <https://doi.org/10.1016/j.iot.2020.100204>
7. Luiz Paulo Fávero, Patrícia Belfiore, Rafael de Freitas Souza, Chapter 13 - Simple and multiple correspondence analysis, Editor(s): Luiz Paulo Fávero, Patrícia Belfiore, Rafael de Freitas

Souza, Data Science, Analytics and Machine Learning with R, Academic Press, 2023, p. 215-234, ISBN 9780128242711, <https://doi.org/10.1016/B978-0-12-824271-1.00013-5>

8. Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar (2023) Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535, <https://doi.org/10.1016/j.inffus.2023.101804>

ONLINE PRIESTOR AKO PROSTRIEDOK NA OVPLYVNŔOVANIA VEREJNEJ MIENKY POČAS VOLEBNEJ KAMPANE V PARLAMENTNÝCH VOĽBÁCH SLOVENSKEJ REPUBLIKY V ROKU 2023

doc, RNDr. Tatiana Hajdúková, PhD.

Katedra informatiky a manažmentu Akadémie Policajného zboru v Bratislave; Sklabinská 1, 831 06 Bratislava, hajdukova@akademiapz.sk

Abstrakt: Polarizácia spoločnosti zjednodušuje podmienky na ovplyvňovanie volebných procesov ako aj volebných výsledkov. Cieľom príspevku je poukázať na možnosti ovplyvňovania verejnej mienky nástrojmi dostupnými v online priestore. V analytickej časti sa príspevok koncentruje na volebnú kampaň v Slovenskej republike pri predčasných voľbách do Národnej rady Slovenskej republiky v roku 2023, z ktorej boli čerpané reálne dáta. Rozlišovanie politických strán je prevedené pomocou číselných kódov, nakoľko nie je účelom príspevku riešiť volebné programy jednotlivých politických strán. Kvantitatívnymi a kvalitatívnymi metódami poukazujeme na variabilitu a taktiku realizácie politickej kampane bez akejkoľvek ambície predikovať volebné výsledky. Sústreďujeme sa na vybrané porušenia volebného zákona pri volebnej kampani v online priestore, ktoré môžu predstavovať ohrozenie stability a demokratického fungovania štátu a jeho ďalšieho politického smerovania.

Kľúčové slová: volebná kampaň, dezinformácie, manipulácia s verejnou mienkou.

ÚVOD

Ako uvádza (Nemec, 1998) od narodenia až do konca života je naša existencia ovplyvňovaná rôznymi formami aktivít štátu. Tvrdenie je platné nezávisle od politického zriadenia a krajiny. Teória verejnej politiky sa zaoberá postupmi kolektivizovania individuálnych záujmov do záujmov nadindividuálnych. Prostredníctvom verejnej politiky subjekty sociálne štruktúrovanej spoločnosti aktívne obhajujú a presadzujú svoje záujmy. Verejná politika predstavuje interakcie, v ktorých sa združujú aktéri z verejného, komerčného i občianskeho sektora (Potůček 2016). Podľa Ľ. Malíkovej „najlepšie pochopíme povahu procesu tvorby verejnej politiky, ak poznáme štruktúru záujmov aktérov a interakcie medzi nimi. (M. Nekola a V. Novotný 2010) klasifikujú metódy verejnej politiky, do dvoch skupín:

- 1) teória spoločne využívaných zdrojov ktorá predpokladá, že jednotlivci nie sú schopní vzájomne kooperovať a kolektívne dosahovať lepšie výsledky, ako by mohli dosiahnuť individuálne.
- 2) skupina teórií, ktoré uprednostňujú význam jednotlivcov a otázku kolektívneho správania dávajú viac do pozadia. V podstate sa jedná o kolektivizovanie individuálnych záujmov do nadindividuálnych záujmov vytváraním rôznych štruktúr a väzieb medzi sebou, v ktorých kooperujú alebo si konkurujú, hľadajú varianty možnosti riešenia alebo i financovania rôznych problémov, vytvárajú medzi sebou koalície, partnerstvá, uzatvárajú zmluvy a dohody, organizujú petície, presadzujú prijímanie alebo pripomienkovanie zákonov atď.

Účasť v politike dynamizuje politický proces a vytvára predpoklady k tomu, aby politická sféra vyvážene akceptovala široké spektrum záujmov, ktoré v spoločnosti vznikajú. „Volebnou účasťou získavajú občania alternatívne kanály pre artikuláciu svojich záujmov“ (Zetková 2016). Vo všeobecnosti môžeme volebné právo deliť na objektívne a subjektívne. V objektívnom zmysle volebné právo predstavuje súbor všetkých právnych noriem, úlohou ktorých je regulovať vzťahy vznikajúce pri príprave, organizácii a uskutočňovaní volieb a zisťovaní či kontrole ich výsledkov (Palúš – Somorová, 2014). Objektívne právo je teda právna úprava volieb obsiahnutá v ústave, zákonoch, ale aj rozhodnutiach ústavného súdu. V subjektívnom zmysle volebným právom rozumieme právo občanov podieľať sa na tvorbe štátnych orgánov a orgánov územnej samosprávy (Palúš a kol., 2016). Ústava Slovenskej republiky poskytuje rámec pre uplatňovanie volebného práva a s ním súvisiace ďalšie politické práva. Na vykonanie jednotlivých ustanovení ústavy slúži volebný kódex, ktorý podrobne upravuje všetky typy a všetky štádia volieb. Podľa Zákona č. 180/2014 Z.z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov (ďalej volebný zákon) volebná kampaň je akákoľvek činnosť strany, koalície alebo kandidátov, za ktorú sa obvykle platí úhrada smerujúca k propagácii ich činnosti, cieľov a programu s cieľom získania funkcie. Znakom demokratickej spoločnosti je periodické organizovanie volieb do zastupiteľských orgánov, aby mali občania priestor na slobodné vyjadrenie svojej vôle. Vzhľadom na vopred ohraničené maximálne trvanie volebného obdobia, volebné kampane majú svoju periodicitu, čo čiastočne prispieva k ich zovšedneniu. Aby tomu tak nebolo, pomerne často vyjadrovanie sklzáva do rétoriky, ako sú nadchádzajúce voľby zlomové, že sa v nich rozhodne o budúcnosti, že sú z pohľadu budúcnosti dôležitejšie než predošlé. Deje sa to s cieľom zvýšiť volebnú účasť, ovplyvniť koho majú voliči voliť. Linek (2015) pri skúmaní volebnej účasti v parlamentných voľbách v Českej republike v roku 2013 zistil, že volebnú účasť vo výraznejšej miere ovplyvňuje mobilizácia voliča či už priama (oslovenie kandidátom a podobne) alebo nepriama (rodinným príslušníkom, známymi). Druhým jeho zistením je, že volebná účasť je výrazne vyššia u ľudí, ktorí považujú ísť voliť za povinnosť oproti tým, ktorí to považujú len za právo.

V každom prípade je zrejmé, že vzhľadom na zložitosť a previazanosť súvislostí sa na formovaní volebnej kampane podieľa väčší počet vstupov. Pre rozhodovanie každého voliča je dôležité, aby mal informácie a rozumel udalostiam, ktoré sa v spoločnosti odohrávajú. Ako negatívum treba vnímať, že participácia občanov na veciach verejných prostredníctvom verejných diskusií býva častokrát sprevádzaná šírením zavádzajúceho a manipulatívneho obsahu (Korauš et. al 2022). Čiastočné alebo rozporuplné informácie podkopávajú istotu v rozhodovaní a voliča dostávajú do neistoty. Niekedy je naozaj ťažké rozlíšiť a nájsť etickú hranicu medzi slobodou slova, alternatívnym myslením, manipuláciou, “hlúposťou” alebo úmyselným klamstvom, konšpiráciou či hoaxom (Ivančík and Andrassy 2023). Predvolebné obdobie zvyknú sprevádzať informačné, manipulačné a dezinformačné kampane. Vzájomne protirečiacie si informácie obvykle vyvolávajú napätie, nedôveru a pochybnosti u jednotlivcov, v dôsledku ktorých dochádza ku polarizácii spoločnosti (Lisoň and Fidler 2022, Grant 2019). Účelom dezinformačných kampaní v kontexte volebných procesov je snaha o ovplyvnenie ich výsledku posilnením politických preferencií, alebo opozitne diskreditovaním politických preferencií protikandidátov.

(Charta základných ľudských práv Európskej únie, 2016) presadzuje názor, že ľudské práva sú vykonateľné ako v „offline“, tak aj v „online“ priestore. Online priestor musíme považovať za ekvivalent fyzického sveta, spolu s aplikáciou jednoznačných pravidiel, ktoré budú rešpektovať ústavou garantované základné ľudské práva a slobody, vrátane práva na súkromie tak, aby bol

nielen bezpečný, ale aj otvorený, slobodný a prístupný pre všetkých, ktorí doň vstupujú. Tak ako fyzický svet, ani kybernetický priestor nie je ideálnym a dokonale bezpečným miestom. Technologické inovácie sa stávajú nástrojom úmyselného hybridného pôsobenia, jedným z účelov ktorého býva zvyšovanie napätia v spoločnosti, jedno či v politickej, hospodárskej či bezpečnostnej oblasti.

Cieľom príspevku je poukázať na niektoré spôsoby ovplyvňovania voličov v online priestore, v ktorom interaguje čoraz väčšie množstvo používateľov a to častejšie a dlhší čas, čo vytvára vhodné predpoklady pre oslovovanie voličov. S cieľom odhaliť niektoré determinanty výsledkov posledných parlamentných volieb v SR v roku 2023, v analytickej časti príspevku sme využili agregované dáta, ku ktorým nie sú dostupné dáta z výberových zisťovaní. Agregované dáta pochádzajú zo sekundárnych zdrojov a to Štatistického úradu SR a z verejne dostupnej databázy vytvorenej organizáciou Transparency International Slovensko. Zdrojové údaje síce neponúkajú priame informácie, ale informácie s tým súvisiace. Použité boli multivariantné štatistické metódy ako je korelačná a korešpondenčná analýza.

1. ŠPECIFIKÁ VOLEBNEJ KAMPANE V ONLINE PRIESTORE

Prvý krát v histórii parlamentných volieb v Slovenskej republike boli výdavky na kampaňové podujatia v roku 2023 nižšie, ako na online reklamu.¹⁷⁹ Online prostredie je osobitné a čoraz viac sa presadzuje na úkor klasických offline mediálnych kampaní alebo billboardov. Verejné prezentovanie názorov a postojov nikdy nebolo dostupnejšie, ako v prostredí internetu. Politické subjekty sa v poslednej kampani presunuli z webových stránok a e-mailov na sociálne siete. Koncepcia sociálnych sietí sa rozvinula v pomerne nedávnej minulosti v polovici 80. rokov v USA (J. Coleman, D. Putnam) a vo Francúzsku (P. Bourdieu), pričom sociálnymi sieťami sú znaky sociálnych organizácií, ako napr. účasť občanov, normy vzájomnosti a dôvera k ostatným, ktoré umožňujú obojstranne výhodnú spoluprácu (Putnam, 1993). Vzhľadom na zameranie článku, v ďalšej časti problematiku online priestoru budeme vnímať z hľadiska realizácie politickej kampane v kontexte uplatnenia volebného práva. V online priestore sa nezmenili ani tak praktiky predvolebného boja, ako výrazne vzrástol jeho rozsah, rýchlosť šírenia informácií a účinok na voličov. Komunikácia občanov s ich volebnými zástupcami v online priestore umožňuje výmenu názorov na každodennej báze pred širokým publikom. Pretože pre mnohých občanov sa sociálne siete stali hlavným zdrojom informácií, presadili sa ako vplyvná platforma pre politické kampane a verejné diskusie, aj napriek tomu, že v tomto prostredí je vo všeobecnosti konštatovaný nedostatok regulácie. Ťažko sa udržiava kontrola nad účelovo zostrihanými videami, zmanipulovanými audionahrávkami, produktami zneužívajúcimi technológiou deep fake či falošnými a nepravdivými informáciami obzvlášť, ak sú šírené aktivistami z anonymných alebo falošných účtov.

Oslovovanie voličov je oveľa účinnejšie prostredníctvom veľkých platforiem ako pri fyzickom stretnutí, pretože inzerciuvidia desiatky tisíc ľudí. Analýza a osobné profilovanie používateľov na základe ich dát otvára dvere k veľmi precíznej a efektívnej manipulácii. Ako uvádza (Bond et al. 2012) v roku 2010 vyskúšal Facebook experimentálne zobrazovať 61 miliónom Američanov výzvu, aby išli voliť. V rámci experimentu boli zobrazované dve podoby výziev. V druhej podobe výzvy boli v porovnaní s prvou výzvou navyše fotografie priateľov danej osoby, o ktorých už Facebook

¹⁷⁹ Podľa údajov vedených na transparentných účtoch politických strán.

vedel, že odvolili (oznámili to na svojom profile na Facebooku). Drobná alternácia upozornenia spojená so známymi osobami formou nepriamej mobilizácie vyburcovala k voľbám o 340 000 voličov navyše. V roku 2012 Facebook experiment zopakoval a oznámil, že sa mu takto podarilo zvýšiť počet voličov o 270 000. Jedná sa o názorný príklad, ako môže stúpnuť intenzita vplyvu na voličské rozhodovanie pri intervencii známych osôb alebo priateľov. Ako je z týchto príkladov vidieť, výrazne ovplyvnenie volebných výsledkov môže byť dôsledkom aj na prvý pohľad triviálnej a na oko nevýznamnej udalosti. Nemusí sa nutne skladať zo šírenia dezinformácií či očierňovania konkrétneho kandidáta.

Ešte výraznejšie zmeny vo volebných výsledkoch by bolo možné dosiahnuť, ak by sa menej účinná správu zobrazila voličom jednej strany a účinnejšia voličom druhej. Z pohľadu prevádzkovateľov sociálnych sietí na základe komentárov či z osobného profilu alebo strojovo, podľa toho aké články osoba „lajkuje“, zdieľa či skrátka len otvára je triviálne určiť, aké základné volebné preferencie osoba má. Dnes sa ukazuje analýza a osobné profilovanie používateľov na základe ich dát ako veľmi precízny a efektívny nástroj na manipuláciu. Hoci je cieľená reklama technologicky aj softvérovo dobre zvládnutá, v prípade volebnej kampane zvykne byť legislatívne zakázaná (napr. Slovenská republika, Česká republika, Poľsko) ako pre politické strany tak aj pre tretie strany. Bez ohľadu na právne prostredie krajiny, cieľená reklama nie je principiálne poskytovaná ani súkromnými poskytovateľmi elektronických služieb formou reklamy.

Zmena názoru a volebnej preferencie ale nemusí byť vždy hlavný účel kampane. Ako príklad uvádzame víťazné prezidentské voľby Donalda Trampa v USA v roku 2016 (Green and Issenberg 2016). Manažéri tejto volebnej kampane verejne priznali, že na Facebooku vykonali akciu, účelom ktorej bola „demobilizácia“. Bola cieľená na Afroameričanov a ženy v kľúčových oblastiach, pričom kampaň v nich mala vyvolať apatie a nechť voliť.

Nakoľko majú veľké spoločnosti, ktoré prevádzkujú sociálne siete celosvetovú pôsobnosť, poskytujú svoje služby v krajinách s rôznymi zákonnými podmienkami. V záujme všeobecnej spokojnosti podporujú zodpovednú politickú reklamu, t.j. všetky politické reklamy a ciele dodržiavajú [miestne zákonné podmienky](#), ktoré zahŕňajú právne predpisy týkajúce sa volebných kampaní a volieb, ako aj moratórií, a to v prípade všetkých geografických oblastí, na ktoré tieto reklamy zaciľujú. Súčasne neumožňujú inzerentom zacieliť politickú reklamu na konkrétnych používateľov na základe ich politických preferencií.

Svojimi reklamami politické strany nemôžu propagovať nenávisťné reklamy, zastrážujúci a obťažujúci obsah, obsah zameraný na zneužívanie iných, reklamy obsahujúce vulgarizmy a nadávky, či udalosti s citlivým charakterom, napríklad zneužitie tragickej udalosti. Pokiaľ by došlo k závažnému porušeniu týchto pravidiel, platformy rýchlo a jednoducho dokážu nevhodné reklamy blokovat a zostane v záujme inzerenta odstrániť alebo opraviť závadný obsah.

Tam, kde sa pohybujú voliči, tam sa zákonite presúvajú aj činnosti a prostriedky spojené s volebnou kampaňou. Volebná kalkulačka nepatrí síce k novým, ale novším online volebným nástrojom, ktoré sú apolitické a nie sú priamou súčasťou volebnej kampane ale doplnkový informačný zdroj. Cieľom volebnej kalkulačky nie je počítať ako by mohlo vyplývať z jej názvu, ale poradiť voličovi pri rozhodovaní. Volebná kalkulačka už bola opakovane využitá vo viacerých európskych krajinách, napríklad na Slovensku, Maďarsku, Poľsku pri rôznych typoch volieb. Na základe osobného záujmu je kalkulačka schopná voličovi poskytnúť porovnanie jeho názorov

s programami, verejnými vyjadreniami a názormi všetkých strán kandidujúcich v konkrétnych voľbách. Porovnanie názorov je sprostredkované odpoveďami na súbor desiatok zmysluplných otázok dôležitých pre voliča pri daných voľbách. Účelom online aplikácie je diskrétno bez toho, aby jeho odpovede boli niekde archivované alebo zverejňované odporučiť názorovo najvhodnejšiu politickú stranu, ktorá by mohla najlepšie presadzovať záujmy voliča. Vyhodnocovaná je blízkosť, resp. rozdielnosť odpovedí. Odporúčanie politickej strany vychádza z najväčšej zhody pri odpovediach voliča a kandidáta, preto je dôležitá úprimnosť voliča.

Volebná kalkulačka by v prípade skresleného algoritmu mohla fungovať ako účinný manipulatívny nástroj, napríklad keby zvýhodňovala vybraného kandidáta. Pri vzniku takéhoto podozrenia si každý môže preveriť jej funkčnosť opakovaným použitím napríklad s vedome odlišnými odpoveďami. Pokiaľ by sa druhý výsledok kalkulačky nelíšil, podozrenie by bolo potvrdené. Možnosť verejnej kontroly by mal byť dostatočný kontrolný nástroj, aby prevádzkovatelia volebnej kalkulačky týmto spôsobom neohrozovali svoju reputáciu. Konečné rozhodnutie vo voľbách zostáva stále na voličovi a je nezávislé od odporúčania volebnej kalkulačky.

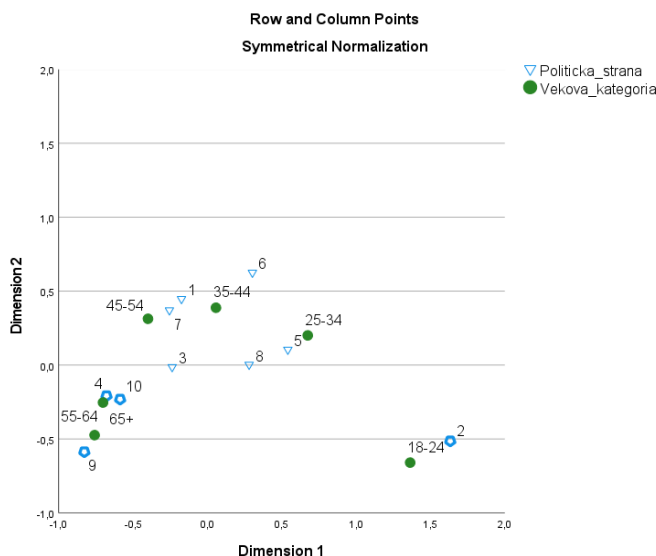
2. ANALÝZA VOLEBNEJ KAMPANE DO NÁRODNEJ RADY V SLOVENSKEJ REPUBLIKE V ROKU 2023

Z hľadiska formátu reklamy pri online volebnej kampani prostredníctvom služieb Google Ads a Google Display & Video 360 vo všeobecnosti bez ohľadu na politickú stranu sa v sledovanej volebnej kampani presadili hlavne videá, s podielom takmer 70% oproti obrázkom, ktorých podiel dosiahol cca 32 %¹⁸⁰. Dynamický audiovizuálny obraz je pridaná hodnota, ktorú statický billboard neposkytuje, preto je pochopiteľná dominancia tohto formátu v rámci online kampane v 21. storočí. Využitie obrázkov v politickej reklame online bolo doplnkové a textová reklama bola v online prostredí zanedbateľná na úrovni percenta.

Významným faktorom ovplyvňujúcim volebnú účasť a tým aj výsledky volieb podľa Gyárfášovej a Krivého (2013) je vek. Gyárfášová a Krivý uvádzajú, že na rozdiel od západných krajín, sa na Slovensku nedá hovoriť o vzťahu volebnej účasti a veku ako o trende obráteného písmena U, pretože ľudia v dôchodkovom veku majú približne rovnakú volebnú účasť ako stredná generácia, na rozdiel od mladých ľudí, ktorí sa vyznačujú nižšou volebnou účasťou ako staršie ročníky. Z vyhodnocovania výsledkov volieb nie je možné exaktne určiť vekovú štruktúru voličov jednotlivých politických strán. Istým priblížením zmýšľania a volebného rozhodovania sa občanov z hľadiska veku predstavuje sledovanosť volebnej online reklamy. Na obrázku č. 1 je zobrazený výsledok korešpondenčnej analýzy pomocou korešpondenčnej mapy, ktorá umožňuje vizuálne porovnať rozdiely viacrozmernej štruktúry, konkrétne vzťah medzi vekom osôb sledujúcich online reklamu politických strán vzhľadom na kandidujúce politické strany v predčasných parlamentných voľbách v SR v roku 2023.

¹⁸⁰ Zdroj údajov Transparency International Slovensko

Obrázok 1 Korešpondenčná mapa sledovanosti reklamy politických strán v online priestore vzhľadom na vek osôb



Zdroj: vlastné spracovanie z údajov Transparency International

Podľa sledovanosti volebnej online reklamy z pohľadu veku potencionálnych voličov boli zaznamenané zreteľné diferencie, ktoré poukazujú na prítomnosť generačných názorových rozdielov. V kategórii najmladších voličov vo veku do 24 rokov sa záujem výrazne vyhranil na jednu politickú stranu. Voliči vo veku medzi 25 až 34 rokov svoj zvýšený záujem rozdelili medzi iné dve politické strany. Pri voličoch nad 35 rokov bol záujem diverzifikovaný medzi viac politických strán. Podľa Plutzerovej vývojovej teórie sa pravidelní nevoliči postupne s rastúcim vekom stávajú pravidelnými voličmi (Plutzerová, 2002). Na základe uvedeného, oslovenie staršieho voliča má väčší potenciál volebného úspechu, ako mladšieho voliča.

Na určenie sily vzťahu medzi všetkými priznanými výdavkami na volebnú kampaň na transparentnom účte (komplet výdaje), výdavkami na reklamu na sociálnych sieťach platformy META (META), výdavkami na reklamu prostredníctvom služieb Google Ads a Google Display & Video 360 (Google), všetkými výdavkami zníženými o online reklamu (Ostatné) jednotlivých politických strán a výsledkami volieb sme použili korelačnú analýzu, výsledky ktorej sa nachádzajú v tabuľke č. 1.

Tabuľka 1 Výsledok korelačnej analýzy medzi výdavkami na volebnú kampaň a výsledkami volieb podľa kandidujúcich politických strán

	Komplet výdaje		META	Google	Ostatné	výsledky 2023
Komplet výdaje	Pearson Correlation	1	,597*	0,479	,994**	,791**
	Sig. (2-tailed)		0,031	0,098	0,000	0,001
	N	13	13	13	13	13
META	Pearson Correlation	,597*	1	0,409	0,532	0,237
	Sig. (2-tailed)	0,031		0,165	0,061	0,437
	N	13	13	13	13	13
Google	Pearson Correlation	0,479	0,409	1	0,397	0,185
	Sig. (2-tailed)	0,098	0,165		0,179	0,545
	N	13	13	13	13	13
Ostatné	Pearson Correlation	,994**	0,532	0,397	1	,822**
	Sig. (2-tailed)	0,000	0,061	0,179		0,001
	N	13	13	13	13	13
výsledky_2023	Pearson Correlation	,791**	0,237	0,185	,822**	1
	Sig. (2-tailed)	0,001	0,437	0,545	0,001	
	N	13	13	13	13	13

Veľmi vysoký koeficient korelácie 0,994 medzi skúmanými premennými v spojitosti s použitím financií na volebnú kampaň vznikol pri všetkých priznaných výdavkoch na politickú kampaň a ostatnými výdavkami, t.j. všetky priznané výdavky na politickú kampaň znížené o výdavky na Meta a Google reklamu. Výsledok indikuje, že popri financovaní klasickej volebnej kampani sa obvykle paralelne investovali prostriedky aj na Meta reklamu a Google reklamu. Porovnanie Pearsonovho koeficienta korelácie výsledkov parlamentných volieb s jednotlivými výdavkami na volebnú kampaň indikuje, že najväčší koeficient korelácie nastal pri ostatných výdavkoch, následne všetkých výdavkoch a pri Meta reklame a Google reklame výrazne klesol pod štatisticky významnú hodnotu. Výsledok v parlamentných voľbách v roku 2023 poukazuje na pretrvávajúci vplyv klasických reklamných nástrojov v rámci volebnej kampane, ako boli dosiahnuté prostredníctvom Meta reklamy a Google reklamy.

ZÁVER

Podľa Rosanvallona je model legitimizácie moci, založený na voľbách a dôvere voličov v stranu, ktorá získala následne parlamentnú väčšinu, už zastaraným modelom. Demokratické mechanizmy

a globálne problémy sa stali príliš komplexnými a previazanými s nadnárodnými záujmami na to, aby sa vôľa zvolených predstaviteľov spoločnosti mohla v plnej miere implementovať. Občania stále aktívnejšie žiadajú, aby sa v procese uplatňovania moci uznali ich individuálne záujmy. Demokratická legitimita moderného štátu preto závisí viac od existencie a efektívnosti kontrolných, dozorných a regulačných inštitúcií, ako aj od kvality kontaktu medzi orgánmi a občanmi a v menšej miere od mandátu, ktorý zástupcovia dostávajú každých niekoľko rokov" (Bodnar 2011, s. 35). Nepodliehanie vplyvu záujmových skupín je princípom nestrannosti nielen počas volebnej kampane, legitimacy týchto agentúr, uznávaných verejnosťou.

Spoločnosť nepredstavuje všeobecnú masu občanov, ale súčet početných individuálnych záujmov, na ktoré musia orgány reagovať. Dosahuje sa to inštitucionálne prostredníctvom kreovania funkcií rôznych ombudsmanov, ale aj posilňovaním transparentnosti činnosti orgánov, účasťou občanov na rozhodovacom procese, uplatňovaním procedurálnej spravodlivosti a pod. (Rosanvallon 2010, s. 209 - 270, Bodnar 2011, s. 35). Je v záujme rozvoja spoločnosti, aby sa občania aktívne zaujímali a zapájali do verejných vecí a využívali možnosť kontroly. Informácie zverejnené v online priestore sú pre občana časovo aj kvantitatívne dostupnejšie, ako v printovej podobe, preto je predpoklad, že pôsobenie na občanov cez toto médium bude narastať. Hoci sme v parlamentných voľbách v roku 2023 nezaznamenali významnú koreláciu výdavkov na Meta reklamu a Google reklamu s výsledkami volieb, dá sa očakávať, že bude pokračovať narastanie vplyvu online komunikácie ako v bežnom živote, tak aj pri volebnej kampani.

PodĎakovanie

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

Zdroje

1. Bodnar, A. 2011. Koniec mitu tradycijnej legítymizacji władzy, *Res Publica Nowa* 2011, nr 16, s. 34–3
2. Bond, R., Fariss, Ch. J. Jones J J., Kramer, A. D., Marlow, C., Settle, J. (2012). A 61-million-person experiment in social influence and political mobilization online <https://research.facebook.com/file/356087889503631/a-61-million-person-experiment-in-social-influence-and-political-mobilization.pdf>, doi: 10.1038/nature11421
3. Coleman, J. S. 1988. Social Capital in the Creation of Human Capital. In: *American Journal of Sociology*, Vol.94., 1988, p. 95-120
4. Ivančík, R. – Andassy, V. 2023. Insights into the development of the security concept. In *Entrepreneurship and Sustainability Issues*, 2023, Vol. 10, No. 4, pp. 26-39. ISSN 2345-0282
5. Gyáfašová, O., Krivý, V. (2013): Vzorové voličského správania. In: Krivý, V. ed.: *Ako sa mení slovenská spoločnosť*. Sociologický ústav SAV, Bratislava, s. 257-342
6. Koraus, A., Kurilovská, L., Šišulák, S. (2022). Increasing the competencies and awareness of public administration workers in the context of current hybrid threats. *RELIK* 2022. ISBN 978-80-245-2466-5. Available from: <https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf>
7. Linek, L. (2015): Účast ve sněmovních volbách v roce 2013: zdroje, mobilizace a motivace. *European Electoral Studies*, 10, č. 2, s. 76-9.

8. Lisoň, M., Fidler, Ľ. (2022) Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb. In Policajná teória a prax. ISSN 1335-1370, 2022, r. XXX, č. 2. 2022, s. 38-53
9. Potuček, M. a kol.: Veřejná politika. Praha: Slon 2005, s. 61 – 84. ISBN 80-86429-50-4
10. Putnam, R- D. 1993. The Prosperous Community; Social Capital and Public Life. In: The American Prospect, Vol. 4, No 13 (<http://www.prospect.org/print/V4/13/putnam-r.html>)
11. Nekola, M. – Novotný, V. 2010. Strategické řízení a teoretické přístupy k procesu tvorby veřejných politik. In: OCHRANA, F. a kol.: Strategické řízení ve veřejné správě a přístupy k tvorbě politiky. Praha: Matfyzpress, 2010, s. 59 – 86. ISBN: 978-80-7378-130-9.
12. Palúš, I. – Somorová, Ľ. 2014. Štátne právo Slovenskej republiky. 4. vyd. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach. ISBN 978-88-08152-129-4
13. Plutzer, E. (2002): Becoming a habitual voter: Inertia, Resources, and Growth in Young Adulthood. The American Political Science Review. 96. č.1, s. 41 – 56
14. Zetková, P.:Straniční funkcionáři versus parlamentní reprezentace.Duvergerův pohled a modifikace pro dnešek. In: Novák, M. (ed.): Strany, volby a demokracie: Od Duvergera k Sartorimu a dále. Praha: Sociologické nakladatelství 2016, s.14 - 40. ISBN 978-80-7419-233-3
15. Charta základných ľudských práv Európskej únie (2016/C 202/02)
16. Zákona č. 180/2014 Z.z. o podmienkach výkonu volebného práva a o zmene a doplnení niektorých zákonov

ŠÍŘENÍ DEZINFORMACÍ V KONTEXTU HYBRIDNÍHO PŮSOBNÍ

Mgr. Lenka Jakubcová, Ph.D.; Mgr. Josef Dubský

Policejní akademie České republiky v Praze, Fakulta bezpečnostního managementu, Lhotecká 559/7, 143 01 Praha 4, Česká republika, jakubcova@polac.cz; dubsky@polac.cz

Abstrakt: Cílem příspěvku je zasadit problematiku masivních dezinformačních kampaní, které se v posledních letech odrazily do znejistění společnosti jak v České republice, tak i na Slovensku, do kontextu hybridního působení (hybridních kampaní či vlivového působení) některých států, které zneužívají informační otevřenosti demokratických společností a principů, na nichž jsou postaveny. Pozornost je věnována přiblížení projektu, kterému se věnuje řešitelský tým Policejní akademie České republiky v Praze, a vybraným výsledkům z realizovaného reprezentativního výzkumu veřejného mínění, které mohou směřovat k doporučením pro veřejnou správu v otázkách posílení odolnosti občanské společnosti vůči dezinformačnímu působení jak v České republice, tak i na Slovensku.

Klíčové slová: dezinformace, dezinformační kampaně, hybridní působení, Ruská federace, výzkum veřejného mínění, strategická komunikace.

ÚVOD

Dezinformace představují jednu ze zásadních bezpečnostních hrozeb, kterým západní demokracie v současné době čelí, a na jejich potenciál ohrožit chod demokratických institucí, procesy právního státu a vnitřní bezpečnost upozorňují dlouhodobě bezpečnostní složky i mezinárodní organizace. Šíření nepravdivých informací s úmyslem klamat druhého sice v principu nepředstavuje zcela nové téma (metody klamání nepřítele pomocí šíření nepravdivých informací a psychologického působení jsou fragmentárně zaznamenány již ve starověkém válečnictví), ale vzhledem k jeho aktuálnímu záběru, zacílení, metodám působení, možností přenosu i rozsahu se jedná o zcela novou zkušenost v globálním měřítku.

Za dezinformace označujeme „*záměrně nepravdivé či manipulativní informace s cílem ovlivnit rozhodování nebo názory těch, kteří je přijímají*“ [1]. Účelem šíření dezinformací je buď způsobit škodu, nebo získat nějaký politický, osobní či finanční prospěch.

Dezinformace v podstatě představují kombinaci tzv. misinformace a malinformace [2].

Misinformace jsou „*nepravdivé nebo zavádějící informace, které nejsou šířeny ani systematicky, ani úmyslně*“ (s úmyslem někoho oklamat) [1]. Ačkoliv se jedná o neutrální jev, mohou misinformace v případech, kdy jsou šířeny ve velkém rozsahu a bez náležité opravy, mít stejné důsledky, jako dezinformace.

Malinformace je naproti tomu „*pravdivá informace šířená s cílem někoho poškodit*“ [3].

Vliv dezinformací na společnost může být značně destruktivní v mnoha rovinách. Cíleným ovlivněním konkrétních událostí (např. voleb či výsledků referenda) počínaje, až po dlouhodobou systematickou kontaminaci veřejného informačního prostoru. Ta může mít za následek relativizaci a zhoršování úrovně veřejné diskuse, provokovat reakce názorově odlišných stran znemožňující konstruktivní dialog, cíleným rozdmýháváním citlivých témat vést k polarizaci politické debaty nebo i společnosti jako takové a k radikalizaci některých skupin. Důsledkem je ztráta důvěry

veřejnosti v demokratické procesy, instituce a autority. Obzvláště nebezpečné pak může být takovéto jednání při „krizových situacích“, jako jsou zdravotní krize, živelní pohromy, teroristické útoky, závažné narušení vnitřní bezpečnosti a veřejného pořádku či vojenské konflikty (jak nakonec ukazují i výsledky šetření mapující v České republice důvěru občanů ve vládní opatření v době koronavirové krize). Vypuštění klamných informací či zarámování informací do „správného“ kontextu, který vyhovuje šířiteli dezinformace, umožňuje „zamlžit“ informační prostor, vyvolat dezorientaci, apatii a negativní emoce, a výrazně tak ztížit oficiálním institucím proces zvládání následků krizové situace. Cílená dezinformační kampaň, případně i spontánně druhotně ve větším rozsahu sdílené dezinformace, mohou dokonce krizovou situaci vyvolat [4].

1. ŠÍŘENÍ DEZINFORMACÍ V KONTEXTU HYBRIDNÍHO PŮSOBNÍ

K masivnímu šíření dezinformací přispívá značný rozvoj komunikačních a informačních technologií. Šířitelé dezinformací (organizace, jednotlivci, ale především státy jako součást hybridních kampaní a vlivového působení) zneužívají informační otevřenosti demokratických společností a principů, na nichž jsou postaveny, stejně jako „hluchých míst“ současného informačního prostoru. Cílené, systematické a záměrné vypouštění klamných či manipulativních informací je v rostoucím měřítku provozováno organizovanými subjekty, tzv. trollími farmami. Šířitelé dezinformací využívají falešných identit, počítačových programů, které uměle navyšují rozsah šíření dezinformací (tzv. botů), manipulace obsahu za pomoci „deepfakes“ aj. sofistikovaných nástrojů, na které se státy musí naučit pružně a efektivně reagovat [4].

Hybridní působení je strategie, kterou používají státy (či nestátní aktéři) k dosažení svých politických cílů. Z Národní strategie pro čelění hybridnímu působení [5] (a odborné literatury) [6], [7], [8] vyplývá, že ke klíčovým znakům hybridního působení patří:

- snaha o rozostření hranic mezi mírem, krizí a konfliktem,
- skrytost, nejednoznačnost,
- obtížná přičitatelnost (atribuce),
- snaha využívat existujících zranitelností a společenských rozporů a dále je prohlubovat.

Cílem hybridního působení může být:

- zpomalení či paralyzování politického rozhodovacího procesu (včetně rozhodování v oblasti obrany a bezpečnosti),
- oslabování důvěry občanů v ústavněprávní uspořádání a demokratické instituce a mechanismy,
- narušování ekonomických procesů,
- získání vlivu v klíkových hospodářských sektorech a strategických podnicích,
- manipulace či ovládnutí informačního prostředí,
- oslabení či ovlivnění fungování kritické infrastruktury aj.

K metodám a nástrojům hybridního působení pak patří zejména:

- kriminální a teroristické akty,
- informační a psychologické operace,
- škodlivé aktivity v kybernetickém prostoru,
- otevřené či skryté ovlivňování politických struktur (včetně politických stran) a politického rozhodovacího procesu, soudů, policie, ozbrojených sil, sdělovacích prostředků a

veřejného mínění, usilující o destabilizaci či štěpení společnosti a podlomení důvěry občanů v ideově-hodnotové zakotvení země a ústavněprávní uspořádání státu, zahrnující taktéž ústavní instituce a demokratický proces,

- (může být kombinováno s otevřeným vojenským konfliktem).

Co je potřeba zdůraznit je skutečnost, že hybridní působení cílí na zranitelnosti protivníka, a právě od toho by se měla odvíjet i obranná strategie, která přináší do popředí fenomén odolnosti (resilience).

2. SITUACE V ČESKÉ REPUBLICE

Česká bezpečnostní komunita se shoduje na tom, že masivní dezinformační kampaně, spojené v mnoha případech (ať už přímo či nepřímo) zejména se zájmy Ruské federace a Čínské lidové republiky, v České republice již mnoho let intenzivně probíhají. Kromě Auditů národní bezpečnosti na ně již několik let upozorňují výroční zprávy Bezpečnostní informační služby i Vojenského zpravodajství. Označení Ruska a Číny jako zdrojů výrazného bezpečnostního ohrožení České republiky v této oblasti potvrdilo také výzkumné šetření provedené na Policejní akademii České republiky v Praze na přelomu let 2019/2020, jehož respondenty byla elitní skupina analytiků Bezpečnostní informační služby [9].

V kontextu minulých i probíhajících událostí (ruská anexe Krymu 2014, výbuch muničního skladu ve Vrběticích 2014, pandemie Covid-19, válka na Ukrajině, energetická a ekonomická krize) si v ČR všímáme především informačního působení Ruské federace. Informační působení v tomto kontextu označuje použití informací jako nástroje k dosažení politických nebo strategických cílů, často prostřednictvím šíření propagandy, dezinformací nebo jiných forem informační války [10]. Koncepce informační konfrontace tedy v sobě nese kybernetické operace vedle či v propojení s disciplínami, jako jsou psychologické operace, strategická komunikace nebo činnost zpravodajských služeb, tedy různé ofenzivní i defenzivní praktiky zaměřené na dezinformace, klamání, sabotáž, destabilizaci a špionáž, vyplývající z předpokladů a priorit zahraniční politiky Ruské federace (tzv. „aktivní opatření“). Dohromady tento koncept tvoří celek systémů, metod a úkolů s cílem ovlivnit vnímání a chování nepřítele, obyvatelstva a mezinárodních společenství na všech úrovních [11].

Lze konstatovat, že Česká republika je pro Rusko geopoliticky naprosto klíčový stát z hlediska dezinformačního působení, což naznačují i průzkumy veřejného mínění na Slovensku nebo situace v Maďarsku, ze kterých lze naprosto čitelně vyčíst stopu a dosah ruské propagandy a dezinformačních kampaní. Na to by měla Česká republika umět reagovat, neboť česká společnost, zmítaná dlouhodobě neřešenými sociálními problémy vystupňovanými pandemií onemocnění Covid-19, válkou na Ukrajině, energetickou a ekonomickou krizí, je bohužel snadným terčem rozkladných a polarizujících dezinformačních kampaní a dalších hybridních aktivit zejména ze strany Ruské federace.

Odolnost české společnosti vůči dezinformačnímu působení je poměrně nízká, a to i ve srovnání s jinými evropskými státy (jako např. pobaltské státy, Francie, Velká Británie či Finsko), které na rozdíl od České republiky mají již vybudovány mechanismy obrany vůči působení dezinformací, či na jejich zlepšování pracují. V zahraničí je běžné, že státu s komunikací a bojem s dezinformacemi pomáhají tisíce lidí. Např. v Německu funguje Vládní komunikační služba s více

než 5000 lidmi. Tvoří ji týmy reagující na jednotlivá aktuální témata – od koronaviru až po válku na Ukrajině. Nejodolnější vůči cizí propagandě je podle expertů Finsko, které se dle průzkumu Institutu Open Society v roce 2022 umístilo v čele z 41 zemí. Velkou roli v tom hraje i mediální gramotnost, která se ve Finsku vyučuje už od předškolního věku. Ke vzdělávacímu systému, který patří k nejlepším na světě, se přidává i důvěra ve vládu a média, což tvoří jeden z klíčových prvků odolné společnosti. Politikům věří až 70% Finů, na rozdíl od České republiky, kde se důvěra vládě pohybuje maximálně kolem 30% a má klesající tendenci.

2.1 Aktivity Policejní akademie České republiky v Praze

Tytéž signály zaznamenáváme ze (zatím) průběžných výsledků výzkumu veřejného mínění, který realizovala Policejní akademie (ve spolupráci s agenturou IPSOS) v tomto roce v rámci projektu „Odolnost příslušníků Policie České republiky vůči dezinformačním vlivům a možnosti posilování jejich rezistence prostřednictvím vzdělávání“ (DEZINFOPOL), který byl podpořen Ministerstvem vnitra v rámci 1. veřejné soutěže programu OPSEC (bezpečnostní výzkum MV ČR). Cílem tohoto projektu je zvýšit odolnost příslušníků Policie ČR vůči dezinformačním vlivům, a to zejména cestou cíleného vzdělávání. Příslušníci Policie ČR jsou totiž specifickou skupinou, protože se nacházejí v duálním postavení „příjemců“ dezinformačních obsahů (stejně jako celá společnost), ale zároveň jsou na ně optikou profesního statusu kladeny zvláštní nároky a požadavky, a je tudíž celospolečensky žádoucí věnovat zvláštní pozornost kontinuálnímu sledování jejich odolnosti vůči dezinformačnímu působení a nalézání nových opatření k jejímu navyšování. Příslušníci Policie ČR se zároveň v pozici orgánu činného v trestním řízení podílejí na odhalování, prověřování a řešení trestné činnosti související s šířením dezinformací nebo chováním pod vlivem dezinformací, které vykazuje znaky skutkové podstaty některého ze stávajících trestných činů, a musí tudíž disponovat potřebnými znalostmi, dovednostmi, schopnostmi a kompetencemi, které jim umožní v maximální možné míře dezinformační obsahy rozpoznávat, ověřovat jejich zdroje, a připisovat autorství konkrétním osobám, v jejichž případě by v úvahu přicházely trestněprávní konsekvence [4].

V prvním roce projektu (2023) proběhl mimo jiné rozsáhlý reprezentativní výzkum veřejného mínění směřující k nalezení indikátorů odolnosti vůči dezinformačnímu působení. V roce 2024 bude následovat výzkum zaměřený do řad příslušníků Policie ČR, ve kterém bude zkoumána odolnost příslušníků Policie ČR vůči dezinformačnímu působení a možnosti posilování jejich resilience, a k výsledkům projektu budou patřit např. edukační kurzy a materiály, implementace problematiky do strategických dokumentů Policie ČR či metodická pomůcka ke zvyšování odolnosti příslušníků Policie ČR vůči dezinformačnímu působení a navýšení kompetencí v oblasti řešení trestných činů souvisejících s šířením dezinformací nebo páchaných pod jejich vlivem.

2.1.1 Výzkum veřejného mínění: „Odolnost české populace vůči dezinformačnímu působení“ (PA ČR ve spolupráci s IPSOS, 2023)

Cílem reprezentativního výzkumu veřejného mínění bylo zjistit míru odolnosti české veřejnosti vůči dezinformacím. Výzkum proběhl v srpnu 2023 na reprezentativním vzorku české populace ve věku od 15–65 let, na výběrovém souboru 1409 respondentů. Sběr dat proběhl metodou CAWI (prostřednictvím internetových adres dotázaných). Ve výzkumu jsme se zaměřili, kromě konspiračních a dezinformačních narativů, na další proměnné, u kterých předpokládáme, že by mohly souviset s odolností vůči dezinformačnímu působení, jako jsou:

- důvěra v instituce a představitele státu,

- politické postoje,
- mediální a informační gramotnost (konzumace médií a dalších informačních zdrojů),
- zkušenost s dezinformacemi,
- konspirační mentalita,
- anomie,
- psychická stabilita / labilita,
- kognitivní reflexe aj.

Výzkum je nyní ve fázi zpracování, vyhodnocování a interpretace dat. Již nyní lze ale demonstrovat určité trendy vyplývající z jeho výsledků. Vybrané poznatky uvádíme níže:

- Češi si uvědomují, že dezinformace jsou problém. 18 % Čechů je dokonce považuje za naprosto zásadní bezpečnostní hrozbu, významnější než například terorismus.
- Přestože se 42 % občanů ČR považuje za vysoce odolné vůči dezinformačnímu působení, je patrné, že česká veřejnost vítá, pokud stát dopady dezinformací reguluje, a to i za cenu „omezení svobody slova“ - téměř 2/3 české populace sdílí názor, že je ze strany státu správné omezit či znemožnit působení médií, která šíří dezinformace.
- Boji proti dezinformacím by se podle české veřejnosti měly věnovat všechny instituce, orgány i samotní občané, především však Vláda ČR, a dále také sdělovací prostředky a sociální média – což opět koresponduje s názorem, že by politika v oblasti boje s dezinformacemi měla mít jednoznačně stanovenou gesci a strategii zahrnující proaktivní a reaktivní kroky a koordinovaný postup jednotlivých aktérů k jejich dosažení.
- Dlouhodobě klesající trend zaznamenáváme v otázkách důvěry veřejnosti ve vládu a státní instituce (s výjimkou prezidenta republiky).
- Zásadní rozdíly jsou v ČR mezi příznivci vládních a opozičních stran, a to i v podléhání dezinformacím – příznivci opozice jim důvěřují častěji.
- Důvěra v instituce úzce souvisí s podléháním dezinformacím – a to prakticky u všech typů dezinformací, které jsme zkoumali, a také u všech institucí. Například – mezi těmi, kdo důvěřují policii, 20 % zcela věří tvrzení *„Ukrajínští uprchlíci zvyšují kriminalitu, což nám vedení státu tají.“* Mezi respondenty, kteří policii nedůvěřují, to je ale už 43 % dotázaných, kteří tuto informaci považují za pravdivou.

Přitom právě důvěra ve stát, instituce nebo média je klíčovým parametrem, který ovlivňuje náchylnost člověka věřit dezinformacím a konspiračním teoriím. Pokud člověk věří, že společenský systém funguje, a že funguje také v jeho prospěch, a že on sám je schopný se v takovém systému orientovat, pak tento jedinec podle výsledků výzkumů [12] pravděpodobněji odolá dezinformačnímu působení. Výzkumy ukazují, že společenská důvěra, důvěra ve stát a jeho fungování, je jednoznačným prediktorem, který přehluší třeba i vzdělání nebo socioekonomickou situaci [13], což potvrzují i průběžné výsledky našeho výzkumu.

Zároveň se zde ukazuje, že důvěra v dezinformační narativy také souvisí s obecnějším vztahem jedince ke společnosti a jejím normám – tedy s mírou anomie. Ti, kdo jsou silně anomičtí (41 % občanů ČR), tj. nevěří politikům, společenským normám ani ostatním lidem, podstatně více dezinformace přijímají. Například 22 % silných anomičtů věří, že Vláda ČR chtěla krizi kolem nemoci Covid-19 využít k trvalému omezení demokratických práv a svobod. Oproti tomu ti, kdo na škále anomie skórují nízko, věří tomuto výroku jen ve 4 % případů.

Z výsledků zároveň vyplývá, že odolnost vůči dezinformačním narativům souvisí i s důvěrou v média, zejména ta „tradiční“ a/nebo „veřejnoprávní“ (pro příklad – mezi těmi, kdo důvěřují informacím České televize (ČT), se pouze 2 % domnívají, že vládou zamýšlená legislativa na ochranu proti dezinformacím má sloužit jako nástroj cenzury. Ti, kdo ČT nedůvěřují, si to ale myslí v 52 % případů), a také s „informační gramotností“ celkově, tedy kompetencí, která odráží jak znalosti respondenta o médiích, tak jeho schopnost poznat „podezřelé“ informace a dohledat si k nim další zdroje.

3. POSILOVÁNÍ ODOLNOSTI VŮČI DEZINFORMAČNÍMU PŮSOBENÍ – NÁVRHY A DOPORUČENÍ

Přestože některé aktivity v oblasti posilování odolnosti české společnosti vůči dezinformacím probíhají, vidíme jako klíčové:

- určit jednoznačnou gesci za řízení politiky v oblasti dezinformací a nastavit systémová opatření a procesy, které by umožňovaly řízení a plánování dlouhodobých strategických kroků, sjednocení přístupů napříč resorty a koordinaci jednotlivých složek státu,
- vyčlenit dostatečné kapacity na monitoring, sledování klíčových trendů a včasnou identifikaci hrozeb v této oblasti tak, aby stát dokázal účinně a rychle reagovat na změny v dezinformačním ekosystému a na konkrétní dezinformační kampaně,
- obranu proti dezinformačnímu působení je potřeba zakotvit v národních bezpečnostních dokumentech,
- výrazně posílit strategickou komunikaci státu,
- systematicky zvyšovat mediální gramotnost a podporovat kritické myšlení,
- podporovat etiku v mediálním prostředí,
- dbát na transparentnost státní inzerce (demonetizace dezinformační scény).

Boj s dezinformacemi leží vedle státu i na dalších institucích, profesních skupinách, neziskových organizacích, fact-checkerech, novinářích i digitálních platformách, avšak stát musí jasně deklarovat svou vizi, svůj postoj vůči dezinformacím dovnitř státu i navenek, vytvářet podmínky k účinnému boji proti dezinformačním kampaním a převzít odpovědnost za strategickou komunikaci vůči občanské společnosti.

Zároveň je třeba konstatovat, že pro Českou republiku, jako relativně malý stát, jsou možnosti, jak například ovlivnit regulaci sociálních sítí a platform (jejichž dosah využívají zahraniční i domácí aktéři dezinformační scény), jejich algoritmů a pravidel fungování, velmi omezené. Zejména z tohoto úhlu pohledu je tedy nutné, aby Česká republika podporovala aktivity Evropské unie v této oblasti, jejíž regulatorní iniciativy mají mnohem větší dosah a dopad.

Uvedená opatření a doporučení je nutné vnímat jako vzájemně se podporující systém kroků směřující k dosažení vytýčeného cíle. Vzhledem k zacílení konference a sborníku se dále zaměříme na jedno z uvedených doporučení, a to na strategickou komunikaci státu (StratCom) s cílem zúročit poznatky z výzkumů veřejného mínění ukazující, že důvěra ve stát a jeho představitele a instituce je jedním z klíčových prvků odolnosti občanské společnosti vůči podvrtným vnějším vlivům.

Dokument Analýza připravenosti ČR čelit závažné dezinformační vlně [1] uvádí, že: StratCom

- představuje soubor koordinovaných a synchronizovaných komunikačních aktivit státních/veřejných institucí s definovanými cílovými skupinami občanů nebo celou veřejností, jejichž cílem je informování v souladu se stanovenými národními zájmy a vládními prioritami,
- předpokládá plánování a kombinování nejrozličnějších forem přístupů ke komunikaci, prostřednictvím kterých stát systematicky buduje a rozvíjí různá sdělení v komunikovaných tématech, stejně jako veřejnou podporu vůči nim,
- důležitost StratCom v boji proti dezinformacím neleží pouze v reaktivním (ad-hoc) vyvracení nepravdivých či zavádějících sdělení (přestože i tato komunikační technika má v rámci strategické komunikace v určitých situacích své místo), ale spočívá především v dlouhodobém budování důvěryhodných komunikačních kanálů, aktivní a efektivní komunikaci prioritních oblastí politiky státu,
- představuje klíčový nástroj v boji proti dezinformacím, jelikož pomáhá mírnit jejich akutní dopad a zároveň (dlouhodobě) posiluje společenskou odolnost vůči nim.

Je tedy zjevné, že StratCom by měla vycházet z předem definované strategie státu a jeho cílů v oblasti čelení dezinformačnímu působení, a měla by představovat poměrně zásadní a nikoli pouze doplňkový aspekt. Měla by být:

- proaktivní (nikoli pouze reagující na již vzniklou situaci),
- plánovaná a promyšlená,
- hodnotově zakotvená,
- důvěryhodná,
- otevřená,
- kontinuální (státní musí komunikovat svou činnost nepřetržitě a proaktivně hledat příležitosti, které může využít pro podporu svých cílů),
- flexibilní (musí reflektovat komunikační trendy, využívat různé komunikační kanály s ohledem na jednotlivé cílové skupiny apod.),
- depolitizovaná.

StratCom by měla tvořit základní kámen vztahu mezi státem a občanem – stát a potažmo státní instituce by měly více reflektovat svou pozici správce věcí veřejných a vnímat komunikaci s občany jako možnost, jak upevnit důvěru občanů ve stát, protože právě budování důvěry ve stát, jeho oficiální představitele a instituce by mělo být vnímáno jako klíčová obranná hráz proti hybridním hrozbám a dezinformacím.

ZÁVĚR

Je zjevné, že zvyšovat odolnost společnosti vůči dezinformačnímu působení je, spolu s dalšími kroky (včetně např. demonetizace dezinformační scény), nezbytné k zachování hodnot, na kterých demokratické společnosti stojí. Navíc se nacházíme v době bezprecedentního rozmachu nových technologií, včetně využívání umělé inteligence, která je nyní jedním z nejdiskutovanějších témat ve spojitosti s bezpečností. Právě díky těmto technologiím je šíření a vytváření dezinformací, a to včetně jejich audiovizuálních obsahů, mnohem jednodušší a jejich dosah větší. Dezinformace a

jejich masivní šíření dokáže velmi účinně rozleptávat vzájemnou důvěru lidí a soudržnost společnosti. Boj s dezinformacemi je tudíž jednou z největších výzev, před kterými Česko, Slovensko, i celý demokratický svět v 21. století stojí.

Poděkování

Vznik tohoto příspěvku byl finančně podpořen projektem MV ČR č. VK01020187.

Tento příspěvek je výsledkem projektu Odolnost příslušníků Policie České republiky vůči dezinformačním vlivům a možnosti posilování jejich rezistence prostřednictvím vzdělávání VK01020187, zkráceně DEZINFOPOL, který byl podpořen Ministerstvem vnitra ČR z Programu Otevřené výzvy v bezpečnostním výzkumu 2023-2029, zkráceně OPSEC.

Zdroje

1. Analýza připravenosti České republiky čelit závažné dezinformační vlně. Praha: MV ČR ve spolupráci s MO ČR a MS ČR, 2022. [online]. 15. 2. 2023 [cit. 2023-07-30]. Dostupné z: <https://www.mvcr.cz/chh/clanek/analyza-pripravenosti-ceske-republiky-celit-zavazne-dezinformacni-vlne.aspx>
2. HAVLÍK, Martin. Inovativní pohled na metodický proces čelení dezinformacím. *Vojenské rozhledy*. 2022, vol. 31, č. 4. [online]. 2021 [cit. 2023-06-30]. Dostupné z: https://www.vojenskerozhledy.cz/kategorie/proces-celeni-dezinformacim#_ftn32
3. GREGOR, Miloš a Petra VEJVODOVÁ. Nejlepší kniha o dezinformacích a manipulacích!!! Brno: Albatros Media, 2018. ISBN 8026425537.
4. JAKUBCOVÁ, Lenka, HOLUBOVÁ, Kristýna a Karel ŠILINGER. Duální postavení příslušníků Policie ČR ve vztahu k dezinformačnímu působení. *Bezpečnostní teorie a praxe*. 2023, č. 1, s. 3 – 32. ISSN 1801-8211.
5. Národní strategie pro čelení hybridnímu působení. Praha: Ministerstvo obrany, 2021. [online]. 2021 [cit. 2023-06-30]. Dostupné z: https://mocr.army.cz/images/id_40001_50000/46088/N__rodn__strategie_pro__elen__hybridn__mu_p__soben__.pdf
6. DESHPANDE, Vikrant. Hybrid Warfare: The Changing Character of Conflict. Institute for Defence Studies & Analyses. Raj Publication, 2018, s. 16-18. ISBN 978-9386618351.
7. KURFÜRST Jaroslav. Momenty z historie válčení a přívlastek „hybridní“: nic nového pod sluncem. In: KURFÜRST Jaroslav a Jan PAĎOUREK. *Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů*. Praha: Academia, 2021, s. 27 - 39. ISBN 978-80-200-3237-9.
8. BAHENSKÝ, Vojtěch. Kritika konceptu hybridní války. In: KURFÜRST Jaroslav a Jan PAĎOUREK. *Za zrcadlem: Hybridní válka jako staronový fenomén mezinárodních vztahů*. Praha: Academia, 2021, s. 55 - 70. ISBN 978-80-200-3237-9.
9. PAĎOUREK, Jan. Rozdílné pohledy českých expertů a politiků na klíčové bezpečnostní hrozby: Jedna středoevropská lekce. *New Direction*. [online]. [cit. 2022-07-06]. Dostupné z: <https://newdirection.online/2018-publications-pdf/NDreportCZ-RozdilnePohledy.pdf>
10. GILES, Keir a R. Evan ELLIS. *The Rise of Russia – Turning Point for Russian Foreign Policy & The Change of Strategy*: Strategic Studies Institute. Madison & Adams Press, 2017, s. 15-34. ISBN 978-80-268-7962-6
11. SELHORST, Tony. Russia's Perception Warfare. *Militaire Spectator* [online]. 22. 4. 2016 [cit. 2023-06-20]. Dostupné z: <https://militairespectator.nl/artikelen/russias-perception-warfare>

12. Výzkumný projekt Českého Rozhlasu, Národního institutu pro výzkum socioekonomických dopadů nemocí a systémových rizik – SYRI a Sociologického ústavu AV ČR. Společnost nedůvěry: konspirace a dezinformace v české společnosti. [online]. 12.6.2023 [cit. 2023-09-08]. Dostupné z: [https:// www.irozhlas.cz/zpravy-domov/spolecnost-neduvetry-konspirace-dezinformace-stat-politika-duvera-serial_2306170600_pik](https://www.irozhlas.cz/zpravy-domov/spolecnost-neduvetry-konspirace-dezinformace-stat-politika-duvera-serial_2306170600_pik)
13. Konspiritualita. Co ukazuje nový průzkum víry v dezinformace. Seznam Zprávy. [online]. 15.6.2023. [cit. 2023-09-08]. Dostupné z: [https:// www.seznamzpravy.cz/clanek/audio-podcast-5-59-neco-na-tom-je-kdo-a-jak-moc-v-cesku-veri-konspiracim-a-dezinformacim-232520](https://www.seznamzpravy.cz/clanek/audio-podcast-5-59-neco-na-tom-je-kdo-a-jak-moc-v-cesku-veri-konspiracim-a-dezinformacim-232520)

HYBRIDNÉ HROZBY VO FINANČNOM SYSTÉME A MOŽNOSTI NOVÝCH TECHNOLOGIÍ V BOJI PROTI TÝMTO HROZBÁM

Dr. habil. Ing. Eva Jančíková, PhD., Ing. Stanislava Veselovská, PhD.

Ekonomická univerzita v Bratislave, Fakulta medzinárodných vzťahov; Dolnozemska cesta 1, 852 35 Bratislava; email eva.jancikova@euba.sk, Paneurópska vysoká škola v Bratislave, Fakulta ekonómie a podnikania; Tematínska 10, 851 05 Bratislava; email stanislava.veselovska@paneurouni.com

Abstrakt: Rozvoj nových technológií v posledných rokoch zásadným spôsobom ovplyvnil bezpečnostnú situáciu vo svete. K sektorom, ktoré boli najviac ovplyvnené technologickými zmenami, môžeme zaradiť finančné systémy, hlavne bankovníctvo. Bankový sektor prispôsobuje ponuku svojich produktov novým inovatívnym technológiám, ktoré sú na jednej strane vystavené hybridným hrozbám a na strane druhej práve nové technológie môžu pomáhať v boji proti týmto hrozbám. Cieľom tohto príspevku je definovať vplyv nových produktov a technológií na postupy bánk v boji proti hybridným hrozbám s využitím skúsenosti z boja proti praniu špinavých peňazí a financovaniu terorizmu a porušovaniu sankcií.

Kľúčové slová: hybridné hrozby, pranie špinavých peňazí, financovanie terorizmu, dodržanie sankcií, nové technológie.

ÚVOD

Rozvoj nových technológií v posledných rokoch zásadným spôsobom ovplyvnil bezpečnostnú situáciu vo svete. Čoraz častejšie sa hovorí o hybridných hrozbách, ktoré sa definujú ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie (Národný bezpečnostný úrad SR, 2022). Aj vojnový konflikt na Ukrajine ukazuje ako sa popri priamych vojenských operáciách využívajú aj mnohé nevojenské prostriedky, z ktorých môžeme spomenúť hlavne nepriateľskú propagandu, podporu extrémizmu, využívanie národnostných alebo náboženských komunít nespokojných so svojim postavením v spoločnosti, podporu kriminálnych aktivít, ale hlavne útoky na kritickú infraštruktúru.

EÚ musí prijať celý rad aktívnych a pasívnych opatrení na prevenciu, identifikáciu a pôsobenie proti nepriateľským aktivitám, spolu so vzdelávaním obyvateľstva a autorít a vytváraním a zvyšovaním ich odolnosti. Círdeia (2017) poukazuje na rast neistoty vplyvom globalizácie, čo je spôsobené úzkym prepojením a vzájomnou závislosťou štátov, regiónov a sietí a využitie takejto zraniteľnosti sa stáva cieľom aktérov destabilizovať systém alebo jeho časť.

Budovaním ľudských zdrojov, technických kapacít a implementáciou vzdelávacích a komunikačných aktivít sa môže výrazne zvýšiť odolnosť voči rôznym formám hybridných hrozieb v príslušných doménach. Systémové slabiny pri hybridných aktivitách vyplní audit zraniteľnosti a následné návrhy na zmenu a doplnenie regulačných rámcov. Okrem toho sa odolnosť Slovenska voči hybridným hrozbám zvýši implementáciou komplexného súboru opatrení, ktoré zahŕňajú optimalizáciu procesov v subjektoch verejnej správy, zvyšovanie vzdelávacích kapacít, získavanie nových kompetencií a zručností verejnými orgánmi prostredníctvom systému profesionálnych školení. (Korauš, 2022)

Skúsenosti z boja proti trestnej činnosti ukazujú akú dôležitú úlohu zohrávajú finančné inštitúcie. Nie je tomu inak ani pri hybridných hrozbách. Na jednej strane finančný systém môže byť využívaný resp. zneužívaný pri financovaní týchto aktivít a na strane druhej môže byť práve finančný systém cieľom hybridných hrozieb, keďže v každej spoločnosti je zdravý finančný systém základom fungovania ekonomiky. V posledných rokoch aj vplyvom ekonomického a politického vývoja sa začali diskutovať otázky hybridných hrozieb v kontexte finančných systémov hlavne z pohľadu ich zraniteľnosti. Politický a ekonomický vývoj vplyvom globalizácie priniesol nové výzvy, na ktoré je potrebné reagovať na národnej a medzinárodnej úrovni.

V kontexte s komplexnými bezpečnostnými výzvami a bojom proti hybridným hrozbám vo finančnom systéme je frekventovanou kategóriou pranie špinavých peňazí a financovanie terorizmu. V tomto kontexte vnímame pranie špinavých peňazí ako proces, ktorým sa nelegálne získané finančné prostriedky transformujú na zdanlivo legálne peniaze. Pri financovaní terorizmu môže ísť o prostriedky získané nelegálnou činnosťou, ktoré prešli procesom prania špinavých peňazí, často však dochádza aj k použitiu finančných prostriedkov, ktoré pochádzajú z legálne nadobudnutých zdrojov, ale ich využitie je nelegálne – na financovanie teroristických akcií. V oboch prípadoch ide o to, že sa na odhalenie trestnej činnosti používa sledovanie finančných tokov. Boj proti praniu špinavých peňazí a financovaniu terorizmu je v súčasnosti upravený na medzinárodnej aj národnej úrovni, čo by sa mohlo veľmi efektívne využiť v ochrane pred hybridnými hrozbami.

Okrem toho je dôležité spojiť všetky dostupné možnosti na to, aby sme zvládli súčasnú “exploziu” zavádzania a využívania nových informačných technológií, ktorý poskytuje obrovský priestor na zneprehľadnenie a zneužívanie tokov finančných prostriedkov a uplatňovaním informačných technológií ich sledovanie a skúmanie náročnejším. Financovanie teroristických aktivít môže teda zahŕňať aj financovanie hybridných hrozieb, ktoré môže byť nekonvenčné a zahŕňať napríklad kybernetické útoky, kradnutie identít, použitie kryptomien a ďalšie. Je nevyhnutné, aby v boji proti financovaniu terorizmu a v boji proti hybridným hrozbám bola úzka a profesionálna spolupráca medzi finančnými inštitúciami, vládami a medzinárodnými organizáciami na monitorovaní podozrivých finančných transakcií a identifikovaní nezvyčajných vzorov správania sa.

Spolupráca na domácej ale aj medzinárodnej úrovni je dôležitá v oblasti regulácie a dohľadu, kde je potrebné, aby regulačné orgány prijali striktné opatrenia na monitorovanie finančných transakcií, identifikáciu podozrivých obchodných operácií a vzájomné zdieľanie týchto informácií. Na predchádzanie hybridným hrozbám vo finančnom systéme môžu prispieť nové informačné technológie, analýza veľkých dát a využitie umelej inteligencie. Významným prvkom prevencie je aj zvyšovanie finančného povedomia a vzdelávanie vo finančných inštitúciách, odbornej ale aj laickej verejnosti. Kombinácia legislatívnych opatrení, technologických riešení a globálnej spolupráce na zabezpečenie stability a integrity finančných trhov je v boji proti hybridným hrozbám vo finančnom systéme kľúčová.

Pranie špinavých peňazí a financovanie terorizmu môžu mať potenciálne ničujúce sociálne, ekonomické a bezpečnostné dôsledky. Finančné inštitúcie zohrávajú kľúčovú úlohu pri odhaľovaní legalizácie príjmov z trestnej činnosti, ktoré okrem boja proti organizovanému zločinu a rôznym kriminálnym aktivitám, pomáha aj v boji proti korupcii a v posledných rokoch aj pri uplatňovaní sankcií. Globalizácia a technologický pokrok, ktoré v posledných desaťročiach formovali svet,

ukázali, že kontrola stoviek miliárd medzinárodných finančných transakcií, ktoré sa uskutočňujú ročne na celom svete, je veľmi náročná priam až nemožná. Novou výzvou v tejto oblasti sú aj nové technologické možnosti, ktoré poskytujú digitálne meny. (Baath, 2016).

Ako reakciu na túto situáciu zverejnila Finančná akčná skupina (FATF) v októbri 2006 správu o nových typoch platobných metód, ktoré sa používajú na legítimne ekonomické transakcie, ale mohli by byť zneužívané na pranie špinavých peňazí a financovanie terorizmu a iných nelegálnych aktivít vrátane financovania hybridných hrozieb. Správa upozornila na rastúcu úlohu nebankových subjektov, ktoré ponúkajú nové produkty, ako sú predplatené karty, elektronické peňaženky, mobilné platby, internetové platobné služby a digitálne drahé kovy. (FAFT, 2006).

V roku 2009 sa Európska komisia (EK) zaoberala možným zneužívaním nových platobných metód teroristami a v Štokholmskom programe uviedla, že nástroje na boj proti financovaniu terorizmu sa musia prispôbiť novým potenciálnym hrozbám finančného systému ako aj zneužívaniu peňažných služieb a nových platobných metód teroristami. (EK, 2009).

Cieľom tohto príspevku je zmapovať riziká spojené s využívaním nových produktov a technológií na postupy finančných inštitúcií v boji proti praniu špinavých peňazí a financovaniu terorizmu a definovať možnosti využitia doterajších skúseností v boji proti hybridným hrozbám. Pri spracovaní príspevku sme použili vedecké a odborné články k danej problematike a dostupné oficiálne zdroje EÚ a SR, ktoré sme podrobili analýze.

1. INŠTITUCIONÁLNE A LEGISLATÍVNE VÝCHODISKÁ K PROBLEMATIKE

V roku 1988 bol prijatý Dohovor Organizácie Spojených národov proti nezákonnému obchodovaniu s omamnými a psychotropnými látkami, ktorý mal za cieľ podporiť medzinárodnú spoluprácu zainteresovaných organizácií a prijatie potrebných legislatívnych a administratívnych opatrení. (UN Office on Drugs and Crime, 2013). V nasledujúcom roku bola založená medzinárodná organizácia Financial Action Task Force on Money Laundering s cieľom analyzovať trendy v praní špinavých peňazí. Položili sa tak základy medzinárodnej spolupráce v boji proti praniu špinavých peňazí.

Dôležitým výsledkom činnosti FAFT bola formulácia 40 odporúčaní na boj proti praniu špinavých peňazí, ktoré boli neskôr po teroristických útokoch v USA doplnené o 9 odporúčaní týkajúcich sa financovania terorizmu.

FATF v rámci svojej činnosti spresňuje a posilňuje odporúčania s cieľom zabezpečiť, aby krajiny mali čo najsilnejšie nástroje na boj proti praniu špinavých peňazí, financovaniu terorizmu a ďalších nelegálnych aktivít. FATF revidovala svoje štandardy tak, aby zahŕňali záväzné opatrenia na reguláciu a dohľad nad činnosťami a poskytovateľmi služieb súvisiacich s virtuálnymi alebo kryptografickými aktívami. (FAFT, 2014). V roku 2022 FATF ďalej posilnila globálne pravidlá skutočného vlastníctva v štandardoch FATF, aby zabránila zločincovi skrývať svoje nezákonné aktivity a špinavé peniaze za tajnými podnikovými štruktúrami.

Dôležitou organizáciou v boji proti praniu špinavých peňazí je aj Egmont Group, ktorý zabezpečuje spoluprácu pri bezpečnej výmene spravodajských informácií a skúseností medzi 170 národnými finančnými spravodajskými jednotkami. (Egmont Group, 2023). Finančné spravodajské jednotky

majú jedinečnú pozíciu na podporu národného a medzinárodného úsilia v boji proti praniu špinavých peňazí a financovaniu terorizmu.

V rámci Európy pôsobí Výbor expertov pre hodnotenie opatrení proti praniu špinavých peňazí a financovanie terorizmu – MONEYVAL, ktorý je stálym monitorovacím orgánom Rady Európy povereným úlohou posudzovať súlad so základnými medzinárodnými štandardmi na boj proti praniu špinavých peňazí a financovaniu terorizmu a účinnosti ich vykonávania, ako aj s úlohou vydávať odporúčania vnútroštátnym orgánom, pokiaľ ide o potrebné zlepšenia ich systémov. Prostredníctvom dynamického procesu vzájomných hodnotení sa MONEYVAL zameriava na zlepšenie kapacít vnútroštátnych orgánov na účinnejší boj proti praniu špinavých peňazí a financovaniu terorizmu. Cieľom MONEYVAL je zabezpečiť, aby jej členské štáty mali zavedené účinné systémy na boj proti praniu špinavých peňazí a financovaniu terorizmu a dodržiavali príslušné medzinárodné štandardy.

Problematika prania špinavých peňazí a financovania terorizmu je upravená príslušnými smernicami EÚ. V júni 2017 nadobudla účinnosť Štvrtá smernica o boji proti praniu špinavých peňazí s cieľom posilniť existujúce pravidlá s ambíciou zefektívniť boj proti praniu špinavých peňazí a financovaniu terorizmu. Dňa 1. februára 2018 schválila NR SR novelu zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaní terorizmu, ktorá implementovala Smernicu do právneho poriadku SR.

Jedným z najdôležitejších nástrojov používaných v boji proti praniu špinavých peňazí a financovaniu terorizmu je znalosť používaných metód, ktoré sú čoraz sofistikovanejšie a komplikovanejšie, čo tiež sťažuje ich odhalenie. Predpokladá sa, že v nasledujúcom období sa pozornosť páchatel'ov tejto činnosti sústreďí najmä na:

- zneužívanie elektronických peňazí využívaním sofistikovanejších spôsobov páchania trestnej činnosti s použitím falošných identifikačných dokladov a ľudí v núdzi, ktorí majú zvyčajne bydlisko mimo Európskej únie,
- zakladanie špecializovaných spoločností a profilovanie odborníkov vykonávajúcich ukrývanie a umiestňovanie príjmov z trestnej činnosti a ich legalizáciu na objednávku,
- investície zahraničných subjektov páhajúcich trestnú činnosť na území SR a naopak; investície do nehnuteľností, cenných papierov, tovaru vysokej hodnoty a do akcií spoločností,
- privátne bankovníctvo, ktoré najmä bohatým klientom ponúka komplexné bankové služby, obchody s cennými papiermi emitované bankou klienta,
- zvýšená organizovanosť a flexibilita páchatel'ov pri umiestňovaní nezákonne získaných finančných prostriedkov, najmä z podvodov na internete a phishingu; v prípade organizovaných skupín ide často o národné skupiny, pričom je predpokladom vzájomná spolupráca viacerých takýchto skupín rôznych národností,
- používanie domácich a zahraničných účtov na online stávkovanie,
- rozšírenie hazardu,
- postupný presun obchodovania s ľuďmi, drogami, zbraňami a odcudzenými motorovými vozidlami z fyzických osôb na obchodné spoločnosti,
- postupné zapájanie nefinančného sektora (najmä notárov, právnikov, audítorov, daňových poradcov, účtovníkov a realitných maklérov) do procesu legalizácie,

- aktívne zapájať daňových poradcov a účtovníkov do umiestňovania, kombinovania a integrácie nelegálne získaných peňazí do legálnej ekonomiky,
- zvýšenie počtu neziskových organizácií, neinvestičných fondov a nadácií pri súčasnom zvýšení počtu zahraničných finančných transakcií prostredníctvom týchto organizácií,
- umiestnenie výnosov z trestnej činnosti na účty životného poistenia a iné alternatívne sporiace produkty mimo bánk,
- zvýšenie počtu transakcií realizovaných v prospech spoločností so sídlom v daňových rajoch alebo v prospech spoločností, ktoré sú registrované v krajine Európskej únie, ale ktoré sú majetkovo prepojené so spoločnosťami registrovanými v offshore oblastiach,
- vymáhanie nárokov na vrátenie dane z pridanej hodnoty a následné umiestnenie výnosov v legálnom podnikateľskom prostredí. (MV SR, 2022)

V roku 2018 zaviedla EÚ prísnejšie pravidlá na boj proti praniu špinavých peňazí. Hlavným cieľom nových pravidiel bolo sťaženie ukrývania nelegálnych finančných prostriedkov pod vrstvami fiktívnych spoločností, posilnenie kontroly rizikových tretích krajín, posilnenie úlohy orgánov finančného dohľadu a zlepšenie prístupu k informáciám. Nové pravidlá je potrebné neustále prispôsobovať technologickým inováciám, ako sú už spomínané virtuálne meny, zvýšenej integrácii finančných tokov na vnútornom trhu, globálnej povahe teroristických organizácií a vynaliezavosti páchatel'ov trestnej činnosti využívajúcich akékoľvek nedostatky alebo medzery v systéme.

Nové pravidlá boli zapracované do Zákona č. 279/2020 Z.z., ktorým sa menil a dopĺňal zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony, Národnej rady Slovenskej republiky. (NR SR, 2020)

V oblasti kontroly plnenia povinností povinných osôb patrí k orgánom dohľadu Národná banka Slovenska a Ministerstvo financií SR, čím je zabezpečená vyššia efektivita kontroly. Obe inštitúcie majú právomoc kontrolovať len subjekty v ich kompetencii. Ak dohliadajúci alebo štátny dozor povinnej osoby zistí porušenie zákona, túto informáciu bezodkladne oznámi Finančnej spravodajskej jednotke (FSJ). Zákon o ochrane legalizácie príjmov z trestnej činnosti a financovania terorizmu zároveň definuje Finančnú spravodajskú jednotku ako osobitný útvar v rámci služby finančnej polície a vymedzuje jej úlohy a právomoci.

Jednou z priorít FSJ je zlepšiť efektívnosť ohlasovania NOO vo všetkých sektoroch povinných osôb. Na správne chápanie rizík a skvalitnenie nahlasovania boli vypracované metodické pomôcky a realizovali sa školenia. V roku 1922 prijala FSJ spolu 2185 hlásení o NOO v celkovej hodnote transakcií takmer 1.160.635.916,- EUR. (MVSR, 2022).

Na základe právnej charakteristiky povinných osôb stanovenej zákonom o boji proti praniu špinavých peňazí a financovaniu terorizmu je možné jednotlivé NOO rozdeliť do 3 základných skupín:

- hlásenia o NOO od všetkých bánk pôsobiacich na území Slovenskej republiky vrátane Národnej banky Slovenska (NBS),
- hlásenia o NOO od iných finančných inštitúcií ako bánk,
- hlásenia o NOO od nefinančných inštitúcií. (MVSR, 2022)

V Slovenskej republike sú najvýznamnejšími povinnými osobami komerčné banky, NBS, poisťovne, platobné inštitúcie a poštové podniky. Čo sa týka kontroly plnenia povinností povinných osôb, medzi tzv. orgány dohľadu zo strany Národnej banky Slovenska a Ministerstva financií SR, čím sa zabezpečí vyššia efektívnosť kontroly. Obe inštitúcie majú právomoc kontrolovať len subjekty v ich kompetencii. Ak dozorný orgán alebo štátny dozor povinnej osoby zistí porušenie zákona, túto informáciu bezodkladne oznámi FTU. (MVSR, 2022). Z Tabuľky 1 vidíme, že počet nahlasovaných neobvyklých obchodných operácií zo strany nefinančných inštitúcií je pomerne malý a preto je potrebné zvýšiť vzdelávacie aktivity v týchto inštitúciách s dôrazom na nové trendy v legalizácii príjmov z trestnej činnosti.

Tabuľka 1 uvádza prehľad o počte hlásení o NOO zaslaných povinnými osoba SFJ v rokoch 2014-2022

POVINNÉ OSOBY	2014	2015	2016	2017	2018	2019	2020	2021	2022
Národná banka Slovenska	126	77	79	59	53	70	33	19	36
Komerčné banky	325 2	287 6	299 4	249 6	228 0	239 0	185 8	186 1	186 1
Nebankové finančné inštitúcie	420	230	179	71	64	91	77	110	166
Nefinančné inštitúcie	130	81	45	10	112	25	40	52	122
CELKOM	392 8	326 4	329 7	263 6	250 9	257 6	200 8	204 2	218 5

Zdroj: Výpočet autorov na základe údajov uvedených vo Výročných správach Finančnej spravodajskej jednotky SR 2014-2022 dostupných na <https://www.minv.sk/?informacie-o-cinnosti-1>

Podľa údajov FSJ sa neobvyklé obchodné operácie nahlasované v roku 2022 týkali aktuálneho ekonomického diania vo svete, ktoré súviselo s infláciou, zdražovaním a vojnou na Ukrajine. Okrem toho sa na NOO podieľali aj medializované korupčné kauzy. V prípade konfliktu na Ukrajine hlásenia obsahovali hlavne informácie o veľkej hotovosti privážanej z Ukrajiny, ale tiež aj o zahraničných platbách akumulovaných na osobných alebo podnikateľských účtoch pod zámienkou pomoci Ukrajine.

2. NOVÉ PLATOBNÉ METÓDY A ICH POTENCIÁL NA ZNEUŽITIE

Nové platobné metódy (predplatené karty, mobilné platby a internetové platobné služby) sa stali viac používanými a akceptovanými ako alternatívne metódy na iniciovanie platobných transakcií. Niektoré sa dokonca v mnohých krajinách začali objavovať ako alternatíva k tradičnému finančnému systému. Nárast počtu transakcií a objemu prostriedkov presúvaných cez národné platobné systémy bol sprevádzaný nárastom počtu zistených prípadov zneužitia týchto platobných systémov na účely prania špinavých peňazí a financovania terorizmu. Na základe analýzy prípadových štúdií FATF identifikovala varovné signály, ktoré sú relevantné pre všetky produkty a služby národných platobných systémov. Tieto varovné signály možno použiť ako indikátory

podozrivej činnosti, ak sa skutočné použitie výrobku odchyľuje od jeho zamýšľaného použitia alebo nedáva ekonomický zmysel. (FAFT, 2010)

Podľa legislatívy EÚ je vydávanie elektronických peňazí regulovanou finančnou činnosťou bez ohľadu na akékoľvek hodnotové limity, ktoré sa môžu vzťahovať na určitý produkt. V súlade s tým podliehajú vydavatelia elektronických peňazí vnútroštátnym zákonom členských štátov v oblasti boja proti praniu špinavých peňazí a financovaniu terorizmu.

Cieľom nového režimu EÚ pre vydávanie elektronických peňazí, ako ho reviduje druhá smernica o elektronických peniazoch, je uľahčiť prístup na trh nováčikom, konkrétne telekomunikačným spoločnostiam alebo veľkým obchodníkom, ktorí sa chcú zapojiť do trhu elektronických peňazí. Po Smernici o platobných službách sa zásada exkluzivity už nebude vzťahovať na inštitúcie elektronických peňazí, ktoré sú odteraz oprávnené vykonávať akúkoľvek podnikateľskú činnosť okrem vydávania elektronických peňazí. Predplatené platobné karty umožňujú prístup k peňažným prostriedkom, ktoré držiteľ karty platí vopred. Aj keď existuje veľa rôznych typov predplatených kariet, ktoré sa používajú rôznymi spôsobmi, zvyčajne fungujú rovnakým spôsobom ako debetné karty a v konečnom dôsledku sa spoliehajú na prístup k účtu. Môže existovať účet pre každú vydanú kartu alebo alternatívne môže existovať združený účet, ktorý obsahuje predplatené prostriedky pre všetky vydané karty. Karty môžu byť vydané a účty môžu byť vedené v depozitnej inštitúcii alebo nebankovej organizácii; združené účty by mal za normálnych okolností držať emitent v banke. (FAFT, 2006).

V Európskej únii s licenciou na elektronické peniaze pôsobí 13 vydavateľov predplatených kariet. Z 3 najväčších ponúkaných predplatených produktov sú 2 nedobíjateľné s maximálnym limitom 150 EUR a jedna je dobíjacia predplatená karta Mastercard. Odhaduje sa, že na konci roku 2008 bolo vydaných 164 miliónov takýchto kariet. V Slovenskej republike 12 poskytovateľov (bánk) vydalo takmer 4 milióny kariet; agenti môžu slúžiť ako sprostredkovatelia a vzťahuje sa na nich Smernica o platobných službách (2007/64/ES). (FAFT, 2010).

Pri mobilných platbách so vo všeobecnosti používajú na platby za tovar a služby mobilné telefóny a iné bezdrôtové komunikačné zariadenia. Platby sa iniciujú z mobilného komunikačného zariadenia pomocou hlasového prístupu, protokolov textových správ (ako je služba krátkej/jednotnej správy alebo SMS) alebo sa využívajú protokoly bezdrôtových aplikácií (WAP), ktoré umožňujú zariadeniu pristupovať k internetovej sieti. Autorizácia sa často uskutočňuje zadáním jedinečného osobného identifikačného čísla (PIN) spojeného so zákazníkom alebo mobilným zariadením. Používanie mobilných platieb sa v jednotlivých krajinách líši. (FAFT, 2006).

Trend v Slovenskej republike za posledné štyri roky ukazuje, že množstvo hotovosti mierne klesá. Ľudia začínajú využívať iné spôsoby platby (bezhotovostné platby a transakcie kartou). V roku 2016 sa objem výberov hotovosti znížil o 1,19 % a počet výberov klesol o 4,88 % v porovnaní s rokom 2015. (EPR, 2018).

V novembri 2017 Európska platobná rada (European Payment Council) zadefinovala novú platobnú schému okamžitých platieb SEPA Instant Credit Transfer (SCT Inst) a podmienky pre ich fungovanie. V rámci schémy okamžite platby (SCT Inst) fungujú ako štandardné SEPA platby v mene euro (SEPA Credit Transfer (SCT)), ale prevod prostriedkov je zrealizovaný okamžite,

najneskôr do 10 sekúnd medzi účastníkmi jednotného európskeho platobného priestoru (SEPA). Použitie okamžitých platieb nie je obmedzené, môžu ich používať spotrebitelia, podnikatelia aj veľké firmy. Maximálna povolená suma transakcie je 100 000 eur. Národná banka Slovenska ako súčasť Eurosystému poskytuje pre slovenský bankový trh službu vyrovnania okamžitých platieb v novom platobnom systéme pre okamžité platby TIPS (Target Instant Payment Settlement), ktorý prevádzkuje Eurosystém. Okamžité platby na Slovensku poskytujú svojim klientom banky : Slovenská sporiteľňa, Tatrabanka, VÚB banka a J&T Banka. Tieto nové formy platieb prinášajú veľké výzvy v boji proti praniu špinavých peňazí a financovaniu terorizmu. Platby sa realizujú za niekoľko sekúnd a len následne sa dajú zistiť neobvyklé operácie. Nové technológie využívajúce umelú inteligenciu ponúkajú aj možnosti vyhľadávania podozrivých a neobvyklých transakcií. (NBS, 2023).

V posledných rokoch sa k existujúcim problémom pridali aj problém so zabezpečením dodržiavania sankcií, ktoré je v niektorých prípadoch pre finančné inštitúcie pomerne náročné. Sankcie zavedené Organizáciou Spojených národov, Radou EÚ alebo jednotlivými krajinami môžu obmedziť finančné inštitúcie pri poskytovaní niektorých produktov, ktoré sa opierajú o pravidlá a zvyklosti upravené Medzinárodnou obchodnou komorou v Paríži. Finančné inštitúcie môžu byť konfrontované s rôznymi režimami sankcií uložených v rôznych jurisdikciách, v ktorých pôsobia. Pri dokumentárnych transakciách riešia tieto výzvy pomocou doložiek o sankciách, ktoré dopĺňajú do záväzkových prostriedkov, ako sú akreditívy, záruky a inkasá. Snažia sa tak upovedomiť protistrany (korešpondenčné banky alebo príjemcov), že sankcie môžu ovplyvniť plnenie ich záväzkov vyplývajúcich z nástrojov financovania obchodu. Problematické sú najmä sankcie obmedzujúce obchod s tovarom s dvojakým použitím, ktorý vyžaduje implementáciu procesov, ktorých cieľom je zistiť, či sa na príslušný tovar vzťahujú sankcie. Požiadavky týkajúce sa tovaru sa primárne vzťahujú na vývozcov a dovozcov a nie na banky. Niekedy regulačné orgány môžu bankám uložiť určité povinnosti, ktoré však nie sú jasne formulované. Interpretácia „dvojakého použitia“ si vyžaduje určitý stupeň technických znalostí, ktoré zamestnanci finančných inštitúcií nemusia vždy mať. Okrem toho sa v dokumentoch môže uvádzať popis tovaru s použitím formulácie, ktorá neumožňuje identifikovať pri takýto tovar možnosť „dvojakého použitia“. (Jančíková, 2019)

Je dôležité, aby banky zabezpečili, že zamestnanci si budú vedomí rizík tovaru s dvojakým použitím a bežných druhov tovaru s dvojakým použitím a budú schopní identifikovať varovné signály, ktoré naznačujú, že tovar s dvojakým použitím sa môže dodávať na nezákonné účely. Zamestnancom by sa mali poskytnúť odkazy na verejné zdroje informácií a iné usmernenia, ktoré by sa mali formalizovať v bankových zásadách a postupoch, aby sa zabezpečilo, že tovar s dvojakým použitím bude možné identifikovať. Je to však veľmi náročné, napríklad spoločnosti z EÚ musia vychádzať zo zoznamu EÚ, ktorý na 240 stranách uvádza klasifikované položky s dvojakým použitím; t.j. tovar, softvér, technológie, dokumenty a schémy bežne používané na civilné účely, ktoré však môžu mať aj vojenské využitie alebo prispieť k šíreniu zbraní hromadného ničenia. (Jančíková, 2019)

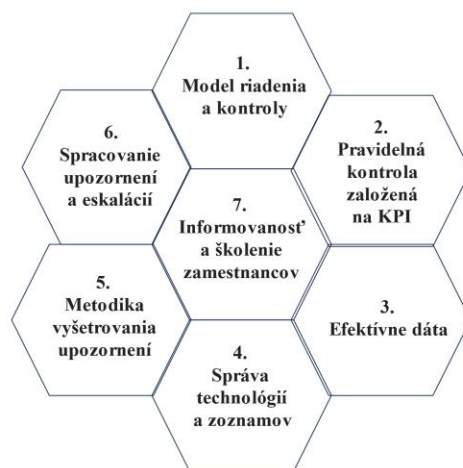
Obchodné embargá zakazujú dodávky tovarov a služieb; priame alebo nepriame finančné služby, ako je financovanie, poistenie, platby, bankové záruky, akreditívy alebo iné služby. Sankcie sa vzťahujú na „určené“ fyzické a právnické „osoby“ a nariaďujú všetkým zmraziť všetok majetok, nerealizovať platby z príkazu alebo v prospech týchto osôb. V skutočnosti sa často používa kombinácia obchodného embarga so sankciami.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) ponúka finančným inštitúciám nástroje pre automatizovaný postup, ktorý im umožňuje kontrolovať mená osôb, spoločností a názvov plavidiel. V niektorých prípadoch môžu preveriť aj popis tovaru, čo je však zložitejšie, ak je popis tovaru napísaný vo voľnom formáte textového poľa, ktoré využíva rôzne prvky informácií, ako sú jednotkové ceny, prepravné značky, počet odoslaných položiek, obchodné podmienky, obchodné zmluvy. Tento problém sa môže vyriešiť aktualizáciou formátu swiftových správ tak, aby sa pole popisu tovaru (45A) v správach MT700, MT710 a MT720 rozdelilo na rôzne „segmenty“ s cieľom izolovať základný opis tovaru, aby sa dal použiť na automatizované preverenie podľa príslušných zoznamov. (SWIFT, 2018)

V obchodnom financovaní sa môžu realizovať aj manuálne kontrolné postupy, pri ktorých banky môžu skontrolovať zúčastnené strany v príslušnom sankčnom zozname, v Európskej únii môžu využiť „Konsolidovaný zoznam osôb, skupín a subjektov podliehajúcich finančným sankciám EÚ“. Banky v USA (aj americké banky v zahraničí) sa odvolávajú na „Zoznam špeciálne určených štátnych príslušníkov“ (SDN) Ministerstva financií USA (Úrad pre kontrolu zahraničných aktív-OFAC). Európska únia ukladá finančné a ekonomické sankcie, ktoré sú záväzné vo všetkých členských štátoch EÚ (prijíma opatrenia OSN alebo na autonómnom základe, niekedy v spolupráci s USA). Môže tiež prijímať opatrenia na autonómnom základe a v spolupráci s inými krajinami. Program preverovania sankcií umožňuje finančným inštitúciám zabezpečiť, aby priamo ani nepriamo neposkytovali sankcionovaným stranám žiadnu formu služieb. Takýto skríningový program je kombináciou zásad, postupov a technológií, ktoré pomáhajú odhaliť transakciu, ktorú by finančná inštitúcia nemala realizovať. Program skríningu sankcií je navrhnutý tak, aby dôkladne zosúladiť politiky, systémy a kontroly s regulačnými usmerneniami a spojil ich s osvedčenými postupmi. Program pomáha finančným inštitúciám hodnotiť, zlepšovať a optimalizovať ich postupy, a tým im umožňuje dodržiavať opatrenia uložené príslušnými regulačnými orgánmi. (PWC, 2015)

Podľa PWC obsahuje efektívny program preverovania sankcií rôzne komponenty zahŕňajúce procesy, ľudí a technológie. V centre toho je ľudský aspekt súvisiaci so školeniami a informovanosťou. Diagram 1 zobrazuje tieto kľúčové komponenty.

Schéma 1: Kľúčové zložky programu sankčného skríningu



Zdroj: Program skríningu prvkov sankcií (PWC, 2015)

1. Komplexná politika sankcií – mala by pokrývať všetky príslušné regulačné požiadavky a mala by byť ľahko zrozumiteľná.
2. Pravidelné preskúmanie – dobre navrhnuté KPI na analýzu rôznych procesov a kontrol rámca skríningu sankcií a pravidelné kontroly a transparentné výkazníctvo manažmentu.
3. Efektívny súbor údajov – zber údajov by mal byť konzistentný a primeraný, tok údajov z rôznych systémov by mal byť neobmedzený, posvätnosť údajov by mala byť zachovaná.
4. Robustná skrínigová platforma – skrínig proti rôznym sledovaným zoznamom by mal byť prepojený s kľúčovými systémami obsahujúcimi statické údaje.
5. Podrobná metodika vyšetrovania – mala by pokrývať všetky aspekty vyšetrovania vrátane kritérií vyhľadávania a technológie na ich podporu.
6. Komplexný proces likvidácie výstrah – pracovný postup pre eskaláciu a ukončenie výstrah, manažment prípadov a audit. (PWC, 2015).

Implementácia rozsiahleho programu preverovania sankcií znamená pre finančné inštitúcie na celom svete viaceré výzvy, od technologických, systémových až po organizačné a kultúrne. V budúcnosti by bolo efektívne, aby využitie nových skrínigových technológií okrem sankcií zahrňovalo všetky nelegálne aktivity vrátane korupcie, prania špinavých peňazí, financovania terorizmu a financovania hybridných hrozieb. V rámci jednotného školenia povinných osôb by sa mohlo takto dosiahnuť skvalitnenie spolupráce.

ZÁVER

Boj proti praniu špinavých peňazí je dôležitou súčasťou celkového boja proti obchodovaniu s drogami, organizovanému zločinu a už niekoľko rokov aj proti financovaniu terorizmu. Tridsať rokov po prijatí prvého medzinárodného dohovoru, Dohovoru OSN proti nedovolenému obchodovaniu s omamnými a psychotropnými látkami, vidíme, že tento boj sa ešte neskončil. Práve naopak. Globalizácia a nové technológie formovali svet v posledných desaťročiach. Napriek všetkému dobrému, čo nám otvorené hranice a online bankové prevody poskytli, poskytli zločincovi aj úplne nové možnosti, ktoré môžu použiť na transfer a skrývanie nezákonne získaných peňazí, a tým znížiť transakčné náklady trestnej činnosti. Je čoraz ťažšie kontrolovať stovky miliárd medzinárodných transakcií, ktoré sa uskutočňujú ročne po celom svete. Legislatíva v oblasti boja proti praniu špinavých peňazí v Slovenskej republike je v súlade s medzinárodnými normami a normami Európskej únie, stále však môžeme vidieť rezervy v ich uplatňovaní v praxi.

Finančné inštitúcie musia čeliť aj novým výzvam v oblasti sankcií, ktoré okrem sankcií voči subjektom zahŕňajú preverovanie určitých komodít, ktoré majú dvojaké použitie. Niektoré opatrenia sa môžu realizovať manuálne, ale finančné inštitúcie hľadajú nové technologické možnosti, ktorými môžu odhaľovať transakcie podozrivé z prania špinavých peňazí, financovania terorizmu alebo obchádzania sankcií. Tieto technológie by bolo možno využiť aj pri odhaľovaní financovania hybridných hrozieb.

Pri využití nových technológií zohráva svoju úlohu aj medzinárodná organizácia SWIFT, ktorá umožňuje kontrolovať niektoré údaje, ako napríklad mená osôb, spoločností a názvov plavidiel. Pre skvalitnenie skrínigu je potrebné zmeniť štruktúru niektorých štandardizovaných správ. V tejto súvislosti je možno otázne, či sankcie na používanie SWIFTu nie sú kontraproduktívne, vzhľadom na to, že vylúčením niektorých krajín z používania SWIFTu sa znemožní aj kontrola ich medzinárodných finančných transakcií.

Pod'akovanie

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

Zdroje

1. Baath D., Zellhorn Handledare F. 2016. How to combat money laundering in Bitcoin? An institutional and game theoretic approach to antimoney laundering prevention measures aimed at Bitcoin. [online]. [cit.2018-02-22]. Dostupné na internete: www.liu.se
2. Cîrdei, I.A. and Ispas, L. [online]. 2017. A Possible Answer of the European Union to Hybrid Threats. In Scientific Bulletin, 22(2), s.71–78. [cit.15.3.2023]. Dostupné na internete: <<https://doi.org/10.1515/bsaft-2017-0009> >.
3. Egmont Group, 2022. Annual Report 2021. [Online]. [cit.2023-09-09]. Dostupné na internete: https://egmontgroup.org/wp-content/uploads/2023/07/Egmont-Group_AnnualReport_2021-22_FINAL_07-31-23_SINGLE-PGS_WEB.pdf
4. European Commission. 2016. Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering, Strasbourg, 5. July 2016. [online]. [cit.2018-02-22]. Dostupné na internete: http://europa.eu/rapid/press-release_TP-16-2380_en.htm
5. European Council, 2009, Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, [Online]. [cit.2018-02-22]. Dostupné na internete: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF>
6. European Payment Council. (2018). The Slovak payment landscape. [Online]. [cit.2018-02-22]. Dostupné na internete: <https://www.europeanpaymentscouncil.eu/news-insights/insight/slovak-payment-landscape>
7. FATF, (2006) Report on new payment methods. [online]. [cit.2018-02-22]. Dostupné na internete: <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.Pdf>
8. FATF, (2010). Money Laundering Using New Payment Methods- October 2010. [online]. [cit.2018-02-22]. Dostupné na internete: http://www.ctif-cfi.be/website/images/NL/typo_fatf/46705859.pdf
9. FATF (2014). FATF Report. Virtual Currencies Key Definitions and Potential AML/CFT Risks.[online]. [cit.2018-02-22]. Dostupné na internete: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
10. Jančíková, E. 2019. Impact Of Eu And Us Sanctions Against Russia And Iran On Trade Finance, In *Medzinarodne vzťahy (Journal of International Relations)*, Ekonomická univerzita, Fakulta medzinárodných vzťahov, vol. 17(3), pages 210-223.
11. Korauš, A. – Kurilovská L. – Šišulák, S. 2022. Increasing the Competencies and Awareness of Public Administration Worker in the Context of Current Hybrid Threats. In Conference Proceedings RELIK 2022. Reproduction of Human Capital – mutual links and connections, November 10-11, 2022. Praha: Vysoká škola ekonomická, 2022. ISBN 978-80-245-2466-5.

12. Ministerstvo vnútra SR (2022). Výročné správy Finančných spravodajských jednotiek SR v rokoch 2016-2022. [online]. [cit.2023-09-02]. Dostupné na internete: <https://www.minv.sk/?informacie-o-cinnosti-1>
13. Národný bezpečnostný úrad SR, 2022. *Koncepcia pre boj SR proti hybridným hrozbám* [online]. [cit.15.3.2023]. Dostupné na internete: <<https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>
14. Národná banka Slovenska. (2023). SEPA okamžité platby. [online]. [cit.2023-09-02]. Dostupné na internete: <https://nbs.sk/platby/platobne-nastroje/sepa-okamzite-platby/>
15. PWC. 2015. Elements of Sanction Screening Programme. PriceWaterhouseCoopers, Private Limited. [online]. [cit.2023-09-02]. Dostupné na internete: <https://www.pwc.in/assets/pdfs/publications/2016/elements-of-sanctions-screening-programme.pdf>
16. SWIFT. 2018. Sanctions filters: the expert guide. A practical guide to maximising the effectiveness of your sanction's filters. [cit.2018-05-25]. Dostupné na internete: <https://www.swift.com/resource/sanctions-filters-expert-guide>.
17. UN Office on Drugs and Crime, 2013. United Nations Convention against Illicit Traffic in Narcotic, Drugs and Psychotropic Substances. [Online]. [cit.2018-02-22]. Dostupné na internete: <https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20VI/VI-19.en.pdf>
18. Zákon č. 279/2020 Z.z., ktorým sa menil a doplňal zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a doplňajú niektoré zákony, Národnej rady Slovenskej republiky. [Online]. [cit.2023-09-02]. Dostupné na internete: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/297/T>

PRÁVNE ASPEKTY HYBRIDNÝCH HROZIEB

Mgr. Sebastián Janko, PhD.

Katedra trestného práva, Akadémia Policajného zboru v Bratislave; Sklabinská 1, Bratislava; sebastian.janko@akademiapz.sk

Abstrakt: Predkladaný príspevok predstavuje možnosti právnej regulácie vybraných foriem hybridných hrozieb. Zameriava sa na tie oblasti, v ktorých je možné právnymi prostriedkami čo možno najefektívnejšie regulovať riziká spojené s konaním aktérov hybridných hrozieb, či už vytváraním odolného právneho prostredia, alebo následným vyvodzovaním administratívnoprávnej, resp. aj trestnoprávnej zodpovednosti a ktoré sú zároveň prítomné v podmienkach SR (vychádzajúc z najnovšieho komplexného analytického dokumentu, ktorým je Hĺbková analýza zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám spracovaná Centrom boja proti hybridným hrozbám MV SR). Pozornosť je teda venovaná v stručnosti kybernetickým útokom, pôsobeniu polovojenských organizácií a preverovaniu priamych zahraničných investícií. Následne sa príspevok detailnejšie venuje problematike postihovania šírenia dezinformácií.

Kľúčové slová: hybridné hrozby, právna úprava, kybernetické útoky, polovojenské organizácie, preverovanie zahraničných investícií, dezinformácie.

ÚVOD

Už v roku 2018 bolo v Koncepcii pre boj Slovenskej republiky proti hybridným hrozbám¹⁸¹ konštatované, že predstavujú zásadný problém pre Slovensko ako členskú krajinu EÚ a NATO. Uvedené platí aj dnes a to minimálne v rovnakej, ak nie ešte výraznejšej miere. Ambíciou predkladaného príspevku je analyzovať a popísať možnosti kontroly hybridných hrozieb právnymi prostriedkami. Limitovaný rozsah príspevku neumožňuje podrobnú analýzu pri všetkých typoch hybridných hrozieb. Zameriame sa preto na tie, ktoré spĺňajú 2 kritériá:

- 1.) sú prítomné v podmienkach SR - hybridné hrozby sú vo väčšine prípadov špecificky prispôbené subjektu, na ktorý majú pôsobiť. V závislosti od viacerých faktorov tak niektoré druhy hybridných hrozieb môžu byť v podmienkach SR prítomné vo väčšej, či menšej miere. Koncepcia Spoločného výskumného centra EÚ definuje 40 nástrojov hybridných hrozieb v 13 doménach (oblastiach pôsobenia). Podľa Hĺbkovej analýzy zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám¹⁸² je pre SR relevantných 25 nástrojov.
- 2.) právo predstavuje efektívny prostriedok boja proti hybridným hrozbám daného typu - je potrebné skonštatovať, že v niektorých oblastiach môžu mať právne prostriedky nanajvýš podporný charakter. Ako príklad možno uviesť problematiku zneužívania energetickej závislosti a poukázať pritom na zákon č. 357/2022 Z. z., ktorým sa mení zákon č. 534/2021 Z. z. o štátnom rozpočte na rok 2022. Tento zákon navýšil kompenzačné opatrenia súvisiace s energetickou krízou. Energetickú krízu ako takú ale právnymi prostriedkami (minimálne z úrovne SR) riešiť nemožno. Ide tak len o zmiernenie následkov a to opatreniami v podstate ekonomického charakteru, ktoré však nevyhnutne potrebujú určitý právny

¹⁸¹ Uznesenie vlády SR č. 345/2018 zo dňa 11.7.2018

¹⁸² Kol., 2023. *Hĺbková analýza zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám*. CBHH ISBA MV SR, s. 6. [online] Dostupné na https://www.hybridnehrozby.sk/wp-content/uploads/2023/08/CBHH_analyza_final_web.pdf

rámec. Predmetom záujmu predkladaného príspevku však budú najmä oblasti, kde právna regulácia môže pôsobiť (proaktívne, alebo reaktívne) voči samotnej podstate konkrétneho typu hybridnej hrozby.

1. NARÚŠANIE KYBERNETICKEJ BEZPEČNOSTI

S ohľadom na neustále rastúcu mieru digitalizácie možno kybernetickú doménu hybridných hrozieb považovať za jednu z najvýznamnejších. Aktivita v tejto oblasti predstavujú najmä kybernetické útoky (obzvlášť na prvky kritickej infraštruktúry, verejnú správu) a kybernetická špionáž. Z pohľadu možností kontroly tohto druhu hybridných hrozieb právnymi prostriedkami možno identifikovať 2 aspekty:

- 1.) vytváranie odolného prostredia - tento aspekt pokrýva predovšetkým zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý o.i. ustanovuje národnú stratégiu kybernetickej bezpečnosti, definuje jednotky CSIRT a ich kompetencie, postavenie a povinnosti prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb. Ide o značne obsiahlu problematiku, ktorej je v tejto publikácii venovaný priestor na inom mieste.
- 2.) vyvodzovanie zodpovednosti za realizáciu kybernetických útokov - trestný zákon obsahuje osobitné skutkové podstaty aplikovateľné aj v prípadoch kybernetických útokov. Konkrétne ide o trestné činy podľa § 247 a nasl. - najmä neoprávnený prístup do počítačového systému neoprávnený zásah do počítačového systému a neoprávnený zásah do počítačového údajov. V praktickej rovine sú však takéto skutky postihované zriedkavo. Vychádzajúc z údajov Evidenčno-štatistického systému kriminality, nápad sa pri týchto trestných činoch dlhodobo pohybuje najviac v niekoľkých desiatkach, obvykle ale len v jednotkách prípadov ročne, pričom objasnenosť je taktiež minimálna. V kontexte hybridných hrozieb možno dodať, že aj pokiaľ by sa podarilo identifikovať konkrétneho aktéra zodpovedného za kybernetický útok, vysoko pravdepodobne sa táto osoba bude nachádzať mimo dosahu orgánov činných v trestnom konaní a nebude možné zabezpečiť jej prítomnosť pre potreby trestného stíhania. V rámci kybernetickej domény hybridných hrozieb tak jednoznačne dominuje prvý z uvedených aspektov, ktorý by mal byť posilnený vzdelávaním a zvyšovaním všeobecného povedomia v oblasti kybernetickej bezpečnosti.

1.1 Polovojenské organizácie

Za riziká spojené s existenciou polovojenských (paramilitárnych) ozbrojených skupín je potrebné považovať najmä bezpečnostné hrozby spojené s ovplyvňovaním týchto skupín zahraničnými aktérmi, čo by mohlo viesť k agresívnej ozbrojenej účasti príslušníkov týchto skupín na nepokojoch, v krajnom prípade až k vykonávaniu fyzických operácií voči bezpečnostným zložkám SR, kritickej infraštruktúre a ďalším záujmom SR.

Právna úprava v tejto oblasti je nedostatočná, čo konštatuje aj Akčný plán koordinácie boja proti hybridným hrozbám pre obdobie 2022 až 2024 (ďalej len APHH)¹⁸³, ktorý obsahuje úlohu „Zákaz pôsobenia štátu nelojálnych polovojenských skupín.“ Doposiaľ nebola prijatá žiadna osobitná úprava zakazujúca zmienené zoskupenia. Okrajovo je v predmetnej oblasti aplikovateľný zákon č. 83/1990 Zb. o združovaní občanov, ktorý v § 4 písm. c) zakazuje združenia ozbrojené alebo s ozbrojenými zložkami; za také sa nepovažujú združenia, ktorých členovia držia alebo používajú

¹⁸³ Schválený uznesením Vlády SR č. 235/2022 zo dňa 30.3.2022.

strelné zbrane na športové účely. Táto právna úprava sa na prvý pohľad môže javiť ako dostačujúca, nakoľko ustanovuje explicitný zákaz, avšak vecná pôsobnosť zákona je obmedzená na združenia. Združením pritom zákon rozumie spolky, spoločnosti, zväzy, hnutia, kluby a iné občianske združenia a odborové organizácie. V každom z uvedených prípadov ide o právnickú osobu s vlastnou právnou subjektivitou. Neformálne zoskupenia osôb bez právnej subjektivity do pôsobnosti citovaného zákona nespádajú a pokiaľ sa tieto osoby nedopúšťajú protiprávneho konania (napr. manipulácia so zbraňami bez oprávnenia, čo by predstavovalo trestný čin nedovoleného ozbrojovania a obchodovania so zbraňami podľa § 294 TZ), neexistuje právny základ, ktorý by umožňoval zamedzenie ich aktivít.

Inšpiratívnym príkladom môže byť aj ČR, kde je v zmysle § 3 zákona č. 14/2021 Sb. o nakládání se zbraněmi v některých případech ovlivňujících vnitřní pořádek nebo bezpečnost České republiky zakázané zakladat', organizovat', vyzbrojovat' ozbrojenou skupinu, alebo sa zúčastňovať na jej činnosti. Najmä pojmom „zúčastňovať sa na jej činnosti“ je vytvorená kvalitná ochrana bezpečnostných záujmov, nakoľko ide o široký pojem pokrývajúci najrôznejšie (aj skryté resp. zastierané, neformálne) pôsobenie v prospech takýchto skupín. Zároveň ide o pojem s (v podmienkach SR) existujúcim súdnym výkladom v súvislosti najmä s trestným činom založenia, zosnovania a podporovania zločineckej skupiny podľa § 296 TZ. Výklad by teda pri zakotvení obdobnej právnej úpravy u nás bol uľahčený. Samotný pojem ozbrojená skupina ďalej zákon 14/2021 Sb. precizuje ako skupinu, ktorá (1.) má povahu paramilitárnej ozbrojenej zložky, (2.) je určená k ozbrojovaniu presadzovaniu cieľov založených na politickej náboženskej, alebo inej ideológii a (3.) nakladá so zbraňami, usiluje sa o prístup k zbraňam, alebo organizuje osoby, ktoré nakladajú so zbraňami. Uvedené charakteristiky musia byť splnené kumulatívne. Čiastkovú výhradu možno mať k absencii definície pojmu „paramilitárna ozbrojená zložka“. V zásade možno uvedené vysvetľovať ako fungovanie skupiny podľa princípov uplatňovaných v bezpečnostných zložkách (napr. hierarchická organizovanosť a s ňou súvisiace právo vydávať a povinnosť plniť rozkazy). Porušenie uvedeného zákazu zakladá zodpovednosť za priestupok. Tým nie je dotknutá prípadná trestnoprávna zodpovednosť za neoprávnené nakladanie so zbraňami, alebo iné protiprávne činnosti vykonávané skupinou resp. jej členmi. Táto koncepcia tak zároveň rešpektuje požiadavku subsidiarity trestnej represie.

1.2 Priame zahraničné investície

Aktuálna neistá ekonomická situácia a zlý stav verejných financií nepochybne zvýrazňujú potrebu a dôležitosť prílevu zahraničného kapitálu do SR. Zároveň však ide o príležitosť pre aktérov hybridných hrozieb ako získať vplyv vo vybraných strategických sektoroch a tento následne využívať proti bezpečnostným záujmom SR. Uvedené riziká sú aktuálne v celej EÚ na čo upozornila už opakovane aj Európska komisia.¹⁸⁴ Rámec preverovania priamych zahraničných investícií v EÚ je daný Nariadením Európskeho parlamentu a Rady (EÚ) 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie. Ide však v zásade len o podpornú právnu úpravu, Komisia plní úlohy koordinačného orgánu (v prípadoch, kedy sa investícia dotýka viacerých členských štátov, prípadne projektov a programov samotnej Únie; stanoviská Komisie majú prevažne odporúčajúci charakter, hoci ak sa nimi členské

¹⁸⁴ Pozri napr. OZNÁMENIE KOMISIE Usmernenia pre členské štáty týkajúce sa priamych zahraničných investícií z Ruska a Bieloruska s ohľadom na vojenskú agresiu voči Ukrajine a reštriktívne opatrenia stanovené v nedávnych nariadeniach Rady o sankciách. Ú.V. EÚ C 151.

štáty neriadia, musia túto skutočnosť zdôvodniť). Dominantné postavenie v systéme preverovania priamych zahraničných investícií tak majú národné authority. Nie každý členský štát má osobitný systém preverovania priamych zahraničných investícií. SR však s účinnosťou od 1.3.2023 takouto úpravou disponuje - ide o zákon č. 497/2022 Z. z. o preverovaní zahraničných investícií.

Podľa tohto predpisu je zahraničnou investíciou je každá investícia (bez ohľadu na jej výšku) plánovaná alebo uskutočnená zahraničným investorom, ktorá mu umožní priamo alebo nepriamo nadobudnúť cieľovú osobu, vykonávať v cieľovej osobe kontrolu, alebo vykonávať v cieľovej osobe účinnú účasť, nadobudnúť podstatné aktíva v cieľovej osobe. Cieľovou osobou je pritom osoba so sídlom v Slovenskej republike, ktorá existuje alebo vznikne v súvislosti so zahraničnou investíciou, a to bez ohľadu na jej právnu formu, existenciu právnej subjektivity, spôsob financovania a zameranie činnosti vrátane zamerania činnosti na dosahovanie zisku. Pojem zahraničný investor v zásade zahŕňa FO a PO, ktoré nie sú občanmi SR ani iného členského štátu EÚ, resp. nemajú sídlo na území SR ani iného členského štátu. Za zahraničných investorov sa však považujú aj takéto subjekty, ak je financovanie investície zabezpečené prostredníctvom zdrojov poskytnutých subjektom s majetkovou účasťou tretej krajiny, alebo orgánom verejnej moci tretej krajiny. Podstatou rozšírenia pojmu zahraničný investor aj na subjekty zo SR resp. EÚ je snaha o elimináciu konaní, ktoré by zastierali skutočne existujúce prepojenia na subjekty z tretích krajín s cieľom vyhnúť sa preverovaniu investície ako zahraničnej. Osobitným druhom zahraničných investícií sú kritické zahraničné investície, ktoré predstavujú zvýšené riziko negatívneho vplyvu na bezpečnosť alebo verejný poriadok SR. Ide o investície v odvetviach vymedzených Nariadením vlády SR č. 61/2023 Z. z., ktorým sa ustanovujú kritické zahraničné investície. Patrí sem napr. výroba výrobkov obranného priemyslu a položiek s dvojakým použitím, výskum a vývoj v týchto oblastiach, poskytovanie základných služieb a digitálnych služieb v oblasti cloud computingu, pôsobenie v mediálnej oblasti (programové služby, platformy na zdieľanie obsahu s obrátom nad 2 mil. EUR, prevádzkovanie spravodajských webových portálov, vydávanie periodických publikácií).

V samotnom procese preverovania zahraničnej investície má dominantné postavenie Ministerstvo hospodárstva SR. Konanie pozostáva z dvoch hlavných častí:

- 1.) posudzovanie rizika negatívneho vplyvu zahraničnej investície – pri posudzovaní rizika MH SR vychádza z faktorov vymedzených v § 10 predmetného zákona. Informačný servis pre MH SR poskytujú spravodajské služby, Policajný zbor a konzultujúce orgány (MV SR, MZVEZ SR, MO SR, prípadne aj iné ministerstvá, ak sa investícia týka ich pôsobnosti). Ak je investícia vyhodnotená ako riziková (avšak vždy, ak ide o kritickú investíciu), nastupuje druhá fáza procesu.
- 2.) preverovanie – ide o podrobnejšie preverenie zahraničnej investície, vyššie uvedené orgány (a vždy aj MF SR) sú povinné MH SR poskytnúť stanoviská k preverovanej zahraničnej investícii do 40 dní od doručenia informácie o začatí preverovania. MH SR následne vypracuje návrh stanoviska, v ktorom skonštatuje, že:
 - a) zahraničná investícia nemá negatívny vplyv
 - b) zahraničná investícia má negatívny vplyv, ktorý môže byť odstránený pomocou tzv. mitigačných opatrení (spočívajúcich najmä v povinnosti niečo vykonať, alebo sa niečoho zdržať)
 - c) zahraničná investícia má negatívny vplyv – v tomto prípade negatívny vplyv nemožno odstrániť mitigačnými opatreniami

Po predložení návrhu stanoviska investorovi a cieľovej osobe majú tieto subjekty možnosť vyjadriť sa k návrhu stanoviska. Následne MH SR vydá rozhodnutie o povolení zahraničnej

investície, podmienanom povolení zahraničnej investície (s povinnosťou vykonať mitigačné opatrenia), alebo rozhodnutie o zákaze zahraničnej investície (v tomto prípade sa vyžaduje predchádzajúce súhlasné stanovisko vlády SR).

2. DEZINFORMÁCIE A PROPAGANDA

Podľa už citovanej Hĺbkovej analýzy zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám sú dezinformácie najčastejšie využívaným nástrojom hybridných hrozieb. Zároveň ide o pôsobenie s priamym dopadom na široké skupiny obyvateľstva, k čomu prispieva najmä šírenie dezinformácií prostredníctvom sociálnych sietí. Z uvedených dôvodov bude tejto problematike venovaná osobitná pozornosť vo forme samostatnej kapitoly.

Pred úvahami o možnostiach vyvodzovania právnej zodpovednosti za šírenie dezinformácií je potrebné upriamiť pozornosť na skutočnosť, že samotný pojem dezinformácia nie je legálne definovaný. K dispozícii sú len definície z odbornej literatúry a koncepcných dokumentov, ktoré nemajú právnu záväznosť. Uviesť možno definíciu z Krátkeho slovníka hybridných hrozieb vypracovaného Národným bezpečnostným analytickým centrom (NBAC) SIS, v zmysle ktorej je dezinformáciou „overiteľne nepravdivá, zavádzajúca alebo manipulatívne podaná informácia, ktorá je zámerne vytvorená, prezentovaná a šírená s jednoznačným úmyslom klamať alebo zavádzať, spôsobiť nejaký 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.“¹⁸⁵ Veľmi podobne pojem dezinformácia definujú zahraniční autori – podľa Van Hobokena et al.¹⁸⁶ ide o „overiteľne nepravdivú, alebo zavádzajúcu informáciu vytvorenú, prezentovanú, alebo rozširovanú za účelom dosiahnutia ekonomického prospechu, alebo účelového zavádzania verejnosti, ktorá môže spôsobiť verejnú ujmu.“ Totožná je aj definícia dezinformácie v Kódexe postupov EÚ proti šíreniu dezinformácií¹⁸⁷, pričom nad rámec uvedeného precizuje pojem verejnej ujmy ako ohrozenia demokratických politických a rozhodovacích procesov alebo verejných statkov ako ochrana zdravia obyvateľstva, ochrana životného prostredia, bezpečnosť. Bayer et. al.¹⁸⁸ dopĺňajú ďalší, podľa nášho názoru kľúčový znak, ktorým je strategické rozširovanie. Tento znak sa neviaže k samotnému informačnému obsahu, ale k spôsobu, akým sa s týmto obsahom pracuje. Je potrebné skonštatovať, že napriek výrazným podobnostiam sa v jednotlivých definíciách vyskytujú veľmi podstatné odchýlky. Niektoré definície vyžadujú, aby bola dezinformácia overiteľne nepravdivá. Je samozrejme potrebné precizovať výklad tohto pojmu – podľa nášho názoru je potrebné, aby nepravdivosť informácie bola zrejmá pri vynaložení primeraného (v závislosti od subjektu, ktorý túto informáciu vytvára/šíri) úsilia a to v čase, kedy k

¹⁸⁵ Dostupné online na: <https://www.sis.gov.sk/o-nas/nbac-slovník-hh.html>

¹⁸⁶ Van Hoboken, J. et. al., 2019. *The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising* [Report]. Dutch Ministry of Interior and Kingdom Relations, s. 15. [online] https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf

¹⁸⁷ OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Boj proti dezinformáciám na internete: európsky prístup. COM(2018) 236

¹⁸⁸ BAYER, J. et. al. 2019 *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States*. SSRN Electronic Journal. s. 12. [online] Dostupné na: <https://doi.org/10.2139/ssrn.3409279>

vytvoreníu/šíreníu informácie dochádza. Dezinformácia teda na základe uvedeného musí kumulatívne spĺňať 4 znaky:

- 1.) je overiteľne nepravdivá, alebo zavádzajúca. Pod pojmom zavádzajúca je potrebné vnímať informáciu, ktorá síce sama o sebe môže byť pravdivá, ale svojim podaním navádza k nesprávnej interpretácii (napr. vytrhnutie určitého vyjadrenia z kontextu a uvedenie v súvislosti značne odlišnej od zámeru autora vyjadrenia).
- 2.) je vytvorená, prezentovaná, alebo rozširovaná za účelom dosiahnutia zisku, alebo inej výhody
- 3.) je spôsobilá ohroziť verejné záujmy – demokratické procesy, verejné zdravie, verejný poriadok, bezpečnosť.
- 4.) je strategicky rozširovaná – rozširovanie nezriedka prebieha na viacerých úrovniach počnúc subjektami priamo napojenými na pôvodcu naratívu a ďalšími subjektami, ktoré konajú na základe vlastných, niekedy značne odlišných, motivácií.

Napriek tomu, že uvedené definície nepochybne prinášajú do problematiky určitú mieru prehľadnosti a jednoznačnosti, domnievame sa, že je potrebné pojem dezinformácia vnímať ako značne heterogénny. Aj pri splnení všetkých definičných znakov totiž do úvahy pripadá mimoriadne rozmanitá a predovšetkým z hľadiska spoločenskej nebezpečnosti značne rozličná škála konaní. Napríklad masívna, ale krátkodobá reklamná kampaň propagujúca „zázračný“ výživový doplnok na stratu hmotnosti môže viac či menej napĺňať všetky vyššie uvedené kritériá, ale pravdepodobne bude zo spoločenského hľadiska menej závažná ako dlhodobá kampaň dezinterpretujúca napr. problematiku migračnej krízy. Tieto nuansy bude potrebné zohľadňovať aj pri prípadnom obmedzovaní šírenia dezinformácií právnymi prostriedkami, či dokonca vyvodzovaní trestnoprávnej zodpovednosti za šírenie dezinformácií. Akékoľvek obdobné aktivity je potrebné realizovať veľmi citlivo a s ohľadom na rešpektovanie práva na slobodu prejavu. Obavy z možného neoprávneného obmedzovania slobody prejavu (ako frekventovane skloňovaný argument¹⁸⁹ proti zakotveniu trestnoprávneho sankcionovania šírenia dezinformácií) sa javia ako čiastočne opodstatnené. Judikatúra európskych súdov totiž vo viacerých rozhodnutiach konštatovala, že ochranu podľa čl. 10 Dohovoru požívajú aj také informácie, u ktorých existuje silný predpoklad, že sú nepravdivé.¹⁹⁰ V ďalších rozsudkoch sa EŠLP kriticky postavil aj k administratívno-právnej regulácii slobody prejavu (v podobe zásahov voči webovým stránkam, ktoré publikovali podľa štátnych autorít závadový obsah),¹⁹¹ či k zásahom do slobody prejavu (v podobe špekulatívnych a dôkazmi nepodložených tvrdení) v kontexte predvolebnej kampane.¹⁹²

Vo svetle uvedeného je potrebné uplatňovať reštriktívny prístup pri obmedzovaní slobody prejavu administratívnymi zásahmi. Príkladom v podmienkach SR bolo blokovanie niektorých konšpiračných spravodajských webov na základe §27b zákona o kybernetickej bezpečnosti (ZKB). Napriek nespochybniteľnej efektívnosti uvedeného postupu a skutočnosť, že išlo o krajné prípady, zaznievali k spôsobu realizácie blokovania pomerne zásadné výhrady aj z prostredia rešpektovaných organizácií ako Transparency International Slovensko. Predmetom kritiky boli najmä skutočnosti, že išlo len o administratívne rozhodnutie bez predchádzajúceho súhlasu súdu,

¹⁸⁹ ŠAMKO, P. *Slovenské cúvanie z demokracie cenzúrou internetu (pôjde Slovensko pri blokovaní webových stránok tureckou cestou?)*. [online] Dostupné na: <http://www.pravnelisty.sk/clanky/a1071-slovenske-cuvanie-z-demokracie-cenzurou-internetu-pojde-slovensko-pri-blokovaní-webovych-stranok-tureckou-cestou>

¹⁹⁰ Rozsudok EŠLP vo veci Salov proti Ukrajine zo dňa 27.4.2004.

¹⁹¹ Rozsudok EŠLP vo veci OOO Flavas a ďalší proti Rusku zo dňa 23.6.2020.

¹⁹² Rozsudok EŠLP vo veci Brzeziński proti Poľsku zo dňa 25.7.2019.

bez opravného prostriedku (prípustná bola len správna žaloba, avšak bez odkladného účinku a možno predpokladať aj s pomerne dlhým časovým horizontom), rozhodnutia neboli zverejnené, zdôvodnenie bolo hodnotené ako netransparentné. Ambíciu odstrániť uvedené nedostatky mala novela zákona o kybernetickej bezpečnosti vypracovaná Národným bezpečnostným úradom, pričom táto skutočne mala potenciál svoj cieľ naplniť.¹⁹³ Novela však nebola schválená NR SR. Vzhľadom k časovému obmedzeniu účinnosti §27b ZKB tak v súčasnosti absentuje možnosť promptnej a efektívnej reakcie na rozširovanie dezinformácií zo strany štátu.

Určitú inšpiráciu môže poskytovať aj zákon č. 264/2022 Z. z. o mediálnych službách. V zmysle § 61 citovaného predpisu obsahová služba (programová služba ako televízia, ale aj audiovizuálna mediálna služba na požiadanie – rôzne platformy typu Netflix) nesmie obsahovať, propagovať a šíriť problematické kategórie obsahu (propagácia vojny, násilia, nenáležité zobrazovanie utrpenia a pod., šírenie teroristického obsahu). Medzi týmito kategóriami však nie je explicitne zahrnuté rozširovanie dezinformácií. Zákon o mediálnych službách obsahuje aj úpravu konania na zamedzenie šírenia nelegálneho obsahu. Nelegálnym obsahom sa na účely tohto zákona rozumie obsah, ktorý:

- napĺňa znaky detskej pornografie, alebo extrémistického materiálu
- podnecuje ku konaniu, ktoré napĺňa znaky niektorého z trestných činov terorizmu,
- schvaľuje konanie, ktoré napĺňa znaky niektorého z trestných činov terorizmu, alebo
- napĺňa znaky trestného činu popierania a schvaľovania holokaustu, zločinov politických režimov a zločinov proti ľudskosti, trestného činu hanobenia národa, rasy a presvedčenia alebo trestného činu podnecovania k národnostnej, rasovej a etnickej nenávisti.

V prípade výskytu nelegálneho obsahu môže ktokoľvek podať písomný, alebo elektronický podnet na začatie tohto konania regulátorovi, ktorým je Rada pre mediálne služby. Uvedený obsah sa pritom môže vyskytovať aj v obsahových službách, ktoré nespádajú do pôsobnosti zákona o mediálnych službách, ale súvisiaceho zákona č. 265/2022 o publikáciách, t. j. elektronické periodické publikácie, spravodajské webové portály. Je potrebné podotknúť, že konanie o zamedzení šírenia nelegálneho obsahu má subsidiárny charakter a primárne by malo odstraňovanie nelegálneho obsahu realizované prostredníctvom mechanizmov samotných poskytovateľov služieb. Pokiaľ nekoná samotný poskytovateľ služby, regulátor môže rozhodnúť o zamedzení šírenia nelegálneho obsahu. Rozhodnutie obsahuje:

- informácie umožňujúce identifikovať dotknutý obsah,
- odôvodnenie, prečo dotknutý obsah predstavuje nelegálny obsah,
- odôvodnenie, prečo je šírením nelegálneho obsahu ohrozený verejný záujem alebo prečo predstavuje značný zásah do individuálnych práv či oprávnených záujmov osoby v pôsobnosti právneho poriadku Slovenskej republiky,
- lehotu, v ktorej je poskytovateľ obsahovej služby povinný odstrániť dotknutý nelegálny obsah a zamedziť jeho ďalšie šírenie.

Uvedené mechanizmy by mohli byť efektívne aj pri boji proti šíreniu dezinformácií. To ale samozrejme vyžaduje explicitne zaradiť dezinformácie medzi nelegálny obsah a zároveň precízne pojem dezinformácia definovať, pričom za nelegálny obsah by mali aj v nadväznosti na už citovanú judikatúru považované len tie najzávažnejšie dezinformácie.

¹⁹³ LP/2022/245

Okrem právnej úpravy v SR je veľmi dôležitým prameňom aj tzv. Akt o digitálnych službách¹⁹⁴, ktorý obsahuje komplexnú právnu úpravu tejto oblasti v podmienkach EÚ. Analýza tohto komplexného predpisu však presahuje rozsah aj zameranie predkladanej práce.

Okrem administratívnoprávnej roviny pripadá v súvislosti so šírením dezinformácií do úvahy aj možné vyvodzovanie trestnej zodpovednosti. Pokiaľ ale požiadavka reštriktívneho prístupu platí v rovine administratívnoprávnej, tým viac musí byť tento prístup zachovávaný v rovine trestnoprávnej. Je však potrebné skonštatovať, že už aj v súčasnosti sú prípustné obmedzenia slobody prejavu trestnoprávnymi prostriedkami. Najužšie s problematikou dezinformácií súvisí trestný čin šírenia poplašnej správy. V zmysle tejto skutkovej podstaty je postihnutelný ten, kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo. Napriek zreteľnému prieniku s problematikou dezinformácií, postihovanie šírenia dezinformácií podľa § 361 podľa nášho názoru nie je možné v každom prípade (napriek tomu sa v zahraničnej literatúre¹⁹⁵ SR uvádza medzi štátmi EÚ, ktoré majú zakotvenú trestnoprávnu legislatívu proti dezinformáciám). Uvedené tvrdenie možno argumentačne podložiť rozdielom medzi pojmom poplašná správa a dezinformácia. Poplašná správa je taká, ktorá je svojím obsahom spôsobilá vyvolať vážne znepokojenie vo forme strachu, úzkosti, paniky.¹⁹⁶ Je zrejmé, že nie každá dezinformácia musí mať charakter poplašnej správy. Každopádne z vyššie uvedeného vyplýva, že sloboda prejavu nie je neobmedzeným právom a v prípade, že by jej zneužívanie mohlo mať spoločensky nežiaduce dôsledky, môže byť obmedzená aj prostriedkami trestného práva. Ostáva teda položiť si otázku, či sú riziká spojené so šírením dezinformácií natoľko spoločensky nežiaduce, aby boli takéto konania postihované v trestnoprávnej rovine. Podľa nášho názoru je (v niektorých prípadoch – viď. ďalej v texte) odpoveď kladná. Dezinformácie môžu výrazne negatívnym spôsobom ovplyvniť demokratické procesy v krajine. V porovnaní s tým napr. pri trestnom čine šírenia poplašnej správy postačuje vznik nebezpečenstva, že dôjde k znepokojeniu časti obyvateľstva nejakého miesta. Pokiaľ by už aj došlo k poruche v činnosti PO, alebo štátneho orgánu, šlo by o kvalifikovanú skutkovú podstatu – zločin s trestnou sadzbou 3 až 8 rokov. Ide pritom o poruchu v činnosti aj „len“ jedného štátneho orgánu. V tomto kontexte sa určité typy dezinformácií (najmä pokiaľ sú rozširované strategicky a podkopávajú – aj v právne záväzných dokumentoch¹⁹⁷ vyjadrené – hodnotové a geopolitické smerovanie SR) javia spoločensky výrazne nebezpečnejšie. Pokiaľ teda miera nebezpečnosti doposiaľ trestnoprávne nepostihovaného konania prevyšuje mieru nebezpečnosti už trestnoprávne postihovaného konania, bude namieste, aby aj toto nebezpečnejšie konanie (t. j. šírenie dezinformácií; opäť prízvukujeme, že len v špecifických prípadoch) bolo trestnoprávne sankcionované.

Druhá otázka, s ktorou sa treba v tejto – možno povedať že hodnotovej – rovine problematiky vysporiadať, je otázka princípu subsidiarity trestnej represie. V zmysle tohto (v zákone nie explicitne vyjadreného) základného princípu trestného práva hmotného majú byť prostriedky

¹⁹⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách)

¹⁹⁵ Ó FATHAIGH, R., HELBERGER, N., APPELMAN, N. (2021). *The perils of legally defining disinformation*. In: *Internet Policy Review*, 10(4). [online] Dostupné na: <https://doi.org/10.14763/2021.4.1584>

¹⁹⁶ BURDA, E. a kol. 2010. *Trestný zákon. Osobitná časť. Komentár – II. diel*. Bratislava: C. H. Beck, s. 1214.

¹⁹⁷ Napr. Bezpečnostná stratégia Slovenskej republiky – Uznesenie Vlády SR č. 803/2020, schválená NR SR dňa 28.1.2021.

trestného práva využívané až ako posledná možnosť nápravy nežiaduceho stavu a ku kriminalizácii by zákonodarca nemal pristupovať výlučne na základe aktuálnej politickej či spoločenskej objednávky.¹⁹⁸ S uvedeným sa plne stotožňujeme. Práve problematika dezinformácií resp. prejavovania určitých názorov je z hľadiska trestnoprávneho postihovania mimoriadne citlivá a problematická téma a to z viacerých dôvodov:

- možnosť zneužitia trestného práva ako nástroja na prenasledovanie názorových oponentov – história ponúka viacero príkladov, kedy trestné právo skutočne bolo takýmto spôsobom zneužitú. Na druhej strane sme toho názoru, že kriminalizácia určitých konaní prostredníctvom trestného zákona predstavuje len jeden – a nie nevyhnutne najdôležitejší – predpoklad zneužitia trestného práva. Za významnejšiu v tomto kontexte považujeme inštitucionálnu rovinu. Zakotvenie určitej skutkovej podstaty nepochybne môže poskytovať príležitosť na trestnoprávny postih, ktorý by bol v príkrom rozpore so základnými hodnotami demokratického zriadenia. V tejto súvislosti je inšpiratívnym konštatovanie ústavného súdu o tom, že principiálne nemôže byť zákon označený za protiústavný len preto, že by na jeho základe teoreticky mohlo byť vydané aj rozhodnutie, ktoré by bolo v rozpore s ústavou.¹⁹⁹ K zneužitiu trestného práva totiž nedochádza v rovine abstraktnej, ale procesným postupom konkrétnych orgánov aplikujúcich právo v individuálnej trestnej veci. Preto by skutočne nezávislé a nestranné súdy mali poskytovať dostatočnú garanciu proti tomu, aby sa z kriminalizácie šírenia dezinformácií nestal nástroj štátnej cenzúry akéhokoľvek disentaného názoru. Samozrejme nevyhnutným predpokladom účinnej súdnej ochrany pred zneužitím práva je kvalitne konštruovaná skutková podstata trestného činu, umožňujúca citlivé zohľadnenie všetkých osobitostí konkrétneho prípadu tak, aby prípadný trestnoprávny postih bol plne v súlade so štandardmi rešpektovanými v každom právnom štáte.
- existencia účinnejších nástrojov boja proti dezinformáciám – je bezpodmienečne potrebné akceptovať skutočnosť, že trestné právo v súvislosti s potláčaním určitých (čo ako spoločensky nebezpečných) názorov nie je optimálnym nástrojom. Uvedené vyplýva najmä zo skutočnosti, že prostriedkami trestného práva nemožno postihnúť samotný názor, t. j. určitú myšlienku, ale len prejavovanie, rozširovanie tejto myšlienky, konanie na jej základe a pod. Aplikované na príklad pandémie COVID-19, pokiaľ by došlo k trestnoprávnemu postihu osoby šíriacej dezinformácie o tom, že vakcinácia sa vykonáva s utajovaným zámerom redukovať populáciu, nemuselo by to znamenať, že potrestaná osoba od tohto názoru upustí. Práve naopak v mnohých prípadoch by bol efekt opačný a sankcionovaná osoba by sa ešte utvrdila vo svojom presvedčení (s odôvodnením, že štátne orgány sa pokúšajú umlčať pravdu). V súvislosti s osobami, ktoré šíria dezinformácie v presvedčení o ich pravdivosti je teda oveľa vhodnejšie miesto sankcionovania uplatniť iné nástroje, najmä vzdelávanie a osvetu. Uvedené konštatovanie podľa nášho názoru platí v drvivej väčšine prípadov a trestnoprávny postih by mal nasledovať len v tých prípadoch, ktoré v intenciách vyššie prezentovaných kritérií dosahujú vysoký stupeň nebezpečnosti. Malo by teda ísť o overiteľne nepravdivé, alebo zavádzajúce informácie, ktoré sú šírené s cieľom získať určitú výhodu, sú spôsobilé ohroziť verejný záujem (verejné zdravie, verejný poriadok, demokratické zriadenie) a sú strategicky (často s participáciou cudzej moci) produkované, alebo rozširované.

¹⁹⁸ MARKOVÁ, V., STRÉMY, T., 2019. *Trestné právo hmotné. Všeobecná časť*. Plzeň: Aleš Čeněk, s. 19.

¹⁹⁹ Nález ÚS SR sp. zn. PL. ÚS 5/2012 *mutatis mutandis*.

Práve prvok spojenia s cudzou mocou možno považovať v kontexte dezinformácií, ale aj hybridných hrozieb ako takých za veľmi podstatný. V zmysle platnej a účinnej právnej úpravy totiž neexistujú zákonné znaky, ktoré by špecificky sankcionovali určitú trestnú činnosť ako súčasť hybridných operácií – napr. pri trestnom čine korupcie je z pohľadu trestného práva irelevantné, či ide o strategickú korupciu (ktorá predstavuje jednu z foriem hybridných hrozieb), alebo len o „obyčajnú“ korupciu. V oboch prípadoch pôjde o trestný čin prijímania úplatku resp. podplácania podľa § 328 resp. § 332 TZ. Z viacerých už citovaných dokumentov je pritom zrejmé, že hybridné hrozby predstavujú jednu z najzávažnejších výziev pre vnútornú bezpečnosť SR. Z tohto dôvodu sa javí primeraným, aby aj trestná činnosť páchaná v súvislosti s hybridnými hrozbami bola postihovaná prísnejšie. Na to je však potrebné najprv jednoznačne definovať, kedy pôjde o trestnú činnosť spadajúcu do rámca hybridných hrozieb. Znak „v spojení s cudzou mocou, alebo cudzím činiteľom“ je na tento účel obzvlášť vhodný, nakoľko aktéri hybridných hrozieb veľmi často v konečnom dôsledku presadzujú záujmy štátnych aktérov (hoci prepojenie môže byť skryté prostredníctvom „proxy“ subjektov a ďalších štruktúr). Tento fakt vnímali aj predkladatelia APHH, v ktorom sa v bode E.12 hovorí o rozšírení *„prvku cudzej moci ako prvku kvalifikovanej skutkovej podstaty do širšieho okruhu ustanovení Trestného zákona.“* V zmysle aktuálnej právnej úpravy je spáchanie činu v spojení s cudzou mocou, alebo cudzím činiteľom znakom základnej skutkovej podstaty pri 2 trestných činoch (vlastizrada podľa § 311 a vyzvedačstvo podľa § 318), znakom kvalifikovanej skutkovej podstaty pri 1 trestnom čine (ohrozenie mieru podľa § 417 ods. 2) a inak ide len o všeobecne priťažujúcu okolnosť podľa § 37 písm. l). Z hľadiska významu pre výšku trestu je všeobecne priťažujúca okolnosť značne nedostatočná a to vzhľadom k spôsobu, akým priťažujúce okolnosti ovplyvňujú výšku trestu. Podľa § 38 ods. 4 TZ *„Ak prevažuje pomer priťažujúcich okolností, zvyšuje sa dolná hranica zákonom ustanovenej trestnej sadzby o jednu tretinu.“* Problematická je v tomto prípade požiadavka prevažujúceho pomeru, čo znamená, že priťažujúcich okolností musí byť viac, ako poľahčujúcich. V prípade, že je ich počet rovnaký, trestná sadzba sa nemení, pokiaľ naopak prevažujú okolnosti poľahčujúce, znižuje sa horná hranica zákonom ustanovenej trestnej sadzby o jednu tretinu. To znamená, že vplyv spáchania trestného činu v spojení s cudzou mocou, alebo cudzím činiteľom na výšku trestnej sadzby môže byť eliminovaný už jedinou poľahčujúcou okolnosťou (za predpokladu, že neboli dané iné priťažujúce okolnosti). Takáto úprava sa javí nedostatočná. Podľa navrhovanej ostatnej veľkej novely TZ predloženej do NR SR dňa 30.3.2023 Ministerstvom spravodlivosti SR bolo navrhované neposudzovať spáchanie činu v spojení s cudzou mocou, alebo cudzím činiteľom ako všeobecne priťažujúcu okolnosť, ale ako závažnejší spôsob konania v zmysle § 138. Spáchanie činu závažnejším spôsobom konania je pritom vo väčšine trestných činov znakom podmieňujúcim použitie vyššej trestnej sadzby. Napríklad v prípade trestného činu neoprávneného zásahu do počítačového systému podľa § 247a TZ by po tejto úprave spáchanie TČ v spojení s cudzou mocou (t. j. napríklad útok vykonaný cudzou mocnosťou podporovanou hackerskou skupinou) bolo sankcionovateľné trestom odňatia slobody na 3 až 8 rokov v porovnaní so sadzbou 6 mesiacov až 3 roky pri základnej skutkovej podstate. Problematickou je skutočnosť, že viaceré trestné činy relevantné v kontexte hybridných hrozieb (napr. podplácanie, prijímanie úplatku, šírenie poplašnej správy) neobsahujú (a ani podľa predkladaného návrhu novely nemali obsahovať) závažnejší spôsob konania ako znak kvalifikovaných skutkových podstat. V konečnom dôsledku sa ale žiaľ tieto zmeny presadiť doposiaľ nepodarilo, nakoľko predmetný návrh novely nebol schválený NR SR.

ZÁVER

Predkladaná práca predstavuje možnosti právnej regulácie vybraných foriem hybridných hrozieb. Zameriava sa na tie oblasti, v ktorých je možné právnymi prostriedkami čo možno najefektívnejšie regulovať riziká spojené s konaním aktérov hybridných hrozieb, či už vytváraním odolného právneho prostredia, alebo následným vyvodzovaním administratívnoprávnej, resp. aj trestnoprávnej zodpovednosti a ktoré sú zároveň prítomné v podmienkach SR (vychádzajúc z najnovšieho komplexného analytického dokumentu, ktorým je Hĺbková analýza zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám). Pozornosť bola teda venovaná v stručnosti kybernetickým útokom, pôsobeniu polovojenských organizácií a preverovaniu priamych zahraničných investícií. Následne bola osobitná pozornosť venovaná problematike postihovania šírenia dezinformácií.

V oblasti kybernetických útokov možno konštatovať výraznú disparitu v možnostiach budovania odolného prostredia a vyvodzovaní zodpovednosti za zrealizované kybernetické útoky. Kým v prvej zmienenej oblasti majú právne nástroje pomerne výrazný potenciál, v druhej je dosiahnutie žiaduceho výsledku takmer nemožné.

Pôsobenie polovojenských organizácií predstavuje vysoké riziko pre bezpečnostné záujmy SR. Tým výraznejšia je potreba prijať reguláciu, ktorá by takéto organizácie regulovala, ak nie vyslovene zakázala. Aktuálna právna úprava v podobe zákona o združovaní občanov je nepostačujúca, nakoľko sa vzťahuje len na združenia s právnou subjektivitou. Inšpiráciou môže byť český zákon č. 14/2021 Sb.

Naopak v oblasti preverovania zahraničných investícií bol v ostatnom období dosiahnutý významný pokrok reprezentovaný prijatím zákona č. 497/2022 Z. z. o preverovaní zahraničných investícií, ktorý v nadväznosti na európske štandardy komplexne upravuje problematiku investícií z tretích krajín, osobitne v tzv. kritických odvetviach.

Najvýraznejšou oblasťou hybridných hrozieb sú už dlhodobo dezinformácie. Preto sme možnostiam postihovania šírenia dezinformácií venovali osobitnú pozornosť. Zamerali sme sa pritom na administratívnoprávnú, ako aj trestnoprávnú rovinu. V administratívnoprávnej rovine bolo v minulosti efektívnym nástrojom blokovanie podľa § 27b ZKB, avšak toto opatrenie vzhľadom k okolnostiam (snaha o ochranu informačného priestoru ako bezprostredná reakcia na vojenskú inváziu Ruskej federácie na Ukrajinu a s tým súvisiace šírenie dezinformácií), za ktorých bolo relatívne rýchlo prijaté, vykazovalo viaceré nedostatky najmä procesného charakteru. Napriek predloženému návrhu novely ZKB, ktorá viaceré nedostatky inštitútu blokovania odstraňovala, právna úprava ostala bez zmeny a tak je v súčasnosti tento nástroj neaplikovateľný. Rovnako tak je problematická aplikácia konania o zamedzení šírenia nelegálneho obsahu podľa zákona o mediálnych službách. Samotné dezinformácie totiž nie sú legálne definované a nespádajú pod pojem nelegálny obsah (hoci niektoré dezinformácie môžu predstavovať nelegálny obsah, napr. pokiaľ by propagovali vojnu). Aplikovateľnosť zákona o mediálnych službách je obmedzená na poskytovateľov služieb podliehajúcich slovenskému právu, teda v zásade poskytovateľov, ktorí majú sídlo, alebo organizačnú zložku na území SR. Na celosvetovo známe služby ako Facebook, či Youtube sa vzťahuje Akt o digitálnych službách, ktorý je priamo záväzný pre všetky subjekty pôsobiace v EÚ.

Osobitne citlivo je potrebné pristupovať k úvahám o možnostiach trestnoprávneho postihu šírenia dezinformácií. Vyvodzovanie trestnoprávnej zodpovednosti by malo byť prípustné len v tých najzávažnejších prípadoch, v súlade s požiadavkou subsidiarity trestnej represie. Za tým účelom je potrebné kategorizovať dezinformácie podľa stupňa nebezpečnosti na základe kritérií ako nepravdivosť resp. skreslenosť, účel získať prospech, spôsobilosť ohroziť chránené záujmy a najmä strategické šírenie, obzvlášť s pôsobením prvku cudzej moci. Samotný prvok spáchania skutku v spojení s cudzou mocou, alebo cudzím činiteľom predstavuje užitočné diferenciačné kritérium odlišujúce „bežnú“ trestnú činnosť od „hybridnej“ aj v iných oblastiach ako dezinformáciách – napr. pri korupcii, kybernetických útokoch. Za tým účelom by bolo vhodné presadiť už skôr navrhovanú zmenu a presunúť znak spáchania činu v spojení s cudzou mocou alebo cudzím činiteľom z režimu všeobecne prirážajúcich okolností medzi závažnejšie spôsoby konania a zároveň doplniť znak závažnejší spôsob konania ako okolnosť podmieňujúcu použitie vyššej trestnej sadzby do tých skutkových podstát aplikovateľných v súvislosti s hybridnými hrozbami, v ktorých sa tento znak doposiaľ nenachádza (šírenie poplašnej správy, podplácanie, prijímanie úplatku).

Zdroje

1. BAYER, J. et. al. 2019 Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States. SSRN Electronic Journal. [online] [cit. 22.6.2022] Dostupné na: <https://doi.org/10.2139/ssrn.3409279>
2. BURDA, E. a kol. 2010. Trestný zákon. Osobitná časť. Komentár – II. diel. Bratislava: C. H. Beck, 1567 s. ISBN 978-80-7400-394-3.
3. ČENTÉŠ, J. a kol. 2016. Trestný zákon. Veľký komentár. 3. vyd. Bratislava: Eurokódex, 959 s. ISBN 978-80-8155-066-9.
4. Kol., 2023. Hĺbková analýza zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám. CBHH ISBA MV SR, 69 s. [online] Dostupné na https://www.hybridnehrozby.sk/wp-content/uploads/2023/08/CBHH_analyza_final_web.pdf
5. MARKOVÁ, V., STRÉMY, T., 2019. Trestné právo hmotné. Všeobecná časť. Plzeň: Aleš Čeněk, 283 s. ISBN 978-80-7380-771-9.
6. Nález ÚS SR zo dňa 22.1.2014 sp. zn. PL. ÚS 5/2012.
7. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách)
8. Ó FATHAIGH, R., HELBERGER, N., APPELMAN, N. (2021). The perils of legally defining disinformation. In: Internet Policy Review, 10(4). [online] Dostupné na: <https://doi.org/10.14763/2021.4.1584>
9. Rozsudok ESLP vo veci Salov proti Ukraine zo dňa 27.4.2004.
10. Rozsudok ESLP vo veci Brzeziński proti Poľsku zo dňa 25.7.2019.
11. Rozsudok ESLP vo veci OOO Flavus a ďalší proti Rusku zo dňa 23.6.2020.
12. ŠAMKO, P. Slovenské cúvanie z demokracie cenzúrou internetu (pôjde Slovensko pri blokovaní webových stránok tureckou cestou?). [online] Dostupné na: <http://www.pravnelisty.sk/clanky/a1071-slovenske-cuvanie-z-demokracie-cenzurou-internetu-pojde-slovensko-pri-blokovani-webovych-stranok-tureckou-cestou>
13. Uznesenie Vlády SR č. 803/2020 Bezpečnostná stratégia Slovenskej republiky.
14. Uznesenie Vlády SR č. 235/2022 Akčný plán koordinácie boja proti hybridným hrozbám na roky 2022 až 2024.

15. VAN HOBOKEN, J. et. al., 2019. The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising [Report]. Dutch Ministry of Interior and Kingdom Relations [online]
https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf
16. VAN HOBOKEN, J., Ó FATHGAIGH, R. Regulating Disinformation in Europe: Implications for Speech and Privacy. In: UC Irvine Journal of International, Transnational, and Comparative Law, roč. 6 (2021), č. 1. [online] Dostupné na:
<https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1041&context=ucijil>
17. Zákon č. 83/1990 Zb. o združovaní občanov
18. Zákon č. 300/2005 Z. z. Trestný zákon
19. Zákon č. 68/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
20. Zákon č. 264/2022 Z. z. o mediálnych službách
21. Zákon č. 497/2022 Z. z. o preverovaní zahraničných investícií a o zmene a doplnení niektorých zákonov.
22. Zákon č. 14/2021 Sb. o nakládání se zbraněmi v některých případech ovlivňujících vnitřní pořádek nebo bezpečnost České republiky

KULTÚRA ORGANIZÁCIE VEREJNEJ SPRÁVY A JEJ VÝZNAM PRE PROBLEMATIKU HYBRIDNÝCH HROZIEB

Mgr. Martin Kaščák, PhD.

Katedra informatiky a manažmentu Akadémie Policajného zboru v Bratislave; Sklabinská 1, 831 06 Bratislava;
martin.kascak@akademiapz.sk

Abstrakt: Zámerom článku je prispieť k zvyšovaniu odolnosti zamestnancov verejnej správy voči hybridným hrozbám. V úvodnej časti sú stručne analyzované základné pojmy a následne metódy na zvyšovanie odolnosti zamestnancov verejnej správy voči hybridným hrozbám. Druhá časť sa zameriava na úlohy a vplyv manažmentu na kultúru a subkultúru organizácie verejnej správy. V závere sa autor venuje významu ďalšieho vzdelávania, ako dôležitého faktora rozvoja osobnostnej integrity zamestnanca verejnej správy. Príspevok sa opiera o výsledky vedeckého výskumu realizovaného v rámci dizertačnej práce autora.

Kľúčové slová: kultúra organizácie 1, manažment 2, verejná správa 3 Policajný zbor SR 4, etický kódex 5, ďalšie vzdelávanie 6, kritické myslenie 7.

1. KULTÚRA ORGANIZÁCIE

„Kultúra organizácie zahŕňa hodnoty, normy, presvedčenia, postoje a predpoklady, ktoré nemusia byť nijako vyjadrené, ale rozhodne určujú spôsob správania sa ľudí aj spôsob vykonávania práce.“ (1, s. 164) Hodnoty a normy ovplyvňujú komunikáciu, spoluprácu a riešenia konfliktov medzi zamestnancami. Kultúra organizácie definuje jej identitu, čiže to, ako organizácia vníma samu seba a ako ju vnímajú jej zamestnanci, zákazníci a verejnosť. Kultúrou organizácie je aj to, ako ľudia komunikujú v rámci organizácie. Môže zahŕňať spôsob, akým sa informácie šíria, ako sa overujú a ako je zaužívané kritické myslenie. Najdôležitejšie je to, ako organizácia reaguje na zmeny a výzvy. Silná a zdravá kultúra prispieva k úspešnému prispôbeniu sa zmenám a čeleniu výzvam, zatiaľ čo konfliktná kultúra môže narušiť výkonnosť organizácie.

Ak chceme definovať kultúru organizácie verejnej správy, musíme vychádzať z jej poslania a úloh. Pod pojmom verejná správa rozumieme poskytovanie verejných služieb ako sú bezpečnosť, zdravotná starostlivosť, vzdelávanie, infraštruktúra a mnoho ďalších. Ich efektívne plnenie je kľúčom k spravodlivej, demokratickej a funkčnej spoločnosti. Jednou z najdôležitejších úloh je aplikácia zákonov a ďalších právnych noriem. Z uvedeného vyplýva, že poslaním verejnej správy je predovšetkým služba občanom a jej úlohy sa zameriavajú na zachovanie poriadku a bezpečnosti v štáte. V prípade Policajného zboru ide predovšetkým o ochranu práv a slobôd občanov, ktoré sú bazálnymi hodnotami demokracie. Lakonicky to vyjadril prof. Luknič „Polícia je jednou zo zložiek trestného systému, ktorého základnou úlohou je chrániť slobodu užívania si ústavných práv občanov.“ (2, s. 69)

1.1 Etický kódex

Kultúra organizácie verejnej správy sa zakladá na etike, integrite, ale aj na spoľahlivosti a trvalej kontinuite. Etický kódex je významným nástrojom pre zabezpečenie integrity a dôveryhodnosti verejnej správy a pre zachovanie dôvery občanov vo verejný sektor. V etickom kódexe štátneho zamestnanca sú vyjadrené hodnoty organizácie verejnej správy. „Etické správanie štátnych

zamestnancov je dôležitým faktorom pre fungovanie právneho štátu, ochranu ľudských práv a základných slobôd a dôveru v štát a orgány verejnej moci. Štátny zamestnanec pracuje v štátnozamestnaneckom pomere pre štát a reprezentuje jeho inštitúcie. Svojim konaním a správaním vplýva na dôveru verejnosti. Nielen jeho odborné kvality, ale aj dodržiavanie etických požiadaviek sú zárukou riadneho výkonu štátnej služby.“ (3) Ak sa štátny zamestnanec nevhodne vyjadruje, alebo šíri neoverené informácie, znižuje tým dôveru občanov v organizácie verejnej správy. Neoverené správy môžu spôsobiť veľké škody, ako napríklad rozšírenie paniky, nebezpečného správania sa alebo dezinformovanie verejnosti. Môže ísť o informácie o zdravotných hrozbách, politických udalostiach alebo o iných dôležitých témach. Zamestnanci verejnej správy by mali zodpovedne pristupovať k tomu, čo zverejnia, alebo poskytnú ďalej. Dôležité je, aby si overili pôvod informácie a pokiaľ je to možné aj pravdivosť podozrivej správy z iných zdrojov.

Viaceré etické kódexy štátneho zamestnanca ako aj zamestnanca vykonávajúceho práce vo verejnom záujme uvádzajú, že: „zamestnanec nezadržiava informácie, ktoré majú byť riadne zverejnené a neposkytuje informácie, o ktorých vie, že sú nesprávne alebo zavádzajúce.“ (4) Pre objektívne posúdenie správnosti informácií je potrebné kritické myslenie. Ide o schopnosť premýšľať racionálne, analyticky a nezaujať na základe faktov a argumentov. Je to kľúčová zručnosť, ktorá umožňuje rozpoznať chyby v argumentoch, identifikovať nesprávne dedukcie, nekonzistentné a zavádzajúce tvrdenia. Na druhej strane je potrebné taktiež vedieť prehodnotiť svoje vlastné názory, ak ich nové informácie a argumenty vyvracajú. To znamená, byť otvoreným k novým postojom a robiť zmeny, ak sú odôvodnené. Kritické myslenie je zručnosť, ktorá sa dá rozvíjať a zdokonaľovať prostredníctvom vzdelávania a kurzov.

1.2 Zvyšovanie odolnosti zamestnancov verejnej správy voči hybridným hrozbám

Zvyšovanie odolnosti zamestnancov verejnej správy voči hybridným hrozbám vyžaduje komplexný a trvalý prístup, ktorý zahŕňa ďalšie vzdelávanie, technologické opatrenia ako aj zlepšené kritické myslenie. Cieľom je zvýšiť schopnosť zamestnancov odolávať rozmanitým bezpečnostným hrozbám, ktoré kombinujú viaceré aspekty.

Ďalšie vzdelávanie zamestnancov verejnej správy by malo byť iniciované vrcholovým manažmentom. Realizovať by sa malo na základe identifikácie vzdelávacích potrieb, z ktorých vyplynie objektívna potreba konkrétnych vzdelávacích programov. Po ich realizácii je nevyhnutné vyhodnotenie výsledkov, na základe ktorých sa môže pristúpiť ku korekciám v ďalšom cykle vzdelávania. Zároveň by sa mali každoročne prehodnocovať vzdelávacie programy z hľadiska neustáleho vývoja v súlade s meniacimi sa potrebami a technológiami. Kurzy ďalšieho vzdelávania však musia byť blízke praxi a poskytované rôznymi i netradičnými spôsobmi, aby boli pre zamestnancov prítiahľivé, ako napríklad metódou zameranou na praktický nácvik naučeného „action learning“. (5)

Ďalšie vzdelávanie je zároveň cestou k pochopeniu podstaty hybridných hrozieb a ich identifikácií zamestnancami verejnej správy. Ide o schopnosť organizácií, spoločenstiev a štátov reagovať a brániť sa pred rozmanitými hrozbami, ktoré zahŕňajú vojenské, nevojenské, kybernetické, informačné a politické prostriedky. Tieto hrozby môžu byť páchané štátmi alebo neštátnymi subjektami a môžu mať vážne dôsledky na bezpečnosť a stabilitu štátu i regiónu. (6) Pre odolnosť voči hybridným hrozbám je kľúčové včas ich identifikovať a správne vyhodnotiť stupeň nebezpečenstva. „V súčasnosti evidujeme asi 120 dezinformačných webov v priestore bývalého

Československa a približne 2000 facebookových stránok, pričom uzavreté skupiny už prenikli do všetkých oblastí života.“ (7)

Ďalšou metódou zvyšovania odolnosti zamestnancov verejnej správy voči hybridným hrozbám je „diskusia namiesto zosmiešňovania a nálepkovania názorových odporcov.“ Otvorená argumentácia je zároveň „prevenciou depresie, z ktorej môže vyplynúť sklon k extrémizmu, ale skutočne účinným liekom proti hybridným hrozbám je *strategická komunikácia*.“ (8) „Strategická komunikácia je systematické a koordinované používanie objektívnych informácií verbálnymi a neverbálnymi spôsobmi komunikácie s cieľom naplňať strategické záujmy štátu.“ (6) Strategická komunikácia začína jasne definovanými cieľmi, cieľovou skupinou a vytvorením presvedčivého posolstva šíreného vhodnými formami a komunikačnými kanálmi. Základom je však vysoká odbornosť, nakoľko sa často používa na presadzovanie konkrétnych posolstiev a postojov.

2. VPLYV MANAŽMENTU NA KULTÚRU ORGANIZÁCIE

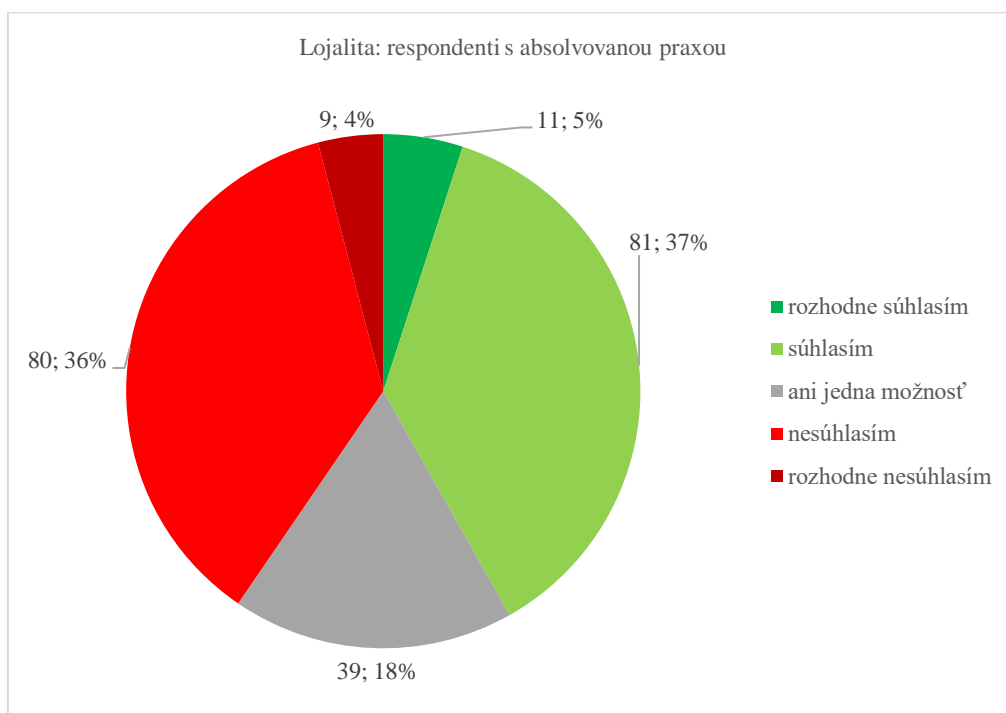
Michael Armstrong vo svojej monografii pojednáva o zásadnom vplyve manažérov na kultúru organizácie: „nezáleží na tom, či boli hodnoty organizácie nejako vyjadrené. Implicitné, teda priamo nevyjadrené a samo sebou sa rozumejúce hodnoty, ktoré sa hlboko zakorenili v kultúre organizácie a sú posilňované správaním sa manažérov, môžu mať významný vplyv, zatiaľ čo výslovne prijaté a verejne presadzované hodnoty, ktoré však zostávajú samotnými slovami a neprejavujú sa v správaní manažérov, majú obyčajne malý alebo nemajú dokonca žiadny vplyv.“ (1, s. 166)

Časť výskumu bývalej psychologickej a sociologickej služby MV SR a inšpekcie MV SR sa dotýkal aj vplyvu manažmentu na kultúru organizácie Policajný zbor Slovenskej republiky. Zistenia, ku ktorým dospeli súhrne vymedzujú päť objektívnych príčin kriminality policajtov, pričom „tri z nich sú spôsobené nesprávnymi postupmi manažérov (nadriadených) páchatel'ov kriminality.“ (9, s. 144) Zároveň sa dopracovali k záveru, že „so vzťahmi k nadriadeným je nespokojných 73,3% policajtov.“ (9, s. 145)

Znepokojujúce výsledky čiastočne podopiera aj výskum v rámci dizertačnej práce autora. Realizovaného výskumu sa zúčastnilo 106 osôb zo strednej odbornej školy Policajného zboru, pričom 88 odpoved'ových hárkov splnilo metodologickú podmienku konzistentnosti odpovedí. Z toho bolo 28 osôb z vekovej kategórie 18 – 21 rokov, 45 osôb z kategórie 21 – 30 rokov a 15 osôb z kategórie 30+. Počet respondentov bez absolvovania praxe bol 33 osôb a respondentov s absolvovanou praxou bolo 55. Príslušníkov Policajného zboru bolo 51 a kadetov Policajného zboru 37, z toho 30 žien a 58 mužov. Respondenti mali možnosť zaujať postoj na škále *rozhodne nesúhlasím – nesúhlasím – súhlasím - rozhodne súhlasím - ani jedna možnosť*. Ich postoje boli v rámci vyhodnotenia oznámkované ako v škole na stupnici 1 – 5. V praxi to znamená, že ak by všetci respondenti odpovedali, že rozhodne súhlasia, alebo rozhodne nesúhlasia priemer ich odpovedí by bol M 1,00, alebo M 5,00. V uvedenom výskume policajní študenti väčšinou *súhlasili* alebo *rozhodne súhlasili* s týmto prehlásením: „Keď si pomyslím na úplatných vysokopostavených policajných funkcionárov, som z toho skutočne znechutený/á.“ M 2,02 pri SD 0,97 („M“ je skratka pre priemer odpovedí, SD je rozptyl odpovedí *Standard Deviation*) (10)

Vyššie uvedený výskum nebol zameraný na odolnosť voči hybridným hrozbám, ale v kontexte predmetnej témy priniesol závažné poznatky o vplyve útvarej subkultúry na kultúru organizácie

Policajný zbor Slovenskej republiky. Subkultúra má vlastné normy a hodnoty. Formuje sa na základe spoločných postojov, ktoré sa líšia od kultúry organizácie Policajný zbor. V anglosaských krajinách sa používa pojem „Police Canteen-culture“. (11) Prof. Luknič vo svojej monografii uvádza, že americký výskum o morálnej dimenzii policajnej práce (H. Cohen, 1986) ukázal, že „hlavným argumentom odôvodňujúcim prijímanie úplatkov políciou nie je to, že morálne slabí jednotlivci vstupujú do radov polície. Výsledky podporujú skôr ten argument, že príslušníci polície sa učia jeden od druhého“. (2, s. 30) Napriek tomu, že kvôli opatreniam na zamedzenie šírenia vírusu covid-19 sa mnohí respondenti zúčastnili namiesto trojtýždňovej praxe len jedného alebo dvoch týždňov praxe, vo všetkých ukazovateľoch zastávali študenti s praxou negatívnejšie postoje v porovnaní s tými, ktorí ešte žiadnu prax neabsolvovali. Tú istú tendenciu zachytil aj náš predvýskum na vzorke 44 študentoch. Najviac negatívnych postojov zaznamenal výskum u manifestných premenných č. 3., 7., 11. a 28. situujúcich konflikt lojality k zákonom a etickým predpisom voči lojalite ku kolegom a priateľom. Uvedené premenné poukazujú na latentnú premennú policajná subkultúra ako na veľmi významne pôsobiaci fenomén, ktorému je potrebné venovať zvýšenú pozornosť. Až 40 % odpovedí bolo *nesúhlasných* alebo *rozhodne nesúhlasných* s uprednostnením zákonných a etických noriem pred kolegiálnosťou. Len 5 % postojov respondentov vyjadrovalo *rozhodný súhlas* s lojalitou k zákonu a služobnej etike pred kolegami. Ďalším mementom je najvyššie percentuálne zastúpenie nerozhodných odpovedí (18 %) v rámci celého výskumu. Tento ukazovateľ môže naznačovať pomerne vysoké zneistenie študentov po absolvovaní praxe a možný príklon v budúcnosti od nerozhodnutých k lojalite ku kolegom, čo by už znamenalo nadpolovičnú väčšinu zaujatých postojov v neprospech dodržiavania noriem. (10, s. 86 - 87)



Zdroj: (10, s. 86)

Graf číslo 1 sumarizuje odpovede (prvá číslica uvádza počet odpovedí; druhá ich percentuálny podiel) na korelujúce prehlásenia č. 3., 7., 11. a 28., ktoré vystavili respondentov do konfliktu

lojality k zákonom a etickým normám, voči lojalite ku kolegom a priateľom: „Kto oznámi nadriadenému svojho kolegu, ktorý porušil etické normy, je zradca - slangovo bonzák.“ (M 2,88; SD 1,17) „Keď vidím, ako často policajti tolerujú porušovanie etických (často aj zákonných) noriem u druhých policajtov (falošná kolegiálnosť), trápi ma to.“ (M 2,55; SD 1,01) „Keby som sa dozvedel/a, že niekto na útvare konal v rozpore s etickými normami, patrične by som nahlásil/a previnenie kolegu - policajta.“ (M 3,10; SD 0,94) „Keby som sa dozvedel/a, že kolega - dobrý priateľ konal v rozpore so zákonom, nekonal/a by som v súlade so zákonom a neprezradil/a by som ho.“ (M 3,02; SD 1,02) (10, s. 75 - 76)

Ďalšie výskumy venujúce sa falošnej kolegiálnosti prinášajú veľmi podobné výsledky. Napríklad výskum v Českej republike o falošnom kamarátstve priniesol výsledky, podľa ktorých „podvádzanie (našepkávanie kamarátom) v škole takmer 40% budúcich pedagógov označilo za konanie *čestné* alebo *skôr čestné* a len necelých 7% toto správanie jednoznačne označilo ako *nečestné*!“ (12, s. 11)

ZÁVER

V príspevku sme sa snažili priblížiť kruciálnu úlohu manažmentu pri vplyve na kultúru organizácie verejnej správy. Od nej totiž záleží, ako budú zamestnanci vystupovať na verejnosti, ako si osvoja zásady kritického myslenia a ako budú odolní voči hybridným hrozbám. Nie je to však priamy, automatický vplyv. Ako sme ukázali, rozhodujúce sú postoje samotného manažmentu, ako vzoru a príkladu pre svojich zamestnancov, a to nie len slovami, ale predovšetkým činmi. Pre účinnosť pôsobenia manažérov na všetkých stupňoch riadenia je potrebné splniť predovšetkým základnú podmienku vyjadrenú v nasledujúcom lapidárnom bonmote „To kým ste kričíte z vás tak hlasno, že nepočujem čo hovoríte.“ (R. W. Emerson).

Výskumy (2), (9), (10), (12) však poukazujú na to, že ani to nemusí stačiť. V rámci organizácie, paralelne s jej kultúrou, totiž môže pôsobiť neformálna kultúra zamestnancov označovaná za subkultúru. V skutočnosti ide o *nekultúru* (13), pretože okrem priateľských zásad vzájomnej pomoci, zahŕňa aj „zásady“, ktoré majú uprednostňovať falošnú kolegiálnosť pred adekvátnym úradným postupom. Na niektorých úradoch sa časom zaužíva aj zľahčovanie si povinností či obchádzanie zákonných a etických noriem. Takáto subkultúra sa môže odovzdávať z generácie na generáciu, pretože novoprichádzajúci zamestnanci sa snažia predovšetkým prispôbiť existujúcej kultúre.

Východiskom z tejto situácie je vedomé utváranie kultúry organizácie na základe inšpirujúcej vízie, s ktorou sa budú môcť, ale predovšetkým chcieť, stotožniť zamestnanci organizácie. Ciele a hodnoty by mali byť prítiažlivé pre zamestnancov tak, aby boli hrdí na príslušnosť k nej. Môžu byť vyjadrené napríklad v etickom kódexe. Ak má byť etický kódex inšpiratívnym a motivačným dokumentom, nemal by mať záväznosť právnej normy. Mal by ostať etickou normou, aby stelesňoval ideál, ku ktorému môžu zamestnanci vzhliadať. Samozrejme musí byť reálne dosiahnuteľný, inak by strácal motivačnú funkciu. K jeho dosiahnutiu by malo viesť ďalšie vzdelávanie, ktoré by vhodnými formami a metódami pôsobilo na vnútornú motiváciu zamestnancov. V zmysle toho, ako to zhrnul odborník na vzdelávanie docent Pavel Vacek z Katedry pedagogiky a psychológie Univerzity Hradec Králové po mnohých rokoch vedeckej a pedagogickej práce: „V stále väčšej miere sa presadzuje presvedčenie, že najlepšou prevenciou výskytu sociálno-patologických javov je namiesto dominancie reštrikcie a dozoru budovanie

vnútorných zábran v osobnosti práve rozvojom vnútornej morálky prostredníctvom procesu zvnútorňovania pravidiel, noriem a utvárania aktívneho svedomia.“ (12, s. 18)

Zdroje

1. ARMSTRONG, Michael, 2015. *Řízení lidských zdrojů*. Praha: Grada Publishing.
2. LUKNIČ, Arnold, 1999. *Etika v činnosti policajta*. Bratislava: Akadémia Policajného zboru.
3. *Výklad etického kódexu štátneho zamestnanca* [online] [01.01.2020] Dostupné na: https://radaprestatnuszbu.vlada.gov.sk/data/files/7500_eticky-kodex-vyklad-v10.pdf
4. *Vyhláška Úradu vlády Slovenskej republiky ktorou sa vydáva Etický kódex štátneho zamestnanca č. 400/2019 Z. z* [online] [01.01.2020] Dostupné na: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/400/20200101>
5. Michael J. Marquardt, *Action Learning*, Vydavateľstvo Management Press, 2011
6. *Krátky slovník hybridných hrozieb*. [online] [18.03.2021] Dostupné na: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>
7. Ing. Peter Gallo, PhD. FF UJPS, vystúpenie na konferencii *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy*, 5. – 6. 10. 2023, Častá - Papiernička.
8. doc. JUDr. PhDr. Ivo Svoboda, Ph.D., MBA, vystúpenie na konferencii *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy*, 5. – 6. 10. 2023, Častá - Papiernička.
9. ČECH, Ján, 1998. *Úvod do policajnej psychológie*, Bratislava: Tlačiareň MV SR.
10. KAŠČÁK, Martin, 2021. Diz. práca. Fenomén svedomia a jeho význam pre sebareguláciu konania príslušníka Policajného zboru, Bratislava: Akadémia Policajného zboru.
11. WADDINGTON, Peter, 1999. Police (Canteen) Sub-culture. In: *The British Journal of Criminology*. Oxford: University Press.
12. VACEK, Pavel, 2014. Morální gramotnost a proces internalizace mravních norem. In: Kaliský, J., 2014. Dobro a zlo, alebo o morálke I. *Psychologické a filozofické aspekty morálky v edukácii*. (Zborník vedeckých štúdií), Banská Bystrica: PF UMB v Banskej Bystrici. ISBN 978-80-557-0538-5.
13. MURDZA, Karol, 2009. Policajná kultúra. In: *Policajná teória a prax*. roč. XVII, číslo 1, s. 37-48. ISSN 1335-1370.

PRIPRAVENOSŤ KAPACÍT SLOVENSKEJ REPUBLIKY NA ZVÝŠENÝ NÁPOR ŽIADOSTÍ O UDELENIE AZYLU, V KONTEXTE HYBRIDNÝCH HROZIEB SÚVISIACICH S MIGRÁCIOU

Mgr. Juraj Klátik

Migračný úrad Ministerstva vnútra SR, externý doktorand, Katedra kriminálnej polície, Akadémia Policajného zboru v Bratislave, e-mail: juraj.klatik@akademiapz.sk

Abstrakt: Príspevok sa zameriava na analýzu kapacít Slovenskej republiky, zastúpených najmä Ministerstvom vnútra SR, využívaných pri práci s osobami, ktoré žiadajú o udelenie azylu v SR. Nápor migrácie, najmä nelegálnej, sa v uplynulom období v SR zvyšuje. Azylová infraštruktúra Slovenskej republiky je nastavená na objemy žiadateľov o azyl, ktoré reflektujú stav z obdobia pred vypuknutím migračnej krízy v Európe. Kapacity zariadení, ktoré poskytujú svoje služby žiadateľom o azyl v SR sú prispôbené stavu, počas ktorého je Slovensko pre migrantov iba tranzitnou krajinou a počet osôb, ktoré požiadajú na území SR o azyl je nízky. S rastúcou dynamikou pri správe hraníc vo vnútri Schengenského priestoru sa však tento stav môže zmeniť a počet osôb žiadajúcich o udelenie azylu by sa mohol zvýšiť, čo si bude vyžadovať reakciu zo strany kompetentných orgánov. Budovanie kapacít pre prácu s migrantmi je nevyhnutné pre udržanie bezpečnostnej a sociálnej stability na území SR.

Kľúčové slová: azyl, migrácia, hybridné hrozby, azylové zariadenia.

1. HYBRIDNÉ HROZBY A MIGRÁCIA

Hybridné hrozby sa ako pojem dostali do slovníka odbornej a laickej verejnosti iba nedávno, najmä s nástupom využívania digitálnych technológií. Skutočnosťou je, že hybridné hrozby sú späté s ľudskou aktivitou oveľa dlhšie a nejde iba o hackerské útoky, alebo iné škodlivé činnosti realizované v digitálnom prostredí. Podľa definície Národného bezpečnostného úradu (NBU) sa pojem hybridná hrozba vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.²⁰⁰

Jednou z foriem hybridného pôsobenia je aj migrácia obyvateľstva, či už legálna alebo nelegálna. Ohrozenie vyplývajúce z migrácie osôb je najmä v nedostatočnom počte infraštruktúrnych kapacít jednotlivých štátov, ktoré nie sú pripravené na masové návaly migrujúcich osôb po materiálnej, technickej alebo personálnej stránke. Slovenská republika v súčasnosti neeviduje vysoký počet osôb žiadajúcich o azyl, avšak situácia spôsobená nelegálnou migráciou môže tento trend zmeniť. Pripravenosť kapacít SR na zvýšený nápor osôb žiadajúcich o udelenia azylu si rozoberieme v tomto príspevku.

Faktor migrácie prináša pre cieľové krajiny veľké množstvo pozitív. V prípade ak ide o regulovanú migráciu, ktorá pomáha pokryť nedostatky na pracovnom trhu prijímacej krajiny môže ísť dokonca o nutnosť. Vzhľadom na vývoj demografickej krivky v európskom kontexte sa v prípade snahy o zachovanie súčasných ekonomických a sociálnych štandardov našich obyvateľov nevyhne nábore kvalifikovanej pracovnej sily z tretích krajín. Okrem pozitívnych faktorov prináša so sebou

²⁰⁰ Národný bezpečnostný úrad [online]. [cit. 01. októbra 2023]. Dostupné na: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html>

migrácia aj mnoho výziev a najmä bezpečnostných ohrození. V mnohých prípadoch môžeme na základe bližšieho rozboru hovoriť o hybridných hrozbách spôsobených migráciou.

Migrácia osôb a najmä tá nelegálna je považovaná za hybridnú hrozbu na základe javov, ktoré spôsobujú komplikácie pri bežnom spôsobe života v krajine, ktorá je ňou ohrozená. Ide napr. o disbalanciu existujúceho pracovného trhu, rozvoj a diverzifikáciu organizovaného zločinu, ekonomickú nerovnováhu spôsobenú zvýšením aktivít spojených s praním špinavých peňazí z prevádzania migrantov, demografickú nerovnováhu, zvýšenú mieru korupcie medzi úradníkmi alebo narušenú rovnováhu ekonomických investícií zahraničných alebo domácich spoločností.²⁰¹

2. SÚČASNÝ VÝVOJ V SLOVENSKEJ REPUBLIKE

V prvej polovici roku 2023 prekročilo nelegálne štátnu hranicu SR 11 362 osôb, z čoho 10 453 osôb uviedlo ako svoju krajinu pôvodu Sýriu. V porovnaní s prvým polrokom roku 2022 ide o značný nárast, keďže za uvedené obdobie bolo na území SR zaznamenaných 1474 nelegálnych migrantov. Väčšina osôb, ktoré nelegálne prekračujú štátnu hranicu SR uvádza ako krajinu svojho pôvodu Sýriu, čoho následkom je v súčasnosti nemožnosť ich vyhostenia²⁰².

Väčšina z týchto osôb využíva SR iba ako tranzitnú krajinu a nerozhodnú sa požiadať tu o azyl. Podľa štatistík požiadalo o udelenie azylu v SR v priebehu roka 2022 spolu 547 osôb, z čoho bol 23 osobám udelený azyl, 48 osobám bola udelená doplnková ochrana a v 76 prípadoch bolo vydané negatívne rozhodnutie. V priebehu azylového konania prišlo k jeho zastaveniu v 387 prípadoch. V prípade zastavenia azylového konania v podmienkach SR je spravidla dôvodom svojvoľné opustenie územia SR zo strany žiadateľa o azyl.²⁰³ Stav v ktorom väčšina nelegálnych migrantov pokračuje ďalej do krajín západnej Európy, sa však vzhľadom na okolnosti môže časom zmeniť, pričom môže nastať situácia, počas ktorej požiada v SR o udelenie azylu zvýšené množstvo nelegálnych migrantov. Následkom takéhoto javu môže nastať krízová situácia v zariadeniach, ktoré poskytujú svoje služby žiadateľom o udelení azylu.

Zodpovedným orgánom v oblasti azylovej politiky v podmienkach SR je migračný úrad Ministerstva vnútra SR. Migračný úrad zodpovedá za prijímanie žiadateľov o azyl, po tom ako cudzinec urobí vyhlásenie, že žiada o udelenie azylu na policajnom útvare. Migračný úrad ďalej zodpovedá aj za organizáciu azylových zariadení v SR, ako aj rozhodovanie o žiadostiach o udelenie azylu a následnú integráciu osôb s udelenou medzinárodnou ochranou.

V súčasnosti poskytuje migračný úrad svoje služby pre žiadateľov o azyl v troch zariadeniach. V záchytnom tábore v Humennom s kapacitou 500 osôb. Ide o kolektívny záchytný tábor, resp. kolektívne tranzitné azylové zariadenie. V súčasnej dobe sa zariadenie využíva aj na ubytovanie osôb so statusom dočasného útočiska. Spolu so žiadateľmi o azyl je v Humennom momentálne

²⁰¹ TARNU L. Threats and risks generated by illegal migration flows and their control. Scientific Bulletin Vol.XX, No2, 2015. [online]. [cit. 01.10.2023]. Dostupné na:

https://www.researchgate.net/publication/296692953_Threats_and_Risks_Generated_by_Illegal_Migration_Flows_and_Their_Control

²⁰² Štatistický prehľad legálnej a nelegálnej migrácie cudzincov na Slovensku[online]. [cit. 01.10.2023]. Dostupné na: <https://www.minv.sk/?rok-2023-2>

²⁰³ Štatistický prehľad migračného úradu MV SR [online]. [cit. 01.10.2023]. Dostupné na: <https://www.minv.sk/?statistiky-20>

umiestnených 55 osôb. Pobytový tábor v Opatovskej Novej Vsi slúži najmä na umiestňovanie rodín s deťmi a zraniteľných skupín žiadateľov o azyl a jeho kapacita je 140 osôb. V súčasnosti využíva toto zariadenie spolu 33 klientov. Tretím zariadením je pobytový tábor v Rohovciach určený primárne pre dospelých mužov, ktorý sa na území SR zdržiavajú samostatne. Kapacita tohto zariadenia je 140 osôb a v súčasnosti ho využíva 17 klientov. Okrem uvedených zariadení určených primárne pre žiadateľov o azyl prevádzkuje migračný úrad aj Humanitné centrum v Gabčíkove, ktoré je určené pre ľudí utekajúcich pred vojnou na Ukrajine so štatútom odídencu. Kapacita humanitného centra je 1000 osôb a v súčasnosti jeho služby využíva 729 klientov. Toto zariadenie je však v súkromnom vlastníctve a Ministerstvo vnútra SR si priestory humanitného centra iba prenajíma. Spolu má momentálne migračný úrad MV SR k dispozícii ubytovanie pre 1780 osôb, obsadených je 834 lôžok a ostáva 946 voľných lôžok. Ak berieme do úvahy iba zariadenia vo vlastníctve Ministerstva vnútra SR, tak v súčasnosti ostáva voľných 675 lôžok pre prípadných žiadateľov o udelenie azylu.²⁰⁴ Podľa oficiálnych údajov MV SR bolo v prvom polroku na území SR zachytených 11 362, ktoré nelegálne prekročili štátnu hranicu. Podľa mediálnych vyjadrení predstaviteľov MV SR ich bolo na konci septembra 2023 viac ako 30 000. Ak vezmeme do úvahy, že Slovenská republika disponuje približne 600 miestami pre žiadateľov o azyl, ide o značný nepomer. Zodpovední predstavitelia štátu sa spoliehajú na fakt, že doteraz bola Slovenská republika vnímaná najmä ako tranzitná krajina. Súčasný vývoj bezpečnostnej politiky okolitých štátov v súvislosti so zavádzaním hraničných kontrol vo vnútri Schengenského priestoru však môže zmeniť status SR z tranzitnej krajiny na krajinu, v ktorej sa nelegálni migranti rozhodnú požiadať o udelenie azylu. Analýza súčasných kapacít azylových zariadení ukázala, že SR na takýto nápor vôbec nie je pripravená.

V minulosti boli v prevádzke viaceré azylové zariadenia, ktoré boli vzhľadom na nízku vyťaženosť časom zatvorené. Ide o záchytné tábory Adamov-Gbely, a Vlachy, ktoré boli zrušené a v súčasnosti sa na účely záchytného tábora využíva zariadenie v Humennom. Na účely pobytového tábora slúžilo zariadenie v Brezovej pod Bradlom, ktorý bol špeciálne vybavený pre zraniteľné skupiny, s bezbariérovými vstupmi do miestností, špeciálnymi zdravotnými pomôckami, oddychovou zónou vo vnútri zariadenia a pod. Tento tábor však v septembri 2006 vyhorel a v súčasnosti je zatvorený.²⁰⁵

3. NÁVRHY OPATRENÍ

Jedným z návrhov ako zlepšiť pripravenosť kapacít SR na prípadný zvýšený nápor žiadateľov o azyl je obnovenie, resp. vybudovanie nových zariadení určených pre žiadateľov o azyl. Pre lepšiu efektivitu využitia a finančnú návratnosť by mohli takéto zariadenia fungovať v tzv. hybridnom režime. To znamená, že tieto objekty by boli primárne zriadené na účel poskytovania služieb žiadateľom o azyl. V prípade, ak by bol počet žiadateľov o azyl v SR nízky a na ich umiestnenie by postačovali súčasné kapacity, mohol by sa účel využitia zariadenia zmeniť a jeho priestory a služby by mohli využívať samosprávy, záujmové združenia občanov, právnické alebo fyzické osoby na svoje aktivity, pričom so zvýšeným počtom žiadateľov o azyl v SR by sa účel využitia zariadenia opäť zmenil na poskytovanie služieb žiadateľom o azyl. Tento proces by si vyžadoval

²⁰⁴ Údaje Migračného úradu MV SR

²⁰⁵ MICHALKOVÁ M. Organizácia azylových zariadení pre žiadateľov o azyl v Slovenskej republike, Bratislava, 2013

úzku kooperáciu všetkých zúčastnených subjektov a to najmä medzi orgánmi štátu a subjektmi, ktoré by využívali zariadenie v prípade, ak by zrovna nebolo určené pre žiadateľov o azyl v SR.

Ďalším návrhom na zlepšenie efektivity absorbovania zvýšeného počtu žiadateľov o azyl je upraviť povinnosti žiadateľov podľa §23 zákona č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov. Odsek 6 tohto paragrafu v súčasnosti žiadateľa obmedzuje pri vstupe do pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu, alebo podnikaní. Oprávňuje však žiadateľa vstupovať do pracovnoprávneho vzťahu po šiestich mesiacoch od začatia konania okrem explicitne vymedzených prípadov. Navrhujeme znížiť obdobie, počas ktorého je žiadateľ obmedzený pri vstupe na trh práce zo šiestich mesiacov na tri mesiace. Dôvodom je zvýšený dopyt trhu práce v SR po pracovnej sile, z dôvodu vysokého množstva voľných pracovných miest. Obmedzenie prístupu na trh práce má zároveň negatívny vplyv na psychiku žiadateľa o azyl, pričom zjednodušenie jeho prístupu ku zamestnaniu by pomohlo pri jeho seberealizácii a zoznamovaní sa s prostredím v SR. Priamo na proces zlepšenia dostupnosti uplatnenia na trhu práce pre žiadateľov o azyl nadväzuje ďalší návrh na zmenu zákona o azyle, konkrétne v §22, ods.2, písm. b, kde je uvedené, že ministerstvo môže povoliť žiadateľovi pobyt mimo pobytového tábora na základe jeho písomnej žiadosti najviac na tri mesiace, a to aj opakovane, ak štátny občan Slovenskej republiky s trvalým pobytom na území Slovenskej republiky alebo cudzinec s udeleným pobytom na území Slovenskej republiky predloží písomné čestné vyhlásenie o tom, že zabezpečí ubytovanie žiadateľa a úhradu všetkých výdavkov spojených s jeho pobytom na území Slovenskej republiky.²⁰⁶ V tomto ustanovení navrhujeme doplniť výpočet subjektov, ktoré môžu predložiť uvedené písomné vyhlásenie o právnické osoby. Z praktického hľadiska by išlo najmä o firmy, ktoré by žiadateľom o azyl poskytli prácu a súčasne by im mohli poskytovať aj ubytovanie. Výsledkom by bolo odľahčenie kapacitného náporu na azylové zariadenia prevádzkované Ministerstvom vnútra SR.

Na záver môžeme konštatovať, že situácia v súvislosti s migráciou osôb v Európe je dlhodobou dynamická a jednotlivé faktory, ktoré na tento proces vplyvajú sa neustále menia. Je naivné sa domnievať, že Slovenská republika bude naveky iba tranzitnou krajinou pre nelegálnych migrantov. Z tohto dôvodu je nevyhnutné akútne posilnenie kapacít v oblasti azylovej politiky. V priebehu posledných rokov zasiahlo Slovenskú republiku niekoľko kríz, pričom ani na jednu z nich sme ako krajina neboli pripravení. Skúsme sa z týchto skúseností poučiť a začať budovať preventívne opatrenia na zamedzenie momentu prekvapenia pri ďalšej kríze, ktorá je vzhľadom na geopolitický vývoj bližšie ako by sme predpokladali.

Zdroje

1. MICHALKOVÁ M. Organizácia azylových zariadení pre žiadateľov o azyl v Slovenskej republike, Bratislava, 2013, ISBN: 978-80-89506-38-5
2. Národný bezpečnostný úrad [online]. [cit. 01. októbra 2023]. Dostupné na: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html>
3. Štatistický prehľad legálnej a nelegálnej migrácie cudzincov na Slovensku, [online]. [cit. 01.10.2023]. Dostupné na: <https://www.minv.sk/?rok-2023-2>

²⁰⁶ Zákon č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov

4. Štatistický prehľad migračného úradu MV SR [online]. [cit. 01.10.2023]. Dostupné na:
<https://www.minv.sk/?statistiky-20>
5. TARNU L. Threats and risks generated by illegal migration flows and their control. Scientific Bulletin Vol.XX, No2, 2015. [online]. [cit. 01.10.2023]. Dostupné na:
https://www.researchgate.net/publication/296692953_Threats_and_Risks_Generated_by_Illegal_Migration_Flows_and_Their_Control
6. Údaje Migračného úradu MV SR
7. Zákon č. 480/2002 Z. z. o azyle a o zmene a doplnení niektorých zákonov

PODPORA BEZPEČNÉHO TESTOVANIA V DISTRIBUOVANÝCH REAKTÍVNYCH SYSTÉMOCH ZALOŽENÁ NA IDENTIFIKÁCIÍ DIAGRAMOV SEKVENCÍÍ

Bc. Viktor Klíma, doc. Ing. Ján Lang, PhD.

Slovenská technická univerzita v Bratislave, Fakulta informatiky a informačných technológií, Ústav informatiky, informačných systémov a softvérového inžinierstva, Ilkovičova 6276/2, 842 16 Bratislava 4, xklimav@stuba.sk, jan.lang@stuba.sk

Abstrakt: Tento článok predstavuje komplexný prehľad identifikovaných problémov súvisiacich so súbežnými a distribuovanými systémami, staršími, alebo viacvláknovými systémami a asynchrónnymi reaktívnymi programami potenciálne aj v kontexte zvyšovania odolnosti voči hybridným hrozbám. Problémy sú zoskupené, pričom skupiny zahŕňajú problémy súvisiace s generovaním testovacích prípadov z modelov UML, problémy súvisiace s reverzným inžinierstvom UML sekvenčných diagramov a pod. Pre každú skupinu sa diskutuje o navrhovaných riešeniach vrátane algoritmu na generovanie testovacích prípadov založených na modeloch UML a algoritmu reverzného inžinierstva na generovanie sekvenčných diagramov UML. Okrem toho sa navrhuje riešenie zahŕňajúce injektovanie chýb a algoritmy generovania testovacej sekvencie na detekciu porúch v asynchrónnych reaktívnych programoch ako príklad simulácie potenciálneho ohrozenia. Načrtnuté sú hypotézy na vyhodnotenie účinnosti navrhovaných riešení, vrátane hypotéz týkajúcich sa pokrytia testovacieho prípadu, presnosti sekvenčného diagramu a miery detekcie chýb pre zvýšenie odolnosti analyzovaného systému. Navrhujú sa hodnotiace metriky, ako je pokrytie testovacieho prípadu, presnosť, spomínanie, skóre F1 a miera detekcie chýb, ktoré by sa použili na meranie výkonu navrhovaných riešení aj v kontexte zvyšovania odolnosti voči hybridným hrozbám. Poskytuje sa špecifický plán evaluácie, ktorý zahŕňa kroky na generovanie testovacích prípadov, reverzné inžinierstvo UML sekvenčných diagramov a zisťovanie chýb v asynchrónnych reaktívnych programoch, spolu s porovnaním s očakávanými výsledkami a validáciou. Na záver tento článok predstavuje komplexný prehľad zistených problémov, navrhovaných riešení, hodnotiacich hypotéz, metrik hodnotenia a plán hodnotenia na riešenie výziev spojených so distribuovanými systémami v kontexte hybridných hrozieb. Navrhnuté riešenia a plán hodnotenia môžu slúžiť ako základ pre ďalší výskum a vývoj v týchto oblastiach.

Kľúčové slová: bezpečné testovanie, problémy a ohrozenia v distribuovaných reaktívnych systémoch, diagramy sekvencií.

ÚVOD

V distribuovaných asynchrónnych alebo reaktívnych systémoch môže byť reakcia na zmeny časovo kritickým spôsobom náročná. Často je potrebná rekonštrukcia príslušnej sekvencie netriviálnych volaní jednotlivých služieb resp. pri spätnej rekonštrukcii možných scenárov hybridných ohrození, čo si vyžaduje vysoké znalosti a odbornosť z vybraných rolí v tíme. Hoci sú k dispozícii nástroje na automatické generovanie sekvenčných diagramov, ich užitočnosť a techniky na vytváranie sekvenčných diagramov sú už známe. V distribuovaných reaktívnych projektoch s fluktuáciou zamestnancov a rozširujúcimi sa projektmi je však dôležité zvážiť synchronizáciu zmien v kóde s existujúcim sekvenčným diagramom opisujúcim bezpečný proces, alebo jeho verziovanie.

Cieľom tohto zámeru je analyzovať možnosti vytvárania sekvenčných diagramov priamo z kódu, konkrétne v distribuovaných projektoch zvlášť citlivých na hybridné hrozby, a navrhnúť a implementovať riešenie na podporu testovania v distribuovaných systémoch pomocou sekvenčných diagramov. Riešenie bude vyvinuté ako prototyp nástroja alebo ako rozšírenie existujúceho nástroja. Navrhované riešenie bude hodnotené na starostlivo vybraných príkladoch

netriviálneho kódu, ktoré predstavujú scenáre reálneho sveta, kde možno očakávať problémy či prípadné ohrozenia hybridnej povahy. Vývojom riešenia pre automatické generovanie sekvenčných diagramov z kódu v distribuovaných systémoch toto zadanie rieši výzvy časovo kritickej reakcie na zmenu a potrebu synchronizácie medzi kódom a dokumentáciou. Zdôrazňuje tiež dôležitosť testovania v distribuovaných systémoch a potenciálne výhody automatického generovania sekvenčných diagramov pri zlepšovaní porozumenia, údržby a testovania distribuovaných systémov pre zvýšenie odolnosti voči hybridným ohrozeniam.

1. SÚVISIACE PRÁCE V OBLASTI SOFTVÉROVÉHO INŽINIERSTVA

V oblasti softvérového inžinierstva existujú rôzne výzvy a problémy, ktoré vznikajú počas vývoja, testovania a údržby zložitých softvérových systémov. Tieto výzvy sú často vzájomne prepojené a vyžadujú si starostlivé zváženie a inovatívne riešenia na zabezpečenie kvality, spoľahlivosti a efektívnosti softvérových systémov. V tomto prehľade budeme diskutovať o niekoľkých prácach týkajúcich sa generovania testovacích prípadov, reverzného inžinierstva sekvenčných diagramov UML, pokrytia chýb a techník testovania, problémov programovania efektívnych asynchrónnych systémov a ďalších. Pri rozdelení výskumov do skupín, budeme používať pre referenciu výskumu index tabuľky 2, ktorá ponúka identifikované skupiny spektra rozpoznaných súvisiacich problémov. Následne tabuľka 1 ponúka klasifikáciu súvisiacich prác do skupín. Jedna skupina Výskumov súvisí s generovaním testovacích prípadov z modelov UML. Modely alebo diagramy UML, ako sú sekvenčné diagramy, komunikačné diagramy a diagramy aktivít, sa široko používajú na znázornenie správania softvérových systémov. Avšak generovanie platných a adekvátnych testovacích prípadov z modelov UML môže byť náročné, najmä pre súbežné alebo distribuované systémy. Výskumy v tejto skupine [1, 2, 3, 5, 13, 14, 15] skúmajú rôzne techniky na generovanie testovacích prípadov z modelov UML, berúc do úvahy zložitosť a súbežnosť moderných softvérových systémov. Na riešenie týchto výziev a zabezpečenie efektívneho generovania testovacích prípadov sa bežne používajú techniky, ako je testovanie založené na modeli, kontrola modelu a testovanie založené na obmedzeniach. Ďalšia skupina výskumov súvisí s reverzným inžinierstvom UML sekvenčných diagramov z kódovej alebo dynamickej analýzy. Sekvenčné diagramy UML sú grafické znázornenia interakcií medzi objektmi v systéme a poskytujú cenné informácie o správaní softvérových systémov. Reverzné inžinierstvo sekvenčných diagramov UML zo starších systémov alebo viacvláknových systémov, ktorým chýba správna dokumentácia alebo zdrojový kód, však môže byť náročné. Výskumy v tejto skupine [4, 6, 7, 8, 9, 10, 11, 12] majú za cieľ obnoviť sekvenčné diagramy UML a preskúmať techniky, ako je dynamická analýza, statická analýza a prístupy založené na strojovom učení na automatické odvodenie sekvenčných diagramov zo stôp kódu alebo vykonávania. Tieto techniky sú kľúčové pre pochopenie správania existujúcich systémov, dokumentáciu starších systémov a podporu činností údržby softvéru. Pokrytie chýb a testovacie techniky sú tiež dôležitými výzvami v softvérovom inžinierstve. Zabezpečenie dôkladného testovania softvérových systémov na odhalenie chýb a porúch je nevyhnutné na dosiahnutie vysokej kvality softvéru. Výskumy v tejto skupine [18, 19] súvisia s pokrytím chýb a testovacími technikami, najmä pre konečné stavové stroje (FSM) a asynchrónne reaktívne programy. Techniky, ako je testovanie založené na stave, kontrola modelu a vstrekovanie porúch, sa bežne používajú na generovanie testovacích sekvencií, ktoré môžu odhaliť chyby spôsobené závodom údajov, synchronizáciou, zablokovaním a sieťovým prenosom. Cieľom týchto techník je poskytnúť primerané pokrytie chýb, pričom sú škálovateľné a efektívne, berúc do úvahy výzvy testovania zložitých softvérových systémov. Programovanie efektívnych asynchrónnych systémov je ďalšou výzvou v softvérovom inžinierstve. Asynchrónne systémy, v ktorých sa

udalosti a akcie vyskytujú nezávisle a súbežne, sú čoraz populárnejšie vďaka svojej schopnosti zvládnuť zložité a dynamické interakcie.

	Meno	Popis
1	Generovanie testovacích prípadov z modelov UML	súvisiace s generovaním testovacích prípadov z modelov alebo diagramov UML, najmä pre súbežné alebo distribuované systémy. Tieto problémy skúmajú rôzne techniky na generovanie platných a adekvátnych testovacích prípadov z modelov alebo diagramov UML, ako sú sekvenčné diagramy, komunikačné diagramy a diagramy aktivít. Hlavnou výzvou v tejto kategórii je zvládnutie zložitosti a súbežnosti moderných softvérových systémov.
2	Reverzné inžinierstvo sekvenčných diagramov UML	súvisiace s reverzným inžinierstvom UML sekvenčných diagramov z kódu alebo dynamickej analýzy. Cieľom týchto problémov je obnoviť sekvenčné diagramy UML zo starších systémov alebo z viacvláknových systémov, ktorým chýba správna dokumentácia alebo zdrojový kód. Hlavnou výzvou v tejto kategórii je riešenie komplexnosti a variability moderných softvérových systémov.
3	Pokrytie chýb a testovacie techniky	súvisiace s pokrytím chýb a testovacími technikami, najmä pre konečné stavové stroje (FSM) a asynchrónne reaktívne programy. Tieto problémy skúmajú rôzne techniky na generovanie testovacích sekvencií, ktoré môžu odhaliť chyby spôsobené závodom údajov, synchronizáciou, zablokovaním a sieťovým prenosom. Hlavnou výzvou v tejto kategórii je zabezpečiť, aby vygenerované testovacie sekvencie poskytovali primerané pokrytie chýb a zároveň boli škálovateľné a efektívne.
4	Výzvy programovania efektívnych asynchrónnych systémov	súvisí s výzvou programovania efektívnych asynchrónnych systémov, ktoré sa dajú ľahko deklaratívne vyjadriť a ktoré sa bránia proti pretekom údajov a porušovaniu tvrdení závislých od prekladania. Hlavnou výzvou v tejto kategórii je navrhnúť komplexné riešenie, ktoré bude riešiť všetky tieto výzvy jednotným a efektívnym spôsobom.
5	Ostatné	Okrajovo súvisiace

Tabuľka 1 Identifikované skupiny spektra rozpoznaných problémov

Avšak programovanie efektívnych asynchrónnych systémov, ktoré sa dajú ľahko deklaratívne vyjadriť a ktoré sa bránia pretekom údajov a porušeniam tvrdení závislým od prekladania, môže byť náročné. Výskum [20] súvisí s touto výzvou a skúma techniky navrhovania komplexných riešení, ktoré riešia tieto výzvy jednotným a efektívnym spôsobom. Techniky, ako sú formálne metódy, súbežné modely a programovacie jazyky so vstavanou podporou súbežnosti a asynchrónnosti, sa bežne používajú na zvládnutie tejto výzvy a zabezpečenie spoľahlivosti a efektívnosti asynchrónnych systémov. Napokon sú tu ďalšie výskumy v oblasti softvérového inžinierstva, ktoré nezapadajú do vyššie uvedených skupín [16, 17]. Tieto výskumy môžu zahŕňať problémy súvisiace s inžinierstvom softvérových požiadaviek, softvérovou architektúrou, testovaním a ladením softvéru, údržbou softvéru, zabezpečením softvéru a vývojom softvéru. Aj keď nie sú priamo spojené s vyššie uvedenými skupinami, tieto výskumy sú stále dôležité a vyžadujú si pozornosť, aby sa zabezpečila celková kvalita a spoľahlivosť.

2. NÁVRH PODPORY BEZPEČNÉHO TESTOVANIA V DISTRIBUOVANÝCH REAKTÍVNYCH SYSTÉMOCH ZALOŽENEJ NA IDENTIFIKÁCII DIAGRAMOV SEKVENCII V OTÁZKACH

Navrhované riešenie zahŕňa využitie testovacích techník založených na generovaní testovacích prípadov z reverzne vytvorených sekvenčných diagramov UML, berúc do úvahy výzvy programovania

	Meno	DOI / ISBN /ISSN	Rok	Grupa
1	Generation of Test Cases from UML Sequence Diagram Based on Extenics Theory	10.9734/BJMCS/2016/25374	2016	1
2	A Survey on Test Case Generation from UML Model	0975-9646	2011	1
3	Test Case Creation from UML Sequence Diagram: A Soft Computing Approach	10.1007/978-81-322-2012-1	2014	1
4	Static control-flow analysis for reverse engineering of UML sequence diagrams	10.1145/1108792.1108816	2005	2
5	Automatic test case generation from UML communication diagrams	10.1016/j.infsof.2006.04.001	2007	1
6	Towards the reverse engineering of UML sequence diagrams for multithreaded java software	10.22436/mns.02.01.05	2018	2
7	Toward the Reverse Engineering of UML Sequence Diagrams for Distributed Java Software	10.1109/TSE.2006.96	2006	2
8	Reverse-engineering of UML 2.0 Sequence Diagrams from~ Execution Traces		2006	2
9	Recovering UML2 Sequence Diagrams from Execution Traces	10.14569/ijacsa.2020.0111213	2020	2
10	A Dynamic Analysis for Reverse Engineering of Sequence Diagram Using CPN	10.1007/978-3-030-00856-7_22	2018	2
11	Towards new hybrid approach of the reverse engineering of UML sequence diagram	10.1109/CIST.2016.7805035	2016	2
12	Combining Static and Dynamic Analyses to Reverse-Engineer Scenario Diagrams	10.1109/ICSM.2013.24	2013	2
13	Generation of Test Cases from UML Diagrams - A Systematic Literature Review	10.1145/3452383.3452408	2021	1
14	Testing for concurrency in UML diagrams	10.1145/2347696.2347712	2012	1
15	A Method for Automated Test Data Generation from Sequence Diagrams and Object Constraint Language	10.1145/2833258.2833294	2015	1
16	Traffic-aware stress testing of distributed systems based on UML models	10.1145/1134285.1134340	2006	5
17	Automatic generation of UML sequence diagrams from test counterexamples	10.1145/2975969.2975977	2016	5
18	Test sequence generation for controller verification and test with high coverage	10.1145/1179461.1179467	2006	3
19	Systematic testing of asynchronous reactive systems	10.1145/2786805.2786861	2015	3
20	Asynchronous programming, analysis and testing with state machines	10.1145/2737924.2737996	2015	4

Tabuľka 2 Klasifikácia súvisiacich prác do skupín

efektívnych a bezpečných asynchrónnych distribuovaných systémov. Celkovým cieľom je zvýšiť kvalitu a spoľahlivosť softvérových systémov zabezpečením efektívneho testovania súbežných a distribuovaných systémov. Riešenie zahŕňa niekoľko kľúčových bodov:

- reverzné inžinierstvo sekvenčných diagramov UML prostredníctvom techník dynamickej analýzy, ako je monitorovanie a protokolovanie za behu, po ktorom nasleduje použitie prístupov strojového učenia na automatické odvodenie sekvenčných diagramov UML z týchto stôp vykonávania
- testovacie techniky založené na modeli, vrátane automatického generovania testovacích sekvencií z odvodených sekvenčných diagramov a generovania vstupných údajov alebo stimulov na vykonanie rôznych ciest a scenárov v systéme
- riešenie výziev testovania asynchrónnych systémov, zvažovanie problémov, ako sú závody s údajmi, uviaznutie a problémy so synchronizáciou; a nakoniec skúmanie ďalších vylepšení, ako sú techniky vkladania chýb na odhalenie slabých miest a slabín a používanie techník statickej analýzy na identifikáciu zápachov kódu, anti-vzorov alebo prekážok výkonu.

Kombináciou silných stránok testovania založeného na modeli, reverzného inžinierstva sekvenčných diagramov UML a riešenia výziev efektívneho programovania asynchrónnych systémov má toto riešenie za cieľ poskytnúť komplexný prístup k testovaniu súbežných a distribuovaných systémov, čo v konečnom dôsledku zlepšuje kvalitu a spoľahlivosť softvéru a odhaľuje potenciálne problémy.

3. DISKUSIA EVALUAČNÝCH SCENÁROV

Evaluácia sa vykoná posúdením účinnosti a výkonu navrhovaného riešenia v porovnaní s existujúcimi technikami. Poskytne empirické dôkazy na podporu alebo vyvrátenie prínosov a výhod navrhovaného riešenia. Hodnotenie bude zahŕňať tri hypotézy:

1. Integrácia testovania založeného na modeli s dynamickou analýzou a strojovým učením zlepši generovanie testovacích prípadov z modelov UML
2. Použitie dynamickej analýzy na zachytenie skutočného správania systému zvýši presnosť a úplnosť reverzne vytvorených sekvenčných diagramov UML
3. Aplikácia prístupov strojového učenia na odvodenie sekvenčných diagramov UML zo stôp kódu povedie k rýchlejšiemu a presnejšiemu reverznému inžinierstvu.

Tieto hypotézy budú vyhodnotené prostredníctvom kontrolovaných experimentov a reálnych prípadových štúdií s použitím metrík, ako je pokrytie, presnosť, miera detekcie a ďalšie metriky, ako je čas vykonania, využitie pamäte, škálovateľnosť a efektívnosť. Cieľom hodnotenia je vyvinúť riešenie, ktoré efektívne využíva rôzne techniky na riešenie výziev pri generovaní testovacích prípadov založených na UML a reverznom inžinierstve sekvenčných diagramov UML komplexným spôsobom.

ZÁVER

Tento článok sumarizuje prehľad identifikovaných problémov súvisiacich so súbežnými a distribuovanými systémami, staršími, alebo viacvláknovými systémami a asynchrónnymi reaktívnymi programami potenciálne aj v kontexte zvyšovania odolnosti voči hybridným hrozbám. Identifikuje problémy a zhlukujem do skupín. Tie exponuje a mapujem na problémy súvisiace s

generovaním testovacích prípadov z modelov UML, problémy súvisiace s reverzným inžinierstvom UML sekvenčných diagramov a pod. Pre každú skupinu sa diskutuje o navrhovaných riešeniach vrátane algoritmu na generovanie testovacích prípadov založených na modeloch UML a algoritmu reverzného inžinierstva na generovanie sekvenčných diagramov UML. Tento prehľadový článok obsahuje nástrel riešenia, ktoré zahŕňa injektovanie chýb a algoritmy generovania testovacej sekvencie na detekciu porúch v asynchrónnych reaktívnych programoch ako príklad simulácie potenciálneho ohrozenia. V závere diskutuje možné evaluačné scenáre.

Pod'akovanie

Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zdroje

1. C. Baidada, E. M. Bouziane, and A. Jakimi. A dynamic analysis for reverse engineering of sequence diagram using cpn. *Model and Data Engineering*, pages 331–345, 2018.
2. C. Baidada, B. El Mahi, and A. Jakimi. Towards the reverse engineering of uml sequence diagrams for multithreaded java software. *Mathematics in Natural Science*, pages 44–50, 05 2018.
3. C. Baidada and A. Jakimi. Towards new hybrid approach of the reverse engineering of uml sequence diagram. 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), 10 2016.
4. E. M. Bouziane, C. Baidada, and A. Jakimi. Recovering uml2 sequence diagrams from execution traces. *International Journal of Advanced Computer Science and Applications*, 11, 2020.
5. L. Briand, Y. Labiche, and J. Leduc. Toward the reverse engineering of uml sequence diagrams for distributed java software. *IEEE Transactions on Software Engineering*, 32:642–663, 09 2006.
6. D. Carballa and L. M. Castro. Automatic generation of uml sequence diagrams from test counterexamples. *Proceedings of the 15th International Workshop on Erlang*, 09 2016.
7. R. Delamare, B. Baudry, and Y. Le Traon. Reverse-engineering of uml 2.0 sequence diagrams from execution traces. *Workshop on Object-Oriented Reengineering at ECOOP* 06, 01 2006.
8. P. Deligiannis, A. F. Donaldson, J. Ketema, A. Lal, and P. Thomson. Asynchronous programming, analysis and testing with state machines. *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation*, 06 2015.
9. A. Desai, S. Qadeer, and S. A. Seshia. Systematic testing of asynchronous reactive systems. *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, 08 2015.
10. V. Garousi, L. C. Briand, and Y. Labiche. Traffic-aware stress testing of distributed systems based on uml models. *Proceedings of the 28th international conference on Software engineering*, 05 2006.
11. S. Gören and F. J. Ferguson. Test sequence generation for controller verification and test with high coverage. *ACM Transactions on Design Automation of Electronic Systems*, 11:916–938, 10 2006.
12. L. C. Jain, S. Patnaik, and N. Ichalkaranje, editors. *Intelligent Computing, Communication and Devices*. Springer India, 2015.

13. K. Jin and K. Lano. Generation of test cases from uml diagrams - a systematic literature review. 14th Innovations in Software Engineering Conference (formerly known as India Software Engineering Conference), 02 2021.
14. M. Khandai, A. A. Acharya, and D. P. Mohapatra. A survey on test case generation from uml model. 2011.
15. Y. Labiche, B. Kolbah, and H. Mehrfard. Combining static and dynamic analyses to reverse-engineer scenario diagrams. 2013 IEEE International Conference on Software Maintenance, 09 2013.
16. W. Rhmann and V. Saxena. Generation of test cases from uml sequence diagram based on extenics theory. British Journal of Mathematics Computer Science, 16:1–13, 01 2016.
17. A. Rountev, O. Volgin, and M. Reddoch. Static control-flow analysis for reverse engineering of uml sequence diagrams. The 6th ACM SIGPLAN-SIGSOFT workshop on Program analysis for software tools and engineering - PASTE '05, 2005.
18. P. Samuel, R. Mall, and P. Kanth. Automatic test case generation from uml communication diagrams. Information and Software Technology, 49:158–171, 02 2007.
19. M. Shirole and R. Kumar. Testing for concurrency in uml diagrams. ACM SIGSOFT Software Engineering Notes, 37:1–8, 09 2012.
20. T.-D. Vu, P. N. Hung, and V.-H. Nguyen. A method for automated test data generation from sequence diagrams and object constraint language. Proceedings of the Sixth International Symposium on Information and Communication Technology, 12 2015

MERANIE KORUPCIE V KRAJINÁCH EÚ

prof. Ing. Antonín Korauš, PhD., prof. RNDr. Beáta Stehlíková, CSc.

Akadémia Policajného zboru, Sklabinská 1, 835 17 Bratislava; antonin.koraus@akademiapz.sk
Slovenská technická univerzita, Vazovova 5, 812 43, Bratislava, beata.stehlikova@stuba.sk

Abstrakt: Korupcia je vnútorne latentný jav, preto je náročné ju merať. Cieľom príspevku je porovnať a overiť, či tri indexy merajúce korupciu – každý iným spôsobom – a výsledok Eurobarometra týkajúceho sa úplatkárstva v krajinách Európskej únie merajú skutočne to isté. Inak povedané je medzi nimi silná signifikantná závislosť. Závislosť sme merali pomocou Spearmanovho korelačného koeficienta. Hodnotili sme tiež priestorové rozloženie hodnôt jednotlivých kompozitných indexov merajúcich korupciu. Výsledky ukázali, že závislosti sú vysoké a signifikantné okrem závislosti medzi výsledkami Eurobarometra GCP a WGI.

Kľúčové slová: CPI, WJP, WGI, GCP.

ÚVOD

Korupcia je široký pojem, ktorý môže zahŕňať rôzne formy nesprávneho správania. Podplácanie je najbežnejšou formou korupcie. Podplácanie môže byť priame, keď verejný činiteľ dostane úplatok priamo od jednotlivca alebo spoločnosti, alebo nepriame, keď verejný činiteľ dostane úplatok prostredníctvom tretej strany. Ďalšia forma korupcie je nepotizmus, pri ktorej sú príbuzní alebo priatelia verejných činiteľov uprednostňovaní pri získavaní zamestnania alebo obchodných príležitostí, čo môže viesť k tomu, že na dôležité pozície budú menovaní ľudia, ktorí nie sú kvalifikovaní alebo skúsení. O korupcii tiež hovoríme, keď verejní činitelia využívajú verejné zdroje na osobné účely, napríklad používanie služobných vozidiel na osobné účely, prijímanie darčiekov od súkromných osôb alebo zneužívanie verejných fondov.

Korupcia má negatívne dôsledky na ekonomiku, spoločnosť a demokraciu. Môže viesť k zníženiu hospodárskeho rastu, lebo môže viesť k neefektívnemu využívaniu zdrojov, čo môže spomaliť hospodársky rast. Korupcia môže viesť k tomu, že bohatstvo sa sústreďuje v rukách privilegovaných, čo môže viesť k nerovnostiam v spoločnosti. Korupcia môže podkopať dôveru v verejnú správu, čo môže viesť k oslabeniu demokracie.

Korupcia – široko definovaná ako zneužívanie verejnej funkcie na súkromné zisky stojí každú krajinu každoročne veľké množstvo finančných, politických a sociálnych zdrojov (Kubbe, Engelbert, 2018).

Korupcia je vnútorne latentný jav, preto je náročné ju merať a vyžaduje si použitie nepriamych ukazovateľov (Shukhova, Nisnevich, 2017).

Boj proti korupcii je kľúčový pre dosiahnutie trvalo udržateľného rozvoja (Castro a Lopes, 2022). Závery štúdie Sarabia et al (2020) poskytujú nové poznatky, ktoré môžu pomôcť identifikovať slabé miesta v demokraciách, kde by mohli rásť populistické strany.

Podľa Bello y Villarino (2021) každý výskumník v oblasti korupcie čelil v určitom bode výskumu dileme súboru údajov. Korupcia je jednou z najnáročnejších hrozieb, ktorým súčasné spoločnosti na celom svete čelia, a napriek tomu stále existuje pomerne slabý konsenzus o tom, ako ju najlepšie

merať (Gnaldi et al., 2021). Prieskumy verejnej mienky podľa Wysmułek (2019) zohrávajú pri výskume korupcie zásadnú úlohu. Prieskumy na širokej verejnosti poskytujú kľúčové informácie na testovanie teórií a rozširovanie myšlienok o mikroúrovniah korelátov vnímanej a prežívanej korupcie a ich interakcií s inštitucionálnym a národným kontextom. Snaha o meranie korupcie dôležitá, v neposlednom rade pre návrh a hodnotenie protikorupčných opatrení (Graycar, 2014). Účinnosť indexov vnímania korupcie na skutočné zachytenie a presné meranie korupčného správania bola často kritizovaná. V skutočnosti sa predstavy o korupcii nemusia zhodovať so skutočnými skúsenosťami, tvrdia Corrado et al. (2023). Treisman (2015) považuje rozdiely vo vnímanom skóre korupcie v jednotlivých krajinách skôr za koreláciu s národnými kultúrnymi stereotypmi alebo širším mediálnym pokrytím napr. korupčných škandálov, než so skutočným rozsahom korupčných aktivít.

Kľúčom k riešeniu korupcie je komplexný prístup. Medzi konkrétne opatrenia, ktoré môžu vlády a jednotlivci podniknúť na riešenie korupcie, patrí zvýšenie transparentnosti verejnej správy, posilniť zodpovednosti verejných činiteľov, zlepšenie účinnosti právnych predpisov a inštitúcií ako aj podpora občianskej spoločnosti vládami jednotlivých krajín. Vývoj sofistikovanejších protikorupčných opatrení môže byť stimulovaný dôslednými a presvedčivými požiadavkami na účinnejšie opatrenia proti korupcii uvádza Malito (2014). Neexistuje však jednoznačná odpoveď, ako riešiť korupciu (Šumah, 2018).

V prostredí verejnej správy, v prostredí tvorenom jej orgánmi musia mať osoby istotu v tom, ako sa voči, resp. s nimi a o ich veci bude konať, že toto konanie bude zákonné, že bude transparentné a že povedie k výsledku, ktorý je možné na základe zákonných pravidiel v príslušnom konaní rozumne predpokladať a očakávať. Korupcia toto očakávanie zmenšuje, v najextrémnejšom prípade úplne neguje. V prostredí skorumpovanej verejnej správy osoby nemajú zachovanú právnu istotu, že pravidlá sa budú zákonne a korektne zachovávať aj bez úplatku.

Cieľom príspevku je porovnať a verifikovať, či tri indexy merajúce korupciu – každý iným spôsobom – a výsledok Eurobarometra týkajúceho sa úplatkárstva v krajinách Európskej únie merajú skutočne to isté. Inak povedané je medzi nimi silná signifikantná závislosť.

1. MATERIÁL A METÓDY

Korupcia je komplexný problém. V práci budeme pracovať s tromi indexami merajúcimi korupciu a výsledky Eurobarometra, týkajúceho sa úplatkárstva v krajinách Európskej únie.

Index vnímania korupcie CPI meria vnímanú korupciu vo verejnom sektore. Hodnotí krajiny na základe na základe výsledkov medzinárodného prieskumu odbornej verejnosti, pozostávajúcej z podnikateľov, analytikov a odborníkov verejnej správy. K číslu 0 sa priradzuje status veľmi skorumpovanej krajiny a hodnota vyjadrená číslom 100 označuje nulovú korupciu v krajine. Dosahované hodnoty vnímania miery korupcie pod 50 indikujú vážne korupčné problémy krajiny.

Rule of Law Index WJP zachytáva dodržiavanie zákonov v štáte, ako ho definujú univerzálne princípy projektu World Justice Project, prostredníctvom komplexného a viacrozmerného súboru 44 ukazovateľov, z ktorých každý odráža konkrétny aspekt tohto komplexného konceptu. Právny štát je trvalý systém zákonov, inštitúcií, noriem a záväzkov komunity, ktorý zabezpečuje zodpovednosť, spravodlivé právo, otvorené vládnutie, prístupnú a nestrannú spravodlivosť. Index

nadobúda hodnoty z intervalu od 0 do 1. Hodnoty blízko nuly predstavujú slabšie dodržiavanie pravidiel zákona. Naopak, hodnoty blízko 1 predstavujú silnejšie dodržiavanie pravidiel zákona.

Druhá dimenzia WJP2 Absencia korupcie obsahuje štyri kategórie:

2.1 Vládni úradníci v exekutive nevyužívajú verejnú funkciu na dosiahnutie súkromného zisku

2.2 Vládni úradníci v súdnej moci nevyužívajú verejnú funkciu na dosiahnutie súkromného zisku

2.3 Vládni úradníci v polícii a armáde nevyužívajú verejné funkcie na dosiahnutie súkromného zisku

2.4 Vládni úradníci v zákonodarnej oblasti nepoužívajú verejnú funkciu na dosiahnutie súkromného zisku.

Worldwide Governance Indicators (WGI) sú navrhnuté tak, aby pomohli výskumníkom a analytikom posúdiť široké vzorce vo vnímaní správy vecí verejných v jednotlivých krajinách v priebehu času. Údaje odrážajú rôzne názory na riadenie mnohých zainteresovaných strán (think-tankov, medzinárodných organizácií, mimovládnych organizácií a súkromných firiem). Jedna zo šiestich dimenzií indexu WGI je Kontrola korupcie. Kontrola korupcie odráža vnímanie rozsahu, v akom sa verejná moc vykonáva pre vlastný súkromný prospech, vrátane drobných a veľkých foriem korupcie, ako aj ovládnutie štátu elitami a súkromnými záujmami. Hodnoty dimenzie sú od -2,5 do 2,5 (silná výkonnosť verejnej moci). Uvádza sa tiež 90 percentný interval spoľahlivosti pre percentil poradia.

Globálny barometer korupcie – Európska únia . V rámci neho sa zisťuje priama skúsenosť ľudí s korupciou. Nemeria korupciu priamo, ale zisťuje, či podľa názoru výskumnej vzorky vrástla, klesla. Uvádzame mieru podplácania v troch vybraných oblastiach. Rozdiel medzi podplácaním a korupciou je v tom, že podplácanie je konkrétny čin, ktorý sa týka odovzdania alebo prijatia úplatku, zatiaľ čo korupcia je širší pojem, ktorý zahŕňa aj iné formy zneužívania moci alebo postavenia na súkromný úžitok. Podplácanie je úmyselné odovzdanie alebo prijatie akejkoľvek neoprávnenej výhody, aby sa ovplyvnilo konanie alebo rozhodnutie niekoho, kto je v úradnom alebo inom postavení. Môže sa to uskutočniť v akejkoľvek podobe, vrátane peňazí, darčiekov, služieb alebo výhod. Korupcia je všeobecnejší pojem, ktorý zahŕňa akékoľvek konanie, pri ktorom niekto zneužije svoju moc alebo postavenie na súkromný prospech. Môže to zahŕňať podplácanie, ale aj iné formy zneužívania moci

Metodika hodnotenia Eurobarometra vychádza z údajov reprezentatívnej vzorky obyvateľov – respondentov. V Tabuľke 1 je prehľad použitých indexov.

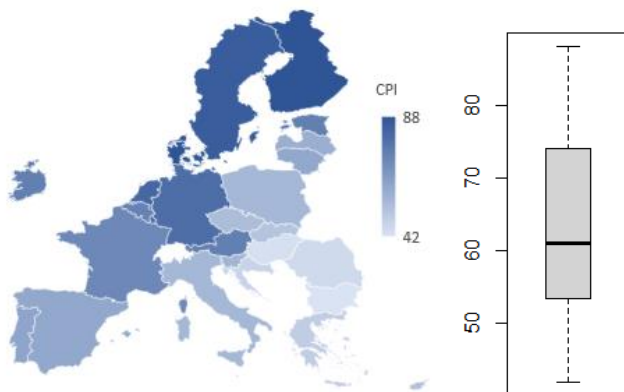
Tabuľka 1 Zoznam použitých indexov

Názov indexu		Skratka	Inštitúcia	Hranice	Lepšie je	Link
Index vnímania korupcie	Corruptions Perceptions Index	CPI	Transparency International	Od 0 do 100	vyššie	https://www.transparency.org/en/cpi/2021
Index právneho štátu	WJP Rule of Law Index	WJP	World Justice Project	Od 0 do 1	vyššie	https://worldjusticeproject.org/rule-of-law-index/global
Celosvetové ukazovatele riadenia	Worldwide Governance Indicators	WGI	World Bank National Resource Governance Institute	od -2,5 do 2,5	vyššie	https://www.govindicators.org/
Globálny barometer korupcie	Global Corruption Barometer	GCP	Transparency International	Od 0 do 100	nižšie	https://www.transparency.org/en/gcb/eu/european-union-2021

V príspevku pracujeme s údajmi za rok 2021. Na meranie závislosti používame Spearmanov korelačný koeficient poradovej korelácie. Je totožný s výberovým Pearsonovým koeficientom korelácie aplikovaným na poradie zložiek výberového súboru. Výpočty sme realizovali v programovom prostredí R.

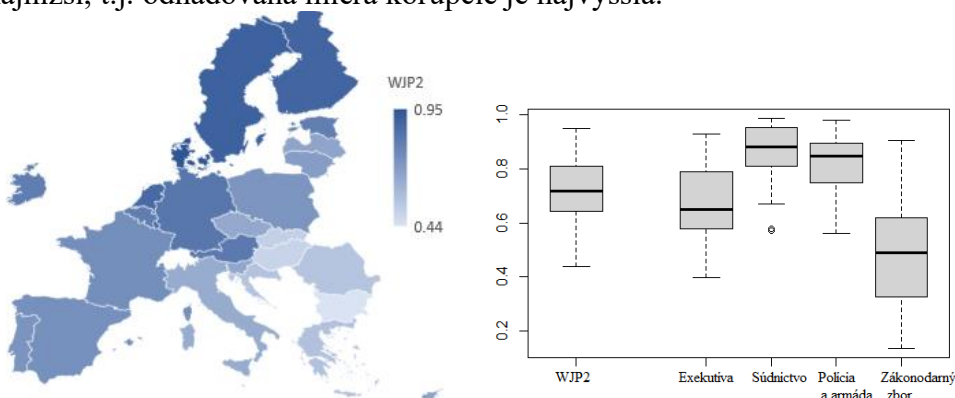
2. VÝSLEDKY A DISKUSIA

CPI meria vnímanú korupciu vo verejnom sektore. Index vnímania korupcie CPI je vysoký v severských krajinách Fínsku a Švédsku, ale aj Luxembursku, Dánsku, Holandsku a Nemecku. Sú to krajiny, ktoré netolerujú korupciu. Korupčné problémy majú krajiny Bulharsko, Maďarsko, Rumunsko, Chorvátsko a Grécko.



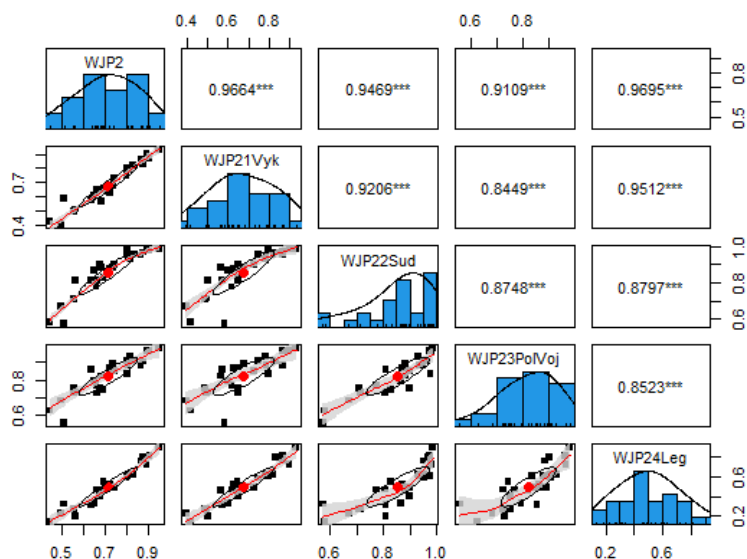
Obrázok 1 Kartogram pre CPI a box-plot CPI pre krajiny EÚ

Údaje indexu WJP pochádzajú z prieskumu domácností ako aj prieskumu v radoch právnikov a expertov. WJP je hlavný zdroj originálnych, nezávislých údajov o právnom štáte. Druhá dimenzia indexu WJP2 meria absenciu korupcie. Faktor zohľadňuje tri formy korupcie: úplatkárstvo, nevhodné ovplyvňovanie verejnými alebo súkromnými záujmami a spreneveru verejných financií alebo iných zdrojov. Tieto tri formy korupcie sa skúmajú s ohľadom na vládnych úradníkov v exekutive, súdnictve, armáde, polícii a zákonodarnom zbore. Výskyt úplatkárstva, neformálnych platieb a iných stimulov pri poskytovaní verejných služieb a presadzovaní predpisov je najnižší v Holandsku, Nemecku, Rakúsku, Belgicku, Írsku a Estónsku. Naopak najväčší problém spôsobuje v Bulharsku, Maďarsku, Slovensku, Rumunsku, Chorvátsku a Grécku. Súdnicstvo a Polícia a armáda majú najmenšie variačné aj kvartilové rozpätie. Súčasne v týchto troch zložkách je najvyšší medián, t.j. najnižšia miera korupcie súhrnne za tri jej formy: úplatkárstvo, nevhodné ovplyvňovanie verejnými alebo súkromnými záujmami a spreneveru verejných financií alebo iných zdrojov. Zákonodarný zbor je dôležitým orgánom štátnej moci, ktorý má právomoc prijímať zákony, financovať štát a kontrolovať výkonnú moc. Práve tu je minimum, maximum aj medián najnižší, t.j. odhadovaná miera korupcie je najvyššia.



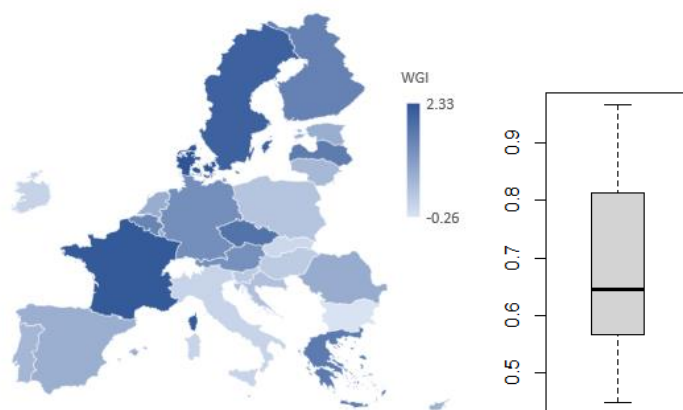
Obrázok 2 Kartogram pre WJP2 a box-plot WJP2 a jeho zložiek pre krajiny EÚ

Miera absencie korupcie meraná druhou dimenziou indexu WJP vysoko a vysoko signifikantne (na hladine významnosti 0,001) koreluje s mierou absencie korupcie s ohľadom na vládnych úradníkov v exekutive, súdnictve, armáde, polícii a zákonodarnom zbore.



Obrázok 3 Kombinovaný graf pre WJP2 a jeho zložiek

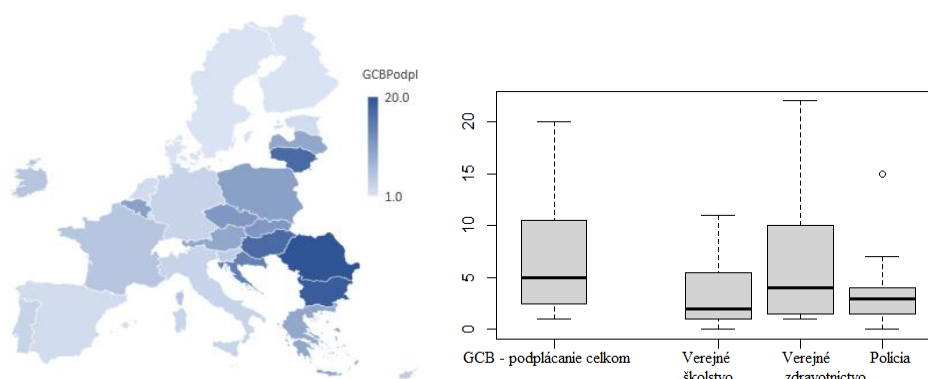
Dobrá správa vecí verejných je pre rozvoj nevyhnutná. Pomáha krajinám zlepšovať hospodársky rast, budovať ľudský kapitál a posilňovať sociálnu súdržnosť. WGI obsahuje šesť súhrnných ukazovateľov, posledný z nich je kontrola korupcie. Kontrola korupcie zachytáva vnímanie rozsahu, v akom sa verejná moc vykonáva pre súkromný prospech, vrátane drobných aj veľkých foriem korupcie, ako aj ovládnutie štátu elitami a súkromnými záujmami.



Obrázok 4 Kartogram pre WGI a box-plot WGI pre krajiny EÚ

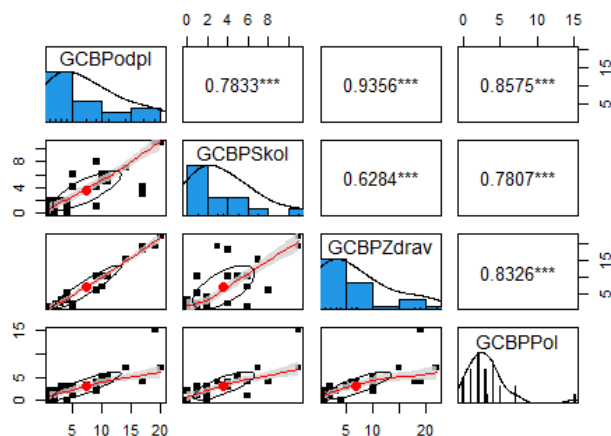
Výkonnosť verejnej moci proti korupcii znamená schopnosť verejnej moci účinne a transparentne bojovať proti korupcii. Výkonnosť verejnej moci proti korupcii je najnižšia v Bulharsku, Slovensku, Taliansku, Írsku a Maďarsku. Naopak najvýkonnejšia je v Dánsku, Francúzsku, Švédsku, na Malte a Českej republike.

Najvyšší podiel ľudí, ktorý za posledných 12 mesiacov dalo úplatok sú Rumunsko, Bulharsko, Litva, Maďarsko a Chorvátsko. Najnižší podiel mali krajiny Dánsko, Fínsko a Švédsko. Globálny barometer korupcie GCP nám ukázal, že úplatky dalo v polovici krajín 5 percent respondentov. Najnižšie priemerné percento aj najmenšie varičné rozpätie (bez extrémne odľahlej hodnoty pre Bulharsko (15 percent) má podiel úplatkov pre políciu.



Obrázok 5 Kartogram pre podiel ľudí ktorí dali úplatok (podľa GCP)

Podiel ľudí, ktorí dali za posledných 12 mesiacov úplatok podľa GCP a podiel ľudí, ktorí dali úplatok vo vybraných hodnotených oblastiach sú vysoké a vysoko signifikantne (na hladine významnosti 0,001)

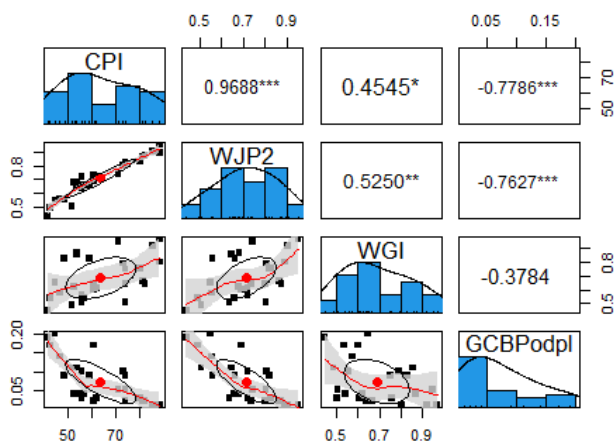


Obrázok 6 Kombinovaný graf pre podiel ľudí ktorí dali úplatok celkom a vo vybraných oblastiach podľa GCP.

Medzi CPI a WJP2 je silná kladná signifikantná monotónna závislosť (0,9688). Krajina vnímaná ako menej skorumpovaná (CPI väčšie hodnoty hodnoty) má vyššie hodnotenie WJP2, t.j. viac absentuje korupcia. Keď je výkonnosť verejnej moci proti korupcii silná (hodnoty WGI sú vyššie) viac absentuje korupcia (hodnoty WJP2 sú vyššie). Hodnota Spearmanovho koeficienta je 0,5250 (signifikantná na hladine významnosti 0,01).

V krajine vnímanej ako menej skorumpovaná (CPI väčšie hodnoty hodnoty) menšie percento ľudí dáva úplatky (Spearmanov korelačný koeficient -0,7786 je signifikantný na hladine významnosti 0,001). Aj v krajinách, v ktorých viac absentuje korupcia, menšie percento ľudí dáva úplatky (Spearmanov korelačný koeficient -0,7627 je signifikantný na hladine významnosti 0,001).

Mohli by sme predpokladať, že v prípade, keď je výkonnosť verejnej správy proti korupcii silná (hodnoty WGI sú vyššie), by menšie percento ľudí malo dávať úplatky. Spearmanov korelačný koeficient -0,3784 však nie je signifikantný, t.j. signifikantne sa nelíši od nuly. Existuje niekoľko dôvodov, prečo výkonnosť verejnej správy nemá signifikantný vplyv na podiel ľudí dávajúcich úplatky. Úplatky môžu byť výsledkom kultúrnych faktorov. V niektorých kultúrach je dávanie úplatkov považované za normálnu súčasť života. V týchto kultúrach ľudia nemusia vnímať dávanie úplatkov ako niečo zlé alebo nezákonné. Úplatky môžu byť spôsobom, ako získať prístup k službám, ktoré sú inak nedostupné. V krajinách s nízkym príjmom alebo s neefektívnou verejnou správou môžu byť úplatky jedným zo spôsobov, ako získať prístup k základným službám, ako je zdravotná starostlivosť alebo vzdelávanie (Bulharsko, Rumunsko).



Obrázok 6 Kombinovaný graf pre hodnotené indexy korupcie

ZÁVERY

Doteraz najpoužívanejším ukazovateľom je kompozitný index CPI. Ako ukázala korelačná analýza, tieto ukazovatele CPI a WJP2 sú mimoriadne dobre korelované, na účely výskumu korupcie na medzištátnej úrovni nie je veľký rozdiel v tom, ktorý ukazovateľ by sa použil. Prieskum vnímania korupcie sú veľmi dobre korelované s kompozitným indexom WJP2, čo naznačuje, že pri použití týchto ukazovateľov týkajúcich sa výskumu korupcie by vo výsledkoch neboli extrémne veľké rozdiely. Keďže nevieme zistiť skutočnú mieru korupcie, nie je možné povedať, ktorý kompozitný ukazovateľ je v ich meraniach správny. Pre analýzu korupcie založenú na skúsenostiach sa ako najlepší ukazovateľ javí Eurobarometer (GCB), keďže má široké časové a celounijné pokrytie, je časovo porovnateľný a ponúka možnosti mikroanalýzy.

PodĎakovanie

Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zdroje

1. Bello y Villarino, J. M. (2021). Measuring corruption: A critical analysis of the existing datasets and their suitability for diachronic transnational research. *Social Indicators Research*, 157(2), 709-747.
2. Castro, C., & Lopes, I. C. (2022). E-government as a tool in controlling corruption. *International Journal of Public Administration*, 1-14.
3. Corrado, G., Corrado, L., De Michele, G., & Salustri, F. (2023). Are perceptions of corruption matching experience? Evidence from microdata. *The British Journal of Criminology*, 63(3), 687-708.
4. Dragulescu, A., Arendt, C. (2020). xlsx: Read, Write, Format Excel 2007 and Excel 97/2000/XP/2003 Files. R package version 0.6.5. <https://CRAN.R-project.org/package=xlsx>
5. Gnaldi, M., Del Sarto, S., Falcone, M., & Troia, M. (2021). Measuring corruption. *Understanding and Fighting Corruption in Europe: From Repression to Prevention*, 43-71.

6. Graycar, A., Prenzler, T., Graycar, A., & Prenzler, T. (2013). Measuring corruption. *Understanding and preventing corruption*, 33-48.
7. Kubbe, I., & Engelbert, A. (2018). Corruption and the impact of democracy. *Crime, Law and Social Change*, 70, 175-178.
8. Malito, D. (2014). Measuring corruption indicators and indices. *Robert Schuman Centre for Advanced Studies Research Paper*, 13.
9. R Core Team (2021). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>.
10. Revelle, W. (2022) psych: Procedures for Personality and Psychological Research, Northwestern University,
11. Evanston, Illinois, USA, <https://CRAN.R-project.org/package=psych> Version = 2.2.5.
12. Sarabia, M., Crecente, F., del Val, M. T., & Giménez, M. (2020). The Human Development Index (HDI) and the Corruption Perception Index (CPI) 2013-2017: analysis of social conflict and populism in Europe. *Economic research-Ekonomska istraživanja*, 33(1), 2943-2955.
13. Shukhova, A., & Nisnevich, Y. (2017). Measurement of validity of corruption indices. *Higher School of Economics Research Paper No. WP BRP*, 42.
14. Šumah, Š. (2018). Corruption, causes and consequences. In *Trade and global market*. IntechOpen.
15. Treisman, D. (2015). What does cross national empirical research reveal about the cause of corruption. In P. M. Heywood (Ed.), *Routledge handbook of political corruption* (pp. 95–109). New York: Routledge.
16. Wymułek, I. (2019). Using public opinion surveys to evaluate corruption in Europe: trends in the corruption items of 21 international survey projects, 1989–2017. *Quality & Quantity*, 53(5), 2589-2610.

POTREBA VNÍMANIA KONCEPTU HYBRIDNÝCH HROZIEB NA NÁRODNEJ ÚROVNI

npor. JUDr. Patrícia Krásná, PhD., LL.M.

Katedra vyšetrovania Akadémie Policajného zboru v Bratislave; Sklabinská 1, 835 17 Bratislava 35;
patricia.krana@akademiazp.sk

Abstrakt: Vnímanie samotnej podstaty hybridných hrozieb a ich konceptu členmi spoločnosti je podstatne dôležité. Kľúčové je, aby bol identifikovaný, zrejme vymedzený a následne špecificky charakterizovaný tak, aby ho vnímala nie len široká laická a odborná, vedecká, verejná, ale špecificky aj aktívni príslušníci Policajného zboru a zamestnanci verejnej správy. Tento účel je podporený skutočnosťami, že hybridné hrozby sú súčasťou našej spoločnosti a je potrebné neustále budovať jej odolnosť proti ich pôsobeniu. Autorka sa pri spracovaní vedeckej štúdie zamerala na špecifikáciu základného konceptu hybridných hrozieb a tiež na špecifikáciu nutnosti odôvodneného vnímania hybridných hrozieb príslušníkmi Policajného zboru a zamestnancami verejnej správy. Cieľom autorky bolo jasne vymedziť súvislosti spojené so základnými piliermi konceptu hybridných hrozieb a prepojiť nadobudnuté relevantné poznatky, získané počas výskumu, s realizáciou každodenných činností príslušníkov Policajného zboru, zamestnancov verejnej správy a odborníkov z aplikačnej praxe. Predložená vedecká štúdia je spracovaná v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu: 314011CDW7.

Kľúčové slová: hybridné hrozby, koncept hybridných hrozieb, príslušníci Policajného zboru, aktér, nástroj, doména, hybridné pôsobenie, riziko.

ÚVOD

Kľúčové je v súvislosti s prezentovaním danej problematiky v úvode vymedziť základnú charakteristiku, ktorá bude určito predikovať následný kontext predloženej štúdie. Predložená štúdia je rozdelená na základe nadobudnutých relevantných vedeckých poznatkov a aplikačnej empirie. Jej kompozíciu vytvárajú konkrétne výsledky realizovanej analýzy, syntézy, pozorovania, zovšeobecňovania a tiež spracované odpovede získané z riadených rozhovorov s príslušníkmi Policajného zboru, zamestnancami verejnej správy a odborníkmi z aplikačnej praxe. Základnou podstatou predloženej vedeckej štúdie je teoretická zakotvenosť, inovatívnosť a nadväznosť.

Počas vedeckého skúmania autorka zamerala svoj interest na rekognoskáciu opodstatnených vedeckých, teoretických, skutočností, ich prepojenie a nachádzanie súvislostí s poznatkami získanými od odborníkov z aplikačnej praxe za účelom jasného smerovania zefektívnenia činnosti príslušníkov Policajného zboru a zamestnancov verejnej správy, ktorí sa stretávajú s hybridným pôsobením takmer počas každého dňa vo svojej aplikačnej praxi. Riadené rozhovory boli realizované, prostredníctvom aktívnych dialógov, s 20 príslušníkmi Policajného zboru, ktorí indikovali jasnú potrebu zadefinovania podstaty hybridných hrozieb a ich konceptu. Taktiež boli realizované riadené rozhovory aj s 3 odborníkmi z aplikačnej praxe, ktorí sa dlhodobo venujú, práve charakteristike a konkrétnemu pôsobeniu hybridných hrozieb z pracoviska pre hybridné hrozby a dezinformácie. Ich indikácia vyplývala z poznatkov, ktoré majú v rámci ich činnosti v aplikačnej praxi a z podnetov, ktoré vnímajú pri realizácii úkonov, ktoré sú v ich kompetencii. Taktiež boli riadené rozhovory realizované aj s 30 zamestnancami verejnej správy. Zamestnanci verejnej správy aj príslušníci Policajného zboru boli účastníkmi vzdelávania v rámci národného

projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“.

Podstatne dôležité je v úvode tiež špecifikovať samotné slovné spojenie „hybridná hrozba“. Pretože aj odborníkmi z aplikačnej praxe nám bolo avizované, že jasná a zrejmá špecifikácia samotných hybridných hrozieb je podstatne dôležitá a následne na základe nej je možné efektívne realizovať činnosti, ktoré sú spojené s elimináciou a predchádzaním pôsobenia hybridných hrozieb.

Toto slovné spojenie označuje činnosť vykonávanú štátnymi alebo neštátnymi aktérmi, ktorej cieľom je podkopať alebo poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni. Takéto akcie sú koordinované a synchronizované a zámerne sa zameriavajú na zraniteľné miesta demokratických štátov a inštitúcií. Aktivita môžu prebiehať v politickej, ekonomickej, vojenskej, civilnej alebo informačnej oblasti. Vykonávajú sa pomocou širokej škály prostriedkov a sú navrhnuté tak, aby zostali pod prahom detekcie a pripisovania.²⁰⁷

Je zrejmé, z poznatkov na teoretickej úrovni, ale aj z poznatkov aplikačnej praxe, že hybridná činnosť sa vyznačuje nejednoznačnosťou, keďže hybridní aktéri stierajú obvyklé hranice medzinárodnej politiky a pôsobia na rozhraní medzi vonkajšou a vnútornou bezpečnosťou, ale vo svojej podstate aj medzi mierom a vojnou. Uvádzaná nejednoznačnosť je dôsledkom kombinácie konvenčných a nekonvenčných prostriedkov, napr. dezinformácií a zasahovania do politickej diskusie či volieb, narušenia či útokov kritickej infraštruktúry, kybernetických operácií, rôznych foriem kriminálnych aktivít a napokon asymetrického využívania vojenských prostriedkov na vedenie vojny.²⁰⁸

Podstatnou skutočnosťou spojenou s uvádzaným je, že použitím nekonvenčných a konvenčných prostriedkov aktéri hybridných hrozieb zakryjú svoju činnosť do nejasnosti a nejednoznačnosti, čo komplikuje ich identifikáciu a samozrejme na základe daného aj odozvu voči nim. Činnosť samotných štátnych, ale aj neštátnych aktérov podporujú jednotlivé konania tzv. „zástupných“, resp. „proxy“ aktérov, ktorých využívajú na čo najefektívnejšie dosiahnutie svojich cieľov. Samotné hybridné konanie je z týchto dôvodov aj finančne aj personálne menej náročné, pretože premieňa zraniteľnosť cieľa na priamu silu hybridného aktéra. Práve uvádzané sťažuje zabránenie hybridnému konaniu.

V aktuálnej dobe sme svedkami realizovaného prepojenia viacerých subjektov, práve v medzinárodných mocenských štruktúrach a táto skutočnosť predstavuje veľmi vhodné podmienky pre hybridné pôsobenie. Narastajúci konflikt hodnôt medzi jednotlivými subjektami narušuje medzinárodné normy a fungovanie medzinárodných inštitúcií, na základe čoho sú realizované konkrétne hybridné, komplexné, ataky v spoločnosti. Konflikt hodnôt, ktorý sa v spoločnosti vytvoril a následne sa prehľbuje, ako nám to bolo potvrdené aj počas realizácií riadených rozhovorov, a tým sa zvyšuje polarizácia a nejednotnosť spoločností. Následne sa spoločnosť ako

²⁰⁷ Hybrid COE. 2023. [online]. [cit. 2023.10.15.] Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.

²⁰⁸ TREVERTON, G. F., THVEDT, A., CHEN, A. R., LEE, K., MCCUE, M. 2018. Addressing Hybrid Threats. [online]. [cit. 2023.10.15.] Dostupné na internete: <https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574</div>>.

taká stáva, opodstatnene, zraniteľnejšia voči vonkajším vplyvom a zásahom a teda aj voči pôsobeniu aktérov hybridných hrozieb. Konštatujeme, že s uvádzaným veľmi úzko súvisí aj progres vývoja moderných technológií a čoraz komplexnejšie informačné prostredie, ktoré jednoznačne poskytujú hybridným aktérom silné nástroje na ich pôsobenie a následne aj efektívne získanie svojho strategického cieľa.

Na základe teoretických, vedeckých, poznatkov a informácií získaných od odborníkov z aplikačnej praxe boli pre spracovanie predloženej vedeckej štúdie vymedzené aj 3 hlavné hypotézy.

H1 Vnímanie hybridných hrozieb na národnej úrovni je dostatočné.

H2 Pri realizácii efektívneho predchádzania hybridným hrozbám je opodstatnené poznať a skúmať základné piliere konceptu hybridných hrozieb.

H3 Vnímanie zraniteľnosti Slovenska voči hybridným hrozbám je podmienené vymedzením konkrétnych odporúčaní, ktoré sú účelné pre jej elimináciu.

V súvislosti s overovaním, špecifikovaním, hypotéz a naplnením hlavného cieľa je následne štruktúrovaný aj obsah vedeckej štúdie.

1. HYBRIDNÉ HROZBY – IDENTIFIKOVANÁ ROVINA ICH VNÍMANIA

V prvej kapitole predloženej vedeckej štúdie je interest autorky adresne zameraný na špecifikáciu podstaty hybridných hrozieb, ich pôsobenia a na ich vnímanie na národnej úrovni. Realizovaný vedecký výskum identifikoval skutočnosť, že vnímanie hybridných hrozieb je na národnej, medzinárodnej, ale i celosvetovej úrovni odlišný. Preto je kľúčové prezentovať jednotlivé, konkrétne, zistenia, ktoré identifikujú samotnú podstatu hybridných hrozieb.

Definície hybridných hrozieb sú síce rozdielne, avšak čo je dôležité zdôrazniť je skutočnosť o potrebe zachovania ich flexibilitnosti z dôvodu, aby reagovali na premenlivú povahu týchto hrozieb, ide však o to, aby sa podarilo vystihnúť súbor rôznych nátlakových a podvratných činností, ktoré môžu rôzne subjekty účelným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu. Snahou je obyčajne zneužívať strategickú zraniteľnosť cieľa a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy. Keďže boj proti hybridným hrozbám súvisí s národnou bezpečnosťou, obranou, zachovaním práva a verejného poriadku je opodstatnene dôležité, aby kompetentné subjekty na ne reagovali primerane a na základe opodstatnených, relevantných, skutočností.

Hybridné hrozby je možné charakterizovať ako koordinované a synchronizované pôsobenie, ktoré zámerne smeruje na systémovú zraniteľnosť demokratických štátov a inštitúcií prostredníctvom širokej škály konkrétnych prostriedkov a nástrojov. Ide o činnosti, ktoré využívajú prahy detekcie a pripisovania, ako aj rôzne rozhrania (vojna - mier, vnútorná - vonkajšia bezpečnosť, miestna - štátna, národná - medzinárodná úroveň). Činnosti zamerané na ovplyvňovanie rôznych foriem rozhodovania na miestnej (regionálnej), štátnej alebo inštitucionálnej úrovni a navrhnuté tak, aby podporovali a/alebo naplňali strategické ciele aktéra hybridného pôsobenia a zároveň podkopávali a/alebo poškodzovali strategický záujem subjektu, voči ktorému je hybridné pôsobenie namierené.²⁰⁹

²⁰⁹ KORYSTIN, O., SVYRYDIUK, N. 2021. Activities of Illegal Weapons Criminal Component of Hybrid Threats. <http://www.doi.org/10.2991/aebmr.k.210320.016>.

Hybridné metódy vedenia vojny, ako napr. propaganda, podvod, sabotáž a iné nevojenské taktiky sa už dlhodobo používajú na destabilizáciu protivníka, resp. subjektu, na ktorý aktéri hybridných hrozieb pôsobia. Avšak v súčasnosti sú v rámci tohto pôsobenia identifikujú nové skutočnosti, ktorými sú rýchlosť, rozsah a intenzita hybridného pôsobenia, ktoré uľahčujú rýchle, inovatívne, technologické zmeny a globálna prepojenosť.²¹⁰

Hybridné hrozby kombinujú vojenské a nevojenské, ako aj skryté a otvorené prostriedky vrátane dezinformácií, kybernetických útokov, ekonomického tlaku, nasadzovania nepravidielných ozbrojených skupín a použitie bežných síl. Hybridné metódy sa používajú na rozmazanie hraníc medzi vojnou a mierom a snažia sa zasiahnuť pochybnosti do mysli cieľovej populácie. Ich cieľom je destabilizovať a podkopať spoločnosti. Pri hybridnom pôsobení sa využíva donucovací vojenský postoj, ale aj rétorika, ktorá je založená na presadzovaní politických cieľov a podkopávaní medzinárodného poriadku založeného na pravidlách. Škodlivé hybridné a kybernetické operácie a konfrontačná rétorika, ale aj šírenie dezinformácií aktérmi hybridných hrozieb sa zameriavajú na spojencov a poškodzujú bezpečnosť subjektu, na ktorého je ich vplyv zameraný. Aktéri hybridných hrozieb sa snažia kontrolovať kľúčové technologické a priemyselné sektory, kritickú infraštruktúru, ale napr. aj strategické materiály. Aktér tak využíva svoj ekonomický vplyv na vytváranie strategických závislostí a posilnenie svojho vplyvu.²¹¹

Hybridné hrozby, tak ako bolo už niekoľko krát uvedené využívajú zraniteľnosti určitej krajiny, resp. subjektu, a často sa snažia dosiahnuť oslabenie základných demokratických hodnôt a slobôd. Práve dané je dôležité pre uvedenie si faktu, že spolupráca medzi jednotlivými subjektami, ktoré podliehajú hybridnému pôsobeniu je kľúčová a to s cieľom získania informácií o situácii v oblasti identifikácie, sledovania a posudzovania rizík, ktoré môžu ohroziť strategické záujmy daného subjektu. Je pozitívnou skutočnosťou, že v súčasnej dobe sa vyvíjajú konkrétne metódy hodnotenia bezpečnostných rizík, ktoré poskytujú informácie subjektom s rozhodovacou právomocou a podporujú vytváranie politík na základe hodnotenia rizík v oblastiach od bezpečnosti leteckej prevádzky až po financovanie terorizmu a pranie špinavých peňazí.²¹² Hlavným cieľom posudzovania rizík je ochrana zdravia, bezpečnosti jednotlivcov, ale aj relevantných subjektov. Dôležité je uviesť skutočnosť, že práve samotné posudzovanie rizík pomáha minimalizovať možné poškodenia, ktoré hybridným pôsobením vznikajú. Posudzovanie rizík, tak ako nám bolo prezentované odborníkmi z aplikačnej praxe, ktorí sa venujú dlhodobo pôsobeniu hybridných hrozieb, pomáha pri zabezpečení efektívnej eliminácie vplyvu hybridných hrozieb na spoločnosť ako takú. Riziko je situačná charakteristika činnosti, ktorá spočíva v tom, že výsledok činnosti je neistý.

Elementárnou podstatou v súvislosti s uvádzaným je fakt, že riziko ako také je vyjadrením pravdepodobnosti a závažnosti poškodenia pôsobením nebezpečenstva. Tu však vyvstáva otázka, v spojitosti so spracovávanou problematikou a to: „*Prečo je potrebné poznať a posudzovať riziká?*“ Pri dôslednom posúdení všetkých relevantných skutočností je možné konštatovať, že

²¹⁰ JACUCH, A. 2020. RESILIENCE IN THE EU AND NATO'S STRATEGIES. *Copernicus Journal of Political Studies* 2020. No. 1/2020, pp. 5–26. ISSN 2299-4335. <http://dx.doi.org/10.12775/CJPS.2020.001>.

²¹¹ SÍLI, V. 2021. Hybrid threats: modern perception and tactics. [online]. [cit. 2023.10.10.] Dostupné na internete: <https://www.cceol.com/search/article-detail?id=859611>.

²¹² SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADY. Spoločný rámec pre boj proti hybridným hrozbám, reakcia Európskej únie. 2016. [online]. [cit. 2023.10.10.] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018>.

hlavným cieľom posudzovania rizík je ochrana bezpečnosti jednotlivcov, ale aj celej spoločnosti. Práve posudzovanie rizík pomáha minimalizovať možné poškodenie, ktoré je pravdepodobnosť, že v spoločnosti vznikne. Pretože riziká a ohrozenia sú súčasťou každej krajiny, každého spoločenstva a my žiadnym spôsobom nevieme zabezpečiť to, aby tieto riziká, hrozby a nebezpečenstvá neexistovali. Vieme však vyvinúť efektívnu iniciatívu na to, aby sme ich v čo možno najvyššej možnej miere eliminovali. Koncept rizika a hodnotenia rizika má dlhú históriu. V súčasnosti sú však vyvinuté nové a sofistikovanejšie analytické metódy, techniky a prístupy k analýze rizík, ktoré okrem iného zahŕňajú: zbieranie informácií, identifikovanie nebezpečenstiev a ohrození, posudzovanie rizík vyplývajúcich z ohrození (odhad pravdepodobnosti a závažnosti následkov a rozhodnutie, či je riziko akceptovateľné). Plánovanie postupu na odstránenie alebo obmedzenie rizík. Opakovanie posudzovania rizík a dokumentovanie posudzovania rizík.²¹³

Následne je tiež však potrebné konštatovať, že jednou z príčin nedostatočného uplatňovania posudzovania rizík v aplikačnej praxi, ktoré je žiaľ aj v súčasnej dobe často identifikované, je aj zbytočný rešpekt k samotnej procedúre realizácie posúdenia rizík. Veľmi veľa kompetentných subjektov identifikuje v posudzovaní rizík zložitosť a neodváža sa samo logicky posúdiť, čo môže a čo nemôže byť rizikom. Dôležité v súvislosti s daným je to, že posudzovanie rizík je kľúčové aj v rámci identifikácie hybridných hrozieb a ich nebezpečenstva. Okrem uvádzaného by však bolo vhodné realizovať aj prieskum s cieľom identifikovať oblasti potenciálne zraniteľné hybridnými hrozbami. Cieľom tejto identifikácie by bolo určiť ukazovatele hybridných hrozieb, začleniť ich do mechanizmov včasného varovania a existujúcich mechanizmov hodnotenia rizík a v prípade potreby ich zdieľať.

V súvislosti so špecifickými poznatkami a charakteristikou hybridných hrozieb uvádzame, že počas realizácie riadených rozhovorov so zamestnancami verejnej správy, ktorí boli účastní na vzdelávaní realizovanom v rámci národného projektu, v kontexte ktorého vznikla aj táto vedecká štúdia, ale aj na základe poznatkov od príslušníkov Policajného zboru a odborníkov pôsobiacich v aplikačnej praxi, sme dospeli k názoru, že povedomie o hybridných hrozbách na národnej úrovni nie je dostatočné. Z daného vyplýva, že hypotéza H1 bola na základe realizácie výskumu falzifikovaná.

Na základe falzifikácie prvej hypotézy uvádzame podnety de lege ferenda na zlepšenie danej situácie. Jednou z podstatných foriem, ktoré podporujú efektívne uplatnenie zodpovednosti a dôslednosti pri aplikácii prvkov zabezpečenia informovanosti, posilnenie situačného povedomia o existencii a boji proti hybridným hrozbám je aj poskytovanie vzdelávania, resp. školení, kurzov.²¹⁴ Pretože ak budeme širokú verejnosť informovať a vzdelávať o možnostiach hybridných hrozieb a tiež ako predchádzať týmto hrozbám, či eliminovať ich, budeme vedieť zabezpečiť to, že akékoľvek hrozby budú mať na našu spoločnosť minimálny dopad. Šírenie osvetu a verejných informačných kampaní, odhaľovanie a reagovanie na dezinformácie, rozprávanie o prebiehajúcich trendoch, hrozbách a rizikách, špecifické varovania, rady a usmernenia pre verejnosť, využitie prieskumu verejnej mienky, zverejňovanie faktov a relevantných výsledkov výskumu nám zaručí

²¹³ COVELLO, V.T., MUMPOWER, J. 1998. Risk analysis and risk management: An historical perspective. <https://doi.org/10.1111/j.1539-6924.1985.tb00159.x>.

²¹⁴ SVOBODA, I. 2018. Efektivita vzdělávání bezpečnostního managementu ve státní správě. In: Vojenské reflexie, vědecko-odborný časopis, Liptovský Mikuláš: AOS GMRŠ, 2018, ročník XIII, číslo 2/2018, s. 142-150, ISSN 1336-9202.

budovanie efektívneho a čo najmenej ohrozeného štátu. Pretože naliehavosť riešenia problematiky hybridných hrozieb ovplyvňujúcich bezpečnostné prostredie na národnej úrovni si vyžaduje okrem nastavenia možností adekvátnej reakcie na elimináciu ich prejavov aj účinnú prevenciu.

2. KONCEPT HYBRIDNÝCH HROZIEB – ZÁKLADNÉ PILIERE

Pri prepojení skutočností prezentovaných počas predchádzajúcej kapitoly a s dôrazom na potrebu budovania odolnosti národného bezpečia voči hybridnému pôsobeniu ďalej budeme verifikovať hypotézu H2, ale aj charakterizovať koncept hybridného pôsobenia a jeho primárne zložky. Dané budeme uskutočňovať so zreteľom, že pri realizácii efektívneho predchádzania hybridným hrozbám je opodstatnené poznať a skúmať základné piliere konceptu hybridných hrozieb. Koncept hybridných hrozieb, resp. jeho štyri základné piliere sú klasifikované na aktérov (kto) a ich strategické ciele, domény (kde), nástroje (ako) a fázy hybridného pôsobenia.

V nasledujúcom texte sa budeme sústreďiť na špecifikáciu jednotlivých pilierov s cieľom popisu, na základe vedeckých poznatkov a poznatkov získaných z riadených rozhovorov, konceptu hybridných hrozieb. Máme za to, že práve pri realizácii efektívneho predchádzania hybridným hrozbám je opodstatnené poznať a skúmať základné piliere konceptu hybridných hrozieb, ako nám to potvrdili aj odborníci z aplikačnej praxe. Totiž práve koncept hybridných hrozieb a jeho štyri základné piliere jasne vymedzujú charakter hybridného pôsobenia, ktoré je potrebné, aby poznali aj samotní príslušníci Policajného zboru, zamestnanci verejnej správy, ale aj široká verejnosť. Práve aj takéto adresné poznanie je efektívnym predpokladom pre vymedzenie potreby vnímania konceptu hybridných hrozieb na národnej úrovni.²¹⁵

Tak ako vyplýva z realizovaného výskumu a poznatkov čerpaných z odbornej literatúry, aktér hybridnej hrozby je pôvodca, resp. šíriteľ hybridnej hrozby. Aktéri hybridných hrozieb využívajú kombináciu rôznych nástrojov s cieľom dosiahnuť vopred určené strategické ciele. Tieto strategické ciele majú jasný charakter a preto aj činnosť aktérov je zreteľne a určito, v úvodných fázach nebadane, zadefinovaná. Dosiahnutie uvádzaného strategického cieľa je podmienené aj nástrojmi, ktoré aktéri využívajú. Práve podľa toho aké nástroje využívajú, vieme následne aj diferencovať samotných aktérov na štátnych, neštátnych a samozrejme vieme podľa uvádzaného vymedziť aj ich ciele. Považujeme za dôležité podotknúť, že každý nástroj, ktorý využívajú aktéri sa zameriava najčastejšie na viacero dôležitých domén, ale tiež i na citlivé „rozhranie“, resp. „hranicu“ týchto domén. Sledovaný cieľ sa snažia dosiahnuť buď priamym alebo postupným účinkom. Z uvádzaného je zrejmé, že dosiahnutie cieľov nie je iba o konflikte, resp. porážke konkurenčných štátov, ale zahŕňa aj neštátnych aktérov, ktorých praktiky nie sú namierené na vojenské získanie územia, ale na získanie kontroly obyvateľstva.²¹⁶

Podstatné v súvislosti s uvádzanými skutočnosťami je odôvodnené zdôrazniť, práve v súvislosti s tým, že hybridné hrozby sú prezentáciou kreatívneho spôsobu prepojenia nových, starých nástrojov a stávajú sa dôležitým taktickým konaním, nástrojom, pre tých, ktorým chýbajú schopnosti alebo príležitosti presadiť svoje strategické záujmy inak. Takýto druh „sily“, „nástroja“

²¹⁵ CULLEN, P. et al. 2021. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 58 p. <http://www.doi.org/10.2760/44985>.

²¹⁶ SMITH, H. 2017. In the era of hybrid threats: Power of the powerful or power of the “weak”? Hybrid CoE. <https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-October-2017.pdf>.

je možné nazvať aj silou alebo nástrojom slabých. Pretože ak aj ten najslabší aktér dokáže účelne skombinovať nástroje útoku, ktoré má k dispozícii, dokáže prostredníctvom nich zaútočiť aj na toho najsilnejšieho súpera. Takáto kombinácia nástrojov útoku napomáha aktérovi k dosiahnutiu jeho strategického cieľa bez jeho detegovania, bez odporu voči nemu a bez akejkoľvek reakcie na jeho útok. Zároveň, využitie sily hybridných hrozieb umožňuje aktérovi minimalizovať riziko otvoreného konfliktu a dosiahnutie svojho strategického cieľa čo najefektívnejšie.

Aktéri hybridných hrozieb sa preto často prikláňajú k ovplyvňovaniu samotného rozhodovacieho procesu, rozhodovacieho centra, v rámci ich cieľa. Konkrétne môže ísť, napr. o vplyv na rozhodovanie v malom rozsahu, ale aj na rozhodovanie veľkého rozsahu. V príklade môže ísť o vplyv na obchodné operácie, ale môžeme hovoriť aj napr. o vplyve na konanie a rozhodnutia jednotlivcov počas volieb, rozhodnutiach tých, ktorí praktizujú, ktorí formujú politiky a legislatívu, ktorí vykonávajú činnosť vo verejnom záujme, v štátnom záujme a pod. Je však dôležité zdôrazniť, že konanie aktéra môže byť úspešné aj v prípade, ak využije iba niektoré, vybrané, prvky hybridných hrozieb a preto je potrebné bezpochyby skúmať a sledovať aj počiatkové štádiá vplyvu hybridných hrozieb prostredníctvom ich aktérov. Tak ako nám bolo uvádzané aj odborníkmi z aplikačnej praxe, činnosť aktérov hybridných hrozieb je veľmi ťažko identifikovateľná, ba priam nemožná ak nie je jasné, zrejmé, identifikujúcim subjektom, ako sa môže aktér správať, aké metódy, formy a nástroje môže využívať pri hybridnom pôsobení a snahe dosiahnuť strategický cieľ.²¹⁷

Cieľom aktérov hybridného pôsobenia je ovplyvniť systémové zraniteľné miesta demokracie za využitia všetkých nástrojov, ktoré majú k dispozícii. Tak ako nám deklarovali aj zamestnanci verejnej správy poznanie o aktéroch im nebolo zjavné a považujú ho za primárne pri poznávaní konceptu hybridných hrozieb pretože aj demokratické štáty sa môžu stretnúť s interferenciou operácií z iných demokratických štátov, ale v takýchto prípadoch je potrebné rozlišovať výrazné rozdiely medzi činnosťou demokratických a autoritárskych štátov. Na základe konkrétneho postavenia aktéra hybridného pôsobenia klasifikujeme aktérov na štátnych a neštátnych. Štátnymi aktérmi sú autoritárske štáty, ktoré čoraz častejšie využívajú hybridné hrozby ako nástroj v boji proti demokratickým štátnym systémom, pretože ich vnímajú ako existenčnú hrozbu pre svoje mocenské postavenie. Toto vnímanie je jedným z dôvodov, prečo cítia potrebu pokúsiť sa podkopať a oslabiť schopnosti demokratických štátov.

Jednou z ich hlavných aktivít je manipulatívne zasahovanie do informačnej domény a to prostredníctvom najpoužívaniejšieho nástroja - manipulácie prostredníctvom dezinformácií na sociálnych sieťach, ktorá zvyšuje šance ovplyvniť a zacieliť na určité publikum aj prostredníctvom sofistikovaných techník mikrotargetingu. Môže ísť napr. o prispôbenie reklám osobnostným črtám občanov. Výsledky ukazujú, že občania sú silnejšie presviedčaní politickými reklamami, ktoré zodpovedajú ich vlastným osobnostným črtám. Tieto zistenia následne slúžia tiež ako relevantné podnety do významnej akademickej a spoločenskej diskusie. Pretože mikrotargeting je

²¹⁷ PRISM, S. M. 2019. Countering Hybrid Warfare: So What for the Future Joint Force? Vol. 8, No. 2, pp. 82-99. <https://www.jstor.org/stable/26803232>.

možné označiť za plošné využitie individuálnych psychometrických informácií o veľkom množstve konkrétnych jedincov populácie v politickej alebo marketingovej kampani.²¹⁸

Následne špecifikuje typy štátnych aktérov, ktorí využívajú aktivity hybridnej hrozby ako podporného mechanizmu pre rôzne politiky a na presadzovanie strategických záujmov. Klasifikujeme ich na revizionistov a darebákov, resp. revizionistické a darebácke štáty. Pri definícii revizionistov je možné hovoriť o skutočnosti, že aktér súpera ovplyvní tak, že súper je presvedčený o svojom konaní a má za to, že to bolo z jeho vôle a v podstate dobrovoľne koná tak, ako si aktér želá bez povšimnutia ovplyvňovania. Darebácke štáty sú prezentované paranoidným odchyľovaním sa od pravidiel reálnych politík, čo podľa bezpečnostných stratégií nemôže vyústiť v nič iné ako vo vojnový konflikt. Darebácke štáty, resp. aktéri hybridného pôsobenia sa vyznačujú aj tým, že národné bohatstvo zneužívajú pre osobný prospech vodcov alebo pre megalomanské plány na získanie zbraní hromadného ničenia. Darebácke štáty využívajú hybridné hrozby na to, aby prispeli k rozpadu súčasného systému a pretvorili ho na podobu fungovania svojho režimu. Tiež významnú úlohu v týchto prípadoch zohrávajú finančný zisk a vôľa aktéra uškodiť.²¹⁹

Po špecifikácii štátnych aktérov je následne tiež veľmi dôležité charakterizovať, už nami spomínaných, neštátnych aktérov, ktorí taktiež vytvárajú koncept hybridných hrozieb. Neštátni aktéri na rozdiel od štátnych aktérov môžu byť pôvodcami hybridných hrozieb vo svojom vlastnom záujme s vlastnými strategickými cieľmi. Títo neštátni aktéri môžu byť zároveň „proxy“ aktérmi (zástupnými), ktorých využívajú štátni aktéri na naplnenie svojich strategických cieľov a sťažujú tým svoju skutočnú identifikáciu a atribúciu. „Proxy“ aktéri môžu byť motivovaní finančne, ideologicky a môže ísť o záujmovú skupinu, hackerov, ale aj o jednotlivcov, ktorí s cieľom hybridného pôsobenia vytvárajú konkrétne aktivity.

Ďalším pilierom v rámci poznania konceptu hybridných hrozieb, ktorý je potrebné špecifikovať sú nástroje hybridných hrozieb. Prostredníctvom nástrojov sa snažia aktéri dosiahnuť svoj strategický cieľ tak, aby vyvinuli čo najnižšiu snahu a zároveň dosiahli svoj cieľ. V súčasnosti je identifikovaných približne 40 nástrojov hybridného pôsobenia, avšak vzhľadom na aktuálny progres samotných hybridných hrozieb je vysoký predpoklad, že počet týchto nástrojov sa bude zvyšovať priamo úmerne s rozvojom aj samotných hybridných hrozieb. Medzi nástroje hybridného pôsobenia môžeme zaradiť - fyzické operácie proti infraštruktúre, vytváranie a využívanie závislosti na infraštruktúre (vrátane civilno-vojenskej závislosti), vytváranie alebo využívanie ekonomických závislostí, priame zahraničné investície, priemyselnú špionáž, narúšanie národného hospodárstva protivníka, ale aj napr. ovplyvňovanie volieb. Konkrétne nástroje hybridného pôsobenia teda napomáhajú a slúžia aktérom na dosiahnutie požadovaného cieľa čo najefektívnejším spôsobom. Poznanie konkrétnych nástrojov je kľúčové aj v rámci poznania samotných hybridných hrozieb, tak ako nám to uviedli aj odborníci z aplikačnej praxe, ale aj samotní príslušníci Policajného zboru a zamestnanci verejnej správy, ktorých sa to bytostne dotýka

²¹⁸ ZAROUALI, B., DOBBER, T., DE PAUW, G., & de VREESE, C. 2022. Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. *Communication Research*, 49(8), 1066-1091. <https://doi.org/10.1177/0093650220961965>.

²¹⁹ CULLEN, P. et al. 2021. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 58 p. <http://www.doi.org/10.2760/44985>.

v ich každodennej práci. Pretože, kľúčové je, že samotné používanie nástrojov hybridných hrozieb môže slúžiť na dosiahnutie konkrétnych cieľov aj bez formálneho vyhlásenia vojny.²²⁰

Ako tretí pilier konceptu hybridných hrozieb identifikujeme domény, ktoré sú cieľom hybridných hrozieb. Na domény hybridných hrozieb pôsobí najčastejšie kombinácia nástrojov používaných aktérmi. Charakteristické je, že každý nástroj sa zameriava na rozhranie medzi doménami a využíva ich zraniteľnosť. Tak, ako bolo zistené počas nami realizovaného výskumu, domény sú kľúčovými oblasťami národnej bezpečnosti a rozhodovacej schopnosti štátu, na ktoré sa zameriavajú nástroje hybridných hrozieb. Toto je práve ten dôvod, prečo je tak dôležité identifikovať oblasti záujmu, resp. kritické oblasti, domény, na ktoré hybridné hrozby pôsobia a ktoré by mal štát zabezpečiť proti aktivitám hybridných hrozieb, keďže spolu úzko súvisia. Keďže pri vplyve hybridných hrozieb na spoločnosť ide o veľmi multiinštitucionálne a viacdimenzionálne vnímanie aj skúmanie konkrétnych domén, je potrebné, aby bolo nastavené na úroveň viacerých okolností. Domény by sa nemali skúmať, vnímať, oddelene, ale v súvislostiach, pretože pôsobenie na jednu doménu vyvoláva následný dopad na inú doménu. Dovoľujeme sa ešte zmieniť v súvislosti s doménami hybridných hrozieb, že špecifické postavenie vo vzťahu k uvedeným nástrojom a doménam má kybernetický priestor, pretože predstavuje špecifické prostredie, kde sa jednotlivé dimenzie moci prelínajú a jeho význam pre fungovanie štátov a ekonomík je kritický. Kybernetické útoky umožňujú zasiahnuť a ohroziť fungovanie verejnej správy, ktorej infraštruktúry, finančného sektora, môžu ohroziť bezpečnosť dôležitých objektov, sú prostriedkom špionáže, dezinformačnej kampane, atď. V prípade národných bezpečnostných plánov zahŕňa počítačovú kriminalitu, propagandu, špionáž, ovplyvňovanie, terorizmus a dokonca aj samotný boj. Poskytuje nové mechanizmy, ktorý môžu zvýšiť rýchlosť, šírenie a silu útoku a zabezpečiť anonymitu. Menší aktéri majú väčšie možnosti na presadenie svojej moci v kybernetickom priestore, než v mnohých tradičných oblastiach svetovej politiky. Kybernetická doména sa týka informačného prostredia pozostávajúceho zo vzájomne prepojených sietí infraštruktúr informačných technológií, vrátane hardvéru, softvéru, údajov, protokolov a informácií vrátane internetu, telekomunikačných sietí, počítačových systémov a zabudovaných procesorov a kontrolných mechanizmov. Kybernetická doména sa v súčasnosti pomerne rýchlo mení. Nástroje, ktoré môže protivník uplatniť, sú zamerané na spôsobenie degradácie, narušenia alebo zničenia sietí alebo na prístup k údajom a informáciám. Prístup k informáciám môže byť tiež cieľom protivníka s cieľom zhromažďovať spravodajské informácie a znižovať možnosť detekcie. Digitálna transformácia môže umožniť použitie kybernetických nástrojov v mnohých ďalších doménach.²²¹

Pri realizácii výskumu sme identifikovali, že aj zamestnancom verejnej správy, aj príslušníkom Policajného zboru nie sú úplne zrejmé jednotlivé fázy hybridného pôsobenia (vrátane typov činností pozorovaných v každej fáze). Preto považujeme za dôležité ich jasne vyšpecifikovať. Prvou fázou je fáza prípravy. Vo fáze prípravy je konečným cieľom aktéra hybridnej hrozby, že cieľ dobrovoľne urobí škodlivé rozhodnutia a nesprávne konanie tak, ako si aktér želá. Podstatou tejto fázy je realizovať aktivity tak, aby následne mohol svoje hybridné pôsobenie zintenzívniť a efektívnejšie dosiahnuť svoj strategický cieľ. Počas tejto fázy sú aktivity aktéra hybridného

²²⁰ SANZ-CABALLERO, S. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun* 10, 360 (2023). <https://doi.org/10.1057/s41599-023-01864-y>.

²²¹ NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/domeny/index.html>.

pôsobenia veľmi ťažko detekovateľné, a nie je zjavné určiť ich zámer. Iba v ojedinelých prípadoch sa podarí ohrozenému subjektu identifikovať aktéra hybridného pôsobenia v tejto fáze. Cieľom týchto aktivít aktéra je prinútiť štát, resp. terč hybridného pôsobenia, aby začal robiť škodlivé rozhodnutia v súlade so záujmami aktéra. Účinným nástrojom je napríklad realizácia účelnej ochrany bezpečnosti jednotlivcov, spoločnosti, organizácií a všetkých zložiek, ktoré môžu byť terčom aktéra a teda aj hybridných hrozieb.²²²

V tejto fáze sa využíva podvedomé ovplyvňovanie rozhodnutí na základe predchádzajúcich informácií. Dochádza k príprave vedomia príjemcov akceptovať dezinformácie ako autoritatívne a pravdivé, ktorá sa realizuje pravidelným zahlcovaním pozornosti cieľovej skupiny osôb veľkým množstvom dezinformácií šírených rôznymi spôsobmi, napríklad dlhodobým kultivovaním dezinformačných webov, ktoré majú šíriť naratívy protivníka, ktoré sú v rozpore so zahraničnopolitickým smerovaním cieľa.²²³

Následne po tejto fáze je možné identifikovať etapu destabilizácie. Táto fáza je štádiom, v ktorom aktér zintenzívňuje svoju činnosť, napr. spôsobom kampane, teda realizáciou viacerých operácií. Cieľom aktéra v rámci tejto fázy je získať čo najviac informácií, aby mohol svoj cieľ čo najefektívnejšie ohroziť. V tejto fáze sú aktivity aktéra čoraz viditeľnejšie, avšak aktér sa k ich vykonávaniu nepriznáva a cieľový štát nemá dostatok dôkazov na to, aby to dôveryhodne preukázal. Počas tejto fázy sa môže v malej miere vyskytovať aj prvok násilia. Destabilizačná fáza je štádiom, v ktorom aktér buď svoje aktivity stupňuje tak, ako bolo uvedené alebo použije len jednu operáciu a potom deeskaluje a vráti sa do počiatočnej fázy. Aj keď sa táto aktivita stane viditeľnejšou, aktér má stále dostatočný priestor na hodnoverné popretie jeho zodpovednosti za takúto aktivitu.²²⁴

Ďalšou etapou je fáza nátlaku alebo aj špecifikovaná ako hybridná vojna. V tejto fáze prekračujú všetky aktivity aktéra rámec nenápadnosti a možno ju označiť za hybridnú vojnu. Hybridná vojna predstavuje tzv. „tvrdý koniec“ eskalačného spektra činností hybridných hrozieb. Hybridná vojna je v zásade kombináciou skrytých a otvorených vojenských operácií v kombinácii s politickými a ekonomickými opatreniami, rozvratom, informačnými a dezinformačnými operáciami, propagandou, falošnými správami, skrytým alebo zjavným nasadením špeciálnych síl, ako aj armády, ale aj kybernetických útokov. Kľúčovým prvkom je použitie sily na dosiahnutie aktérovho zámeru prostredníctvom teroru, sabotáže alebo konvenčnej vojny. Fáza hybridnej vojny mení charakter celého konfliktu na vojnu. V tejto fáze tiež ide už o vyvíjanie otvoreného nátlaku. Hoci aktivita je spravidla už viditeľná, nie vždy je možné hodnoverným spôsobom určiť zodpovednosť konkrétneho aktéra. Hlavnou črtou hybridného pôsobenia v tejto fáze bude, napr. nasadenie

²²² KORAUS, A., KRÁSNÁ, P., ŠIŠULÁK, S., VESELOVSKÁ, S. 2023. Integrated security strategies in the context of hybrid threats in the Slovak Republic. *Entrepreneurship and Sustainability Issues*, 11(1), 233-250. [http://doi.org/10.9770/jesi.2023.11.1\(14\)](http://doi.org/10.9770/jesi.2023.11.1(14)).

²²³ NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>.

²²⁴ NBAC. 2023. Hybridné hrozby. Krátky terminologický slovník. [online]. [cit. 2023.10.09.] Dostupné na internete: NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://mmqx.sis.gov.sk/storage/files/HH-Slovník-2023.pdf>.

vojenských jednotiek do bojových operácií bez vojenských insígnií preukazujúcich ich príslušnosť ku konvenčným ozbrojeným silám aktéra.²²⁵

Pri zhodnotení overovania hypotézy H2 je možné konštatovať, že táto hypotéza bola potvrdená. Pri realizácii efektívneho predchádzania hybridným hrozbám je totiž opodstatnené poznať a skúmať základné piliere konceptu hybridných hrozieb tak, ako nám to potvrdili aj konkrétny účastníci riadených rozhovorov. V súvislosti s uvádzaným špecifikujeme aj konkrétne podnety do budúcnosti, pretože máme za to, že pokiaľ sa vnímanie konceptu hybridných hrozieb nebude vyvíjať, jednotlivé kompetentné subjekty nebudú prijímať adekvátne riešenia a nebude možné vytvárať dostatočný priestor na elimináciu hybridného pôsobenia na národnej úrovni. Kompetentnosť jednotlivých subjektov by si mali identifikovať hlavne subjekty, ktorých sa to týka, či už ide o štátne orgány, médiá, ale aj politické subjekty. Nie je totiž účelné, ak kompetentné orgány nespokupujú, či niekedy si ani neuvedomujú zodpovednosť v rámci predchádzania a eliminácie hybridného pôsobenia.

3. VNÍMANIE ZRANITEĽNOSTI SLOVENSKA VOČI HYBRIDNÝM HROZBÁM A PODNETY DE LEGE FERENDA

V nasledujúcej kapitole by sme sa radi zamerali na konkrétnu špecifikáciu potreby vnímania jednotlivých nedostatkov, resp. zraniteľných miest, ktoré je možné identifikovať na národnej úrovni v rámci prístupu k eliminácii hybridného pôsobenia. Pretože bez zjavnej identifikácie nedostatkov nie je možné efektívne napredovať a vytvárať vhodné podmienky na to, aby hybridné ohrozenia mali čo najnižší vplyv na bezpečnosť našej krajiny.

Hybridné hrozby a ich dopad je náročné pochopiť bez priamej referencie na slabiny, ktoré formujú predstavu o probléme. Hlavným cieľom hybridných útokov je zmeniť podstatu subjektu tak, ako sme už uviedli. V praxi to znamená, že pôvodca útokov sa snaží narušiť spoločenskú súdržnosť krajiny, politický systém, bezpečnostné štruktúry, či celkové fungovanie štátu v medzinárodnom prostredí. Hybridné pôsobenie je v každom prípade namierené na slabé miesta krajiny, na hranice domén a prispôbované tak, aby čo do najväčšej miery využili slabiny a špecifiká cieľového systému. Zraniteľnosť Slovenskej republiky je možné vnímať v nedostatočných kapacitách v oblasti strategickej komunikácie na úrovni ústredných orgánov štátnej správy, tiež v poddimenzovaných analytických kapacitách v oblasti kybernetickej bezpečnosti a v absencii dostatočne konkrétnych a merateľných opatrení na zlepšenie súčasného stavu v tejto oblasti. Zraniteľnosť na národnej úrovni tkvie aj v nedostatočnej pozornosti kladenej na energetickú infraštruktúru v kontexte hybridných hrozieb a dosahu prípadného útoku na uvádzanú infraštruktúru nad rámec prerušenia dodávok energií. Tiež je veľmi podstatné, že na národnej úrovni absentuje právna úprava polovojenských/paramilitárnych skupín, ale aj nedostatočné zohľadnenie prvku cudzej moci pri iných typoch ohrození bezpečnosti a stability Slovenskej republiky. Absentuje tiež zohľadnenie iných, než čisto finančných motívov v anti-korupčnej legislatíve a absentuje aj špecifická právna úprava vedenia volebnej kampane v prostredí internetu a sociálnych sietí.

²²⁵ MUMFORD, A., & CARLUCCI, P. 2023. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2), 192-206. <https://doi.org/10.1017/eis.2022.19>.

V súvislosti s opodstatneným predpokladom, že vplyv hybridných hrozieb na území Slovenskej republiky bude naďalej pokračovať, čoho dôkazom sú aj nami vymedzené skutočnosti, máme za to, že je potrebné charakterizovať odporúčania do budúcnosti.

✓ Prijat' komplexný prístup v oblasti strategickej komunikácie, zahŕňajúci všetky relevantné zložky verejnej správy. Zriaďovať špecializované národné kapacity so zameraním na strategickú komunikáciu vo všetkých relevantných rezortoch. Vytvoriť dostatočné analytické kapacity v oblasti kybernetickej bezpečnosti, ktoré by sa zaoberali tvorbou verejných politík. Prijat' akčný plán v oblasti kybernetickej bezpečnosti s jasnými, merateľnými kritériami. Systematicky riešiť otázku hybridných a kybernetických hrozieb v strategických dokumentoch, ktoré sa venujú energetickej politike, resp. energetickej bezpečnosti.

✓ Klásť väčší dôraz na špecifiká energetického sektora, ktorý je odlišný od ostatných oblastí kritickej infraštruktúry, pretože hybridné hrozby v tejto oblasti majú dôsledky nielen pre energetickú bezpečnosť, ale aj pre tzv. „hard security“. Identifikovať hybridné hrozby a riešenia nielen na úrovni verejnej, štátnej správy, ale aj v rámci súkromného energetického sektora, ktorý zohráva dôležitú úlohu pri zabezpečovaní energetickej bezpečnosti. Zahnúť inovatívne „smart“ technológie do diskusie o možných hybridných hrozbách v oblasti energetickej bezpečnosti. Novelizovať legislatívu v oblasti zbraní a streliva a prijať legislatívu upravujúcu pôsobenie polovojenských skupín a ich podporu zo strany cudzej moci.

✓ Dôsledne uplatňovať ustanovenia Zákona č. 300/2005 Z. z. Trestného zákona v znení neskorších predpisov týkajúce sa účasti na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu a jej podpory.²²⁶ Posilňovať medzinárodné, ale aj domáce nástroje na odhaľovanie podozrivých finančných tokov cez schránkové firmy a daňové raje v kontexte strategickej korupcie s politickými cieľmi. Analyzovať nefinančné aspekty korupcie a zakotviť pojem strategická korupcia do verejných politík a legislatívy. Prijat' legislatívu, ktorá upraví transparentné financovanie politických strán počas celého volebného obdobia, nielen v čase trvania predvolebnej kampane.

✓ Upraviť okruh subjektov oprávnených financovať volebné kampane počas volieb do Národnej rady Slovenskej republiky a Európskeho parlamentu podobným spôsobom, ako je to v prípade prezidentských volieb. Zaviesť povinnosť informovania o zadávateľovi online politických reklám aj v čase mimo predvolebnej kampane.²²⁷

Špecifikovaná hypotéza H3, ktorá znela: „Vnímanie zraniteľnosti Slovenska voči hybridným hrozbám je podmienené vymedzením konkrétnych odporúčaní, ktoré sú účelné pre jej elimináciu“ sa nám potvrdila, pretože bez relevantných poznatkov o zraniteľných oblastiach na národnej úrovni nevieme následne identifikovať konkrétne odporúčania pre možnú zmenu a jej efektívne uplatnenie. Iba pri zrejmom vnímaní a uvedomení si nedostatkov, vieme následne analyzovať a aplikovať konkrétne odporúčania, ktoré sú využiteľné v aplikačnej praxi a v činnosti príslušníkov

²²⁶ ČENTÉŠ, J. a kol. 2018. Trestný zákon Veľký komentár. Vydavateľstvo EUROKODEX, s. 547.

²²⁷ KLINGOVÁ, K., KUPKOVÁ, I., MILO, D., MIŠÍK, D., PIŠKO, M., SIVÁK, J. 2019. HYBRIDNÉ HROZBY NA SLOVENSKU. Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach. [online]. [cit. 2023.10.08.] Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf.

Policajného zboru a zamestnancov verejnej správy. Apelujeme na tiež fakt, že právna úprava v tejto oblasti musí byť bezpodmienečne zrozumiteľná, jednoznačná, precízna a tým bude minimalizované riziko prípadných problémov vyskytujúcich sa v aplikačnej praxi.²²⁸

ZÁVER

Problematica hybridných hrozieb je veľmi aktuálnou a veľmi častou témou, s ktorou sa stretávame na akademickej úrovni v rámci diskusií s aktívnymi príslušníkmi Policajného zboru alebo zamestnancami verejnej správy, ale aj na odbornej úrovni v kontexte obsahov medzinárodných vedeckých konferencií. Veríme, že nami predložená vedecká štúdia prispeje do hodnotnej diskusie spojenej s problematikou hybridných hrozieb aj v aplikačnej praxi. Máme za to, že rozvíjanie poznatkov z aplikačnej praxe a realizácia výskumu je tým správnym postupom pre budovanie národnej odolnosti voči hybridným hrozbám a napomáha odôvodnenej potrebe vnímania konceptu hybridných hrozieb na národnej úrovni. Máme za to, že je tiež veľmi podstatné predikovať odporúčania do budúcnosti, ktoré danému stavu budú napomáhať a preto sú jednotlivé, konkrétne, odporúčania de lege ferenda súčasťou textu predloženej vedeckej štúdie. Konceptualizácia potreby vnímania podstaty hybridných hrozieb na národnej úrovni na základe vedeckého výskumu je založená na predpoklade, že vnímaná úroveň týchto hrozieb reflektuje na aktuálnu bezpečnostnú situáciu. V tomto kontexte je táto potreba vnímania hybridných hrozieb výsledkom predchádzajúcich skúseností z aplikačnej praxe a poznatkov z realizovaných vedeckých výskumov.

Zdroje

1. COVELLO, V.T., MUMPOWER, J. 1998. Risk analysis and risk management: An historical perspective. <https://doi.org/10.1111/j.1539-6924.1985.tb00159.x>.
2. CULLEN, P. et al. 2021. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 58 p. <http://www.doi.org/10.2760/44985>.
3. CULLEN, P. et al. 2021. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 58 p. <http://www.doi.org/10.2760/44985>.
4. ČENTĚŠ, J. a kol. 2018. Trestný zákon Veľký komentár. Vydavateľstvo EUROKODEX. 1008 s. ISBN 978-80-81550-76-8.
5. Hybrid COE. 2023. [online]. [cit. 2023.10.15.] Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.
6. JACUCH, A. 2020. RESILIENCE IN THE EU AND NATO'S STRATEGIES. Copernicus Journal of Political Studies 2020. No. 1/2020, pp. 5–26. ISSN 2299-4335. <http://dx.doi.org/10.12775/CJPS.2020.001>.
7. KLINGOVÁ, K., KUPKOVÁ, I., MILO, D., MIŠÍK, D., PIŠKO, M., SIVÁK, J. 2019. HYBRIDNÉ HROZBY NA SLOVENSKU. Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach. [online]. [cit. 2023.10.08.] Dostupné na internete: https://www.globsec.org/sites/default/files/2018-01/Hybridne-hrozby-na-SR_6-tematickych-oblasti.pdf.

²²⁸ VRTÍKOVÁ, K. 2023. Zabezpečovanie informácií dôležitých pre trestné konanie ako relevantný nástroj odhaľovania organizovanej kriminality 1. časť - Informačno-technické prostriedky. In Bulletin slovenskej advokácie / Bulletin SAK - 2023 / Bulletin SAK - 3/2023. [online]. [cit. 2023.10.08.] Dostupné na internete: <https://www.epi.sk/odborny-clanok/zabezpecovanie-informacii-dolezitych-pre-trestne-konanie-ako-relevantny-nastroj-odhalovania-organizovanej-kriminality-1-cast.htm>.

8. KORAUS, A., KRÁSNÁ, P., ŠIŠULÁK, S., VESELOVSKÁ, S. 2023. Integrated security strategies in the context of hybrid threats in the Slovak Republic. *Entrepreneurship and Sustainability Issues*, 11(1), 233-250. [http://doi.org/10.9770/jesi.2023.11.1\(14\)](http://doi.org/10.9770/jesi.2023.11.1(14)).
9. KORYSTIN, O., SVYRYDIUK, N. 2021. Activities of Illegal Weapons Criminal Component of Hybrid Threats. <http://www.doi.org/10.2991/aebmr.k.210320.016>.
10. MUMFORD, A., & CARLUCCI, P. 2023. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2), 192-206. <https://doi.org/10.1017/eis.2022.19>.
11. NBAC. 2023. Hybridné hrozby. Krátky terminologický slovník. [online]. [cit. 2023.10.09.] Dostupné na internete: NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://mmqx.sis.gov.sk/storage/files/HH-Slovník-2023.pdf>.
12. NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/domeny/index.html>.
13. NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: NBÚ. 2023. [online]. [cit. 2023.10.09.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>.
14. PRISM, S. M. 2019. Countering Hybrid Warfare: So What for the Future Joint Force? Vol. 8, No. 2, pp. 82-99. <https://www.jstor.org/stable/26803232>.
15. SANZ-CABALLERO, S. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun* 10, 360 (2023). <https://doi.org/10.1057/s41599-023-01864-y>.
16. ŠÍLI, V. 2021. Hybrid threats: modern perception and tactics. [online]. [cit. 2023.10.10.] Dostupné na internete: <https://www.ceeol.com/search/article-detail?id=859611>.
17. SMITH, H. 2017. In the era of hybrid threats: Power of the powerful or power of the “weak”? Hybrid CoE. <https://www.hybridcoe.fi/wp-content/uploads/2017/12/Strategic-Analysis-October-2017.pdf>.
18. SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADY. Spoločný rámec pre boj proti hybridným hrozbám, reakcia Európskej únie. 2016. [online]. [cit. 2023.10.10.] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52016JC0018>.
19. SVOBODA, I. 2018. Efektivita vzdělávání bezpečnostního managementu ve státní správě. In: *Vojenské reflexie, vědecko-odborný časopis*, Liptovský Mikuláš: AOS GMRŠ, 2018, ročník XIII, číslo 2/2018, s. 142-150, ISSN 1336-9202.
20. TREVERTON, G. F., THVEDT, A., CHEN, A. R., LEE, K., MCCUE, M. 2018. Addressing Hybrid Threats. [online]. [cit. 2023.10.15.] Dostupné na internete: <https://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574</div>>.
21. VRTÍKOVÁ, K. 2023. Zabezpečovanie informácií dôležitých pre trestné konanie ako relevantný nástroj odhaľovania organizovanej kriminality 1. časť - Informačno-technické prostriedky. In *Bulletin slovenskej advokácie / Bulletin SAK - 2023 / Bulletin SAK - 3/2023*. [online]. [cit. 2023.10.08.] Dostupné na internete: <https://www.epi.sk/odborny-clanok/zabezpecovanie-informacii-dolezitych-pre-trestne-konanie-ako-relevantny-nastroj-odhalovania-organizovanej-kriminality-1-cast.htm>.
22. ZAROUALI, B., DOBBER, T., DE PAUW, G., & de VREESE, C. 2022. Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. *Communication Research*, 49(8), 1066-1091. <https://doi.org/10.1177/0093650220961965>.

KRIZOVÉ ŘÍZENÍ PŘI OHROŽENÍ HYBRIDNÍMI HROZBAMI; RIZIKA PRO BEZPEČNOST STÁTU

doc. Ing. Karel Kubečka, Ph.D., MBA, Ing. Paed-IGIP

AMBIS Praha, a.s. Vysoká škola, Lindnerova 1, 180 00 Praha

Abstrakt: Příspěvek pojednává o tzv. hybridních hrozbách, jako o aktuálním dění v současné době. Z textu je patrné, co vše je zahrnuto pod tento název „hybridní hrozby“, z čehož plyne také extrémně vysoké nebezpečí spolu s kybernetickými útoky spojenými s konvenčními způsoby boje, propagandou a teroristickými útoky. Na praktickém příkladu pak řeší otázku stanovení míry rizika na základě dostupných informací a zabývá se otázkou, zda pro hodnocení míry rizika není vhodnější použití nelineárních závislostí, které přesněji ukazují na míru rizika. Ovšem na podkladě kvality vstupních údajů, které mohou být některou ze složek hybridního působení podstatně ovlivněny. V každém případě jde o shodu, že na relevantnosti informací je závislá bezpečnost našeho státu, Evropy a světa.

Klíčová slova: hrozby; hybridní hrozby; riziko; hodnocení rizik; bezpečnost.

ÚVOD

Náčelník štábu americké armády definoval v roce 2008 hybridní hrozbu jako protivníka, který zahrnuje „rozmanité a dynamické kombinace konvenčních, nelegálních, teroristických a kriminálních schopností“. Velitelství společných sil USA definuje hybridní hrozbu jako „protivníka, který současně a adaptivně zaměstnává na míru šitý mix konvenčních, neregulérních, teroristických a kriminálních prostředků, nebo činností v operačním bojovém prostoru“. Hybridní hrozba nebo vyzyvatel bývá spíše kombinace státních a nestátních aktérů než jedna entita.

Americká armáda definovala hybridní hrozbu v roce 2011 jako „různorodou a dynamickou kombinaci pravidelných sil, neregulérních sil, kriminálních živlů nebo kombinace těchto sil a prvků sjednocených za účelem dosažení vzájemně prospěšného výsledku. Podle evropského Centra excelence pro boj proti hybridním hrozbám, které bylo založeno v roce 2017, „hybridní hrozby jsou metody a činnosti zaměřené na zranitelná místa soupeře“, kde je rozsah metod a činností široký. Definice českých ministerstev jsou ještě méně konkrétní.

1. HYBRIDNÍ HROZBY

Hybridní hrozba, jak je v úvodu obecně uvedeno se v oblasti bezpečnosti týká kombinace různých prostředků a technik, které jsou využívány k útoku na cíl. Jedná se o kombinaci konvenčního a nekonvenčního boje, která zahrnuje různé aspekty, jako jsou kybernetické útoky, dezinformace, propagandu, sabotáže, terorismus **Chyba! Nenašel se žádný zdroj odkazov.** nebo vlastní hybridní válku.

1.1 Hybridní hrozby v ČR

Ministerstvem vnitra České republiky bylo zřízeno Centrum proti terorismu a hybridním hrozbám. Výhrady k centru vyjádřil bezpečnostní analytik a generál v záloze Andor Šándor **Chyba! Nenašel se žádný zdroj odkazov.** a další.

Hybridní hrozba je obzvláště nebezpečná, protože se soustředí na využití slabých míst a nedostatků v systému, aby dosáhla svých cílů. Může se jednat o ovlivňování veřejného mínění, destabilizaci politického systému, poškození ekonomiky nebo dokonce o vojenské útoky.

Takové hrozby mohou pocházet od států, teroristických organizací **Chyba! Nenašel sa žiaden z droj odkazov.**, hacktivistů nebo jiných subjektů, které mají zájem na oslabení nebo poškození cíle. Hybridní hrozby se často využívají v asymetrickém boji, kde slabší strana využívá nekonvenční prostředky k útoku na silnějšího soupeře.

Proti hybridním hrozbám je třeba přijmout komplexní a multidisciplinární přístup, který zahrnuje kybernetickou obranu, ochranu kritické infrastruktury, ochranu informačního prostoru a prevenci dezinformací. Spolupráce mezi zpravodajskými službami, vojenskými složkami a civilními institucemi je také klíčová pro účinnou reakci na hybridní hrozby.

1.2 Kritická infrastruktura a její ochrana

Kritická infrastruktura je soubor systémů, služeb a zařízení, které jsou nezbytné pro fungování společnosti a ekonomiky. Patří sem například energetické sítě, telekomunikační sítě, dopravní infrastruktura, vodní zdroje, zdravotní zařízení, finanční systém, potravinový řetězec apod. Ochrana kritické infrastruktury tedy zahrnuje opatření a strategie zaměřené na ochranu a zabezpečení klíčových prvků infrastruktury, které jsou nezbytné pro fungování společnosti **Chyba! Nenašel sa žiaden zdroj odkazov.** Patří sem dále například elektrárny, vodárny, telekomunikační sítě, dopravní systémy a další.

Ochrana kritické infrastruktury je důležitým úkolem státu a dalších relevantních aktérů, protože její narušení nebo selhání by mělo závažné dopady na společnost. Cílem ochrany kritické infrastruktury je minimalizovat riziko výpadků, sabotáží, teroristických útoků nebo jiných hrozeb, které by mohly mít vážné dopady na společnost. Ochrana kritické infrastruktury je významným tématem v současné době, protože hrozby vůči ní se stále zvyšují. Společnost a vlády musí spolupracovat a investovat do opatření, která zajistí, že kritická infrastruktura zůstane chráněna a spolehlivá i v případě různých hrozeb.

Ochrana kritické infrastruktury zahrnuje několik klíčových aspektů:

- **Identifikace a hodnocení rizik:** Je důležité identifikovat a analyzovat potenciální hrozby a rizika, kterým je kritická infrastruktura vystavena. To zahrnuje přírodní katastrofy, teroristické útoky, kybernetické útoky, technické poruchy apod. Na základě toho jsou přijata opatření pro minimalizaci těchto rizik.
- **Prevence:** Na základě identifikovaných rizik je třeba přijmout opatření k minimalizaci jejich pravděpodobnosti výskytu. To může zahrnovat například fyzickou ochranu zařízení, zabezpečení sítí a systémů, školení zaměstnanců, záložní plány a kontinuitu provozu.
- **Kybernetická ochrana:** Vzhledem k rostoucímu nebezpečí kybernetických útoků je důležité zajistit bezpečnost informačních systémů a sítí kritické infrastruktury. To zahrnuje například používání silných hesel, aktualizace softwaru, šifrování dat a další opatření.
- **Reakce a krizový management:** Pokud dojde k narušení kritické infrastruktury, je důležité rychle a efektivně reagovat. Je nutná připravenost na krizové **Chyba! Nenašel sa žiaden z droj odkazov.** situace a schopnost rychlé reakce; ty jsou klíčové pro ochranu kritické infrastruktury. To zahrnuje vytvoření a aktivaci plánů pro krizový management a pro řízení

krizových situací, spolupráci mezi různými zainteresovanými stranami, trénink personálu a spolupráci s dalšími organizacemi, koordinaci záchranných a opravných prací a informování veřejnosti.

- **Obnova a odolnost:** Po narušení kritické infrastruktury je třeba ji co nejdříve obnovit a zvýšit její odolnost proti budoucím hrozbám. To zahrnuje opravy a obnovu poškozených zařízení, aktualizaci bezpečnostních opatření a zlepšení systémů a procesů.
- **Fyzická ochrana:** Zahrnuje opatření zaměřená na zabezpečení fyzických prvků infrastruktury, jako jsou například ploty, kamery, bezpečnostní systémy a další. Cílem je zabránit neoprávněnému přístupu a ochránit infrastrukturu před možnými útoky.
- **Spolupráce a koordinace:** Ochrana kritické infrastruktury vyžaduje spolupráci různých subjektů, včetně vlády, provozovatelů infrastruktury, bezpečnostních složek a dalších. Koordinace a výměna informací jsou důležité pro úspěšnou ochranu kritické infrastruktury.

Ochrana kritické infrastruktury je složitý a neustále se vyvíjející proces, který vyžaduje spolupráci mezi různými aktéry, včetně vládních orgánů, soukromého sektoru a veřejnosti. Je nezbytné investovat do její ochrany a pravidelně aktualizovat opatření, aby se minimalizovalo riziko narušení a zajistila stabilita a bezpečnost společnosti.

2. HODNOCENÍ RIZIK, VYHODNOCENÍ RIZIK A ŘÍZENÍ RIZIK

Rizikové inženýrství [*risk engineering*] a management **Chyba! Nenašel sa žiaden zdroj odkazov.** rizika [*risk management*] jsou dvě velice úzce vzájemně provázané disciplíny lišící se náplní a cíli. Rizikové inženýrství přejímá od managementu rizika podněty a požadavky, následně pak analyzuje rizika. Management rizika s těmito riziky následně pracuje a ovládá je.

Riziková analýza [*risk assessment*] a management, tedy ovládání rizika, je poměrně nový, dynamicky rozvíjející se obor, který se stal zejména v zahraničí nedílnou součástí manažerských rozhodovacích procesů. Zabývá se mimo jiné získáváním a zpracováváním informací o možných nebezpečích, hrozbách ale i příležitostech, na základě, kterých je následně možné provádět zodpovědnější, informovanější rozhodnutí. Riziková analýza je tak procesem, který shromažďuje a zpracovává informace pro následný management rizik.



Obrázek 1: Ochrana chráněných zájmů proti napadení.

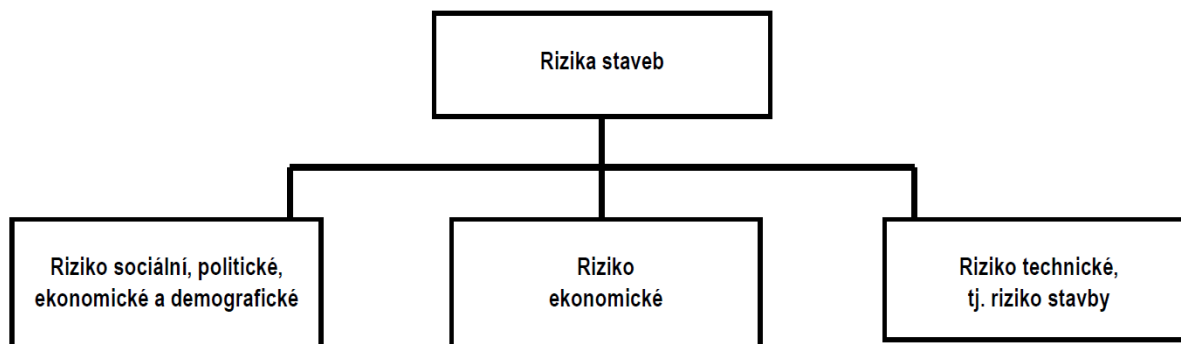
Postupy pro práci s riziky, jsou v současné době velmi dobře rozpracovány [4, 5]. Jedna z nejdůležitějších věcí při tomto posuzování je úplnost a preciznost. Osvědčené metody pro takovéto posouzení vycházejí z povahy expertních logicko-numerických metod. Samozřejmě i tyto metody pracují s obecnými zásadami (*Obrázek 1*).

Tyto obecné zásady (*Obrázek 1*) se vztahují k vlastnímu chráněnému zájmu, kterým je nejen finanční investice, ale také vlastní dopad do ekosystému, který může znamenat antropogenní havárii a rovněž tak v neposlední řadě ohrožení infrastruktury a kritické infrastruktury státu. V širším měřítku pak také s vlivem i na okolní státy z pohledu bezpečnosti. Proto také jednotlivé obecné fáze analýzy rizik je nutno aplikovat i na velké projekty z oblasti bezpečnosti.

Analýza rizik musí přinést odpověď na otázku:

- působení jakých hrozeb jsou aktiva (tedy chráněné zájmy a společnost, která tyto zájmy ochraňuje) vystavena,
 - do jaké míry a s jakou vážností, tedy jak hodně jsou chráněné zájmy společnosti, to znamená aktiva vůči těmto hrozbám zranitelná,
 - jaká je míra pravděpodobnosti, že daná konkrétní hrozba zneužije slabinu chráněného zájmu, to znamená – určitou zranitelnost aktiva a dále
 - jaký dopad by to na primárně chráněný zájem (aktivum) a následně společnost mohlo mít.
- V analýze rizik se používají obecně následující pojmy, které určují směr postupu řešení analýzy použitelné pro management těchto rizik. Jednotlivé milníky je potřeba řádně definovat a pracovat s nimi ve vší vážnosti:
- aktivum, tedy chráněný zájem (*asset*) – představuje vše co má pro společnost nějakou (prakticky jakoukoli) hodnotu a mělo by být odpovídajícím způsobem této hodnotě chráněno,
 - hrozba (*threat*) – je jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti chráněného zájmu, tedy aktiva a hledá možnost impaktu aktiva, což směřuje k vlastnímu narušení
 - zranitelnost (*vulnerability*) – je vlastnost chráněného zájmu, to znamená aktiva anebo slabina chráněného zájmu na kterékoli úrovni (fyzické, logické nebo administrativní bezpečnosti), která může být zneužita hrozbou k napadení chráněného zájmu.
 - riziko (*risk*) – představuje pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti.
 - opatření (*countermeasure*) – opatření na úrovni fyzické logické nebo administrativní bezpečnosti, které snižuje zranitelnost a chrání aktivum před danou hrozbou.
 - ohrožení (*exposure*) – je skutečnost, že existuje zranitelnost chráněného zájmu, která může být zneužita hrozbou pro napadení (narušení) aktiva
 - narušení (*breach*) – je situace, kdy, již došlo k narušení důvěrnosti, integrity nebo dostupnosti v důsledku překonání bezpečnostních opatření chránících aktiva.

Každá lidská činnost je zatížena určitým stupněm rizika. V činnosti souhrnně nazývanou jako „stavebnictví“ se potýkáme s celou řadou rizik **Chyba! Nenašel sa žiaden zdroj odkazov., REF p3 \h * MERGEFORMAT Chyba! Nenašel sa žiaden zdroj odkazov.** Tato rizika (*Obrázek 2*) vyplývají například ze sociálních podmínek daného regionu, demografického složení obyvatelstva regionu apod.



Obrázek 2: Základní rozdělení rizik pro stavební objekty jako součást infrastruktury anebo kritické infrastruktury státu.

2.1 Rizika v oblasti bezpečnosti

Pokud se jedná o oblast bezpečnosti (nebo zajištění bezpečnosti), je situace velmi složitá **Chyba! Nenašel sa žiaden zdroj odkazov.**, komplikovaná a mnohdy i z pohledu hybridního nebezpečí také nepřehledná. Rizika v oblasti bezpečnosti se v dnešní době týkají různých aspektů života, a to jak v reálném světě, tak i v online prostředí. Některá (jedny z mála) hlavních rizik zahrnují:

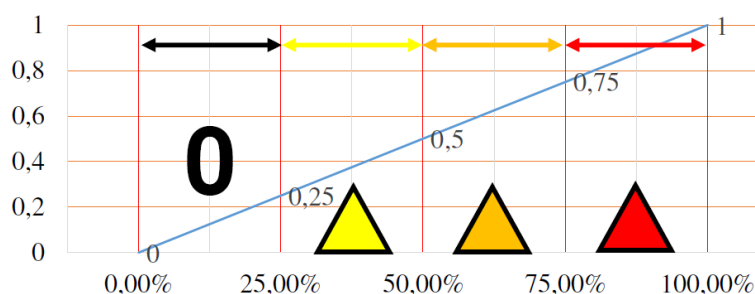
- Fyzická bezpečnost: Riziko útoků, terorismu, násilí, krádeží a dalších trestných činů v reálném světě. Lidé se mohou cítit ohroženi ve veřejných prostorech, na veřejných akcích nebo dokonce ve svém vlastním domově.
- Kybernetická bezpečnost: Riziko útoků na počítačové systémy, sítě a online účty. Kybernetický zločin může zahrnovat krádeže identity, phishing, ransomware, útoky na bankovní účty a další.
- Sociální bezpečnost: Riziko využití sociálních médií a online platform pro šíření dezinformací, šikanu, kybershikany a dalších forem zneužití. Soukromí a osobní údaje mohou být ohroženy.
- Finanční bezpečnost: Riziko finančních podvodů, krádeží kreditních karet, zneužití bankovních účtů a dalších forem ekonomického zločinu. Lidé mohou být okradeni o své úspory nebo se dostat do dluhů.
- Cestovní bezpečnost: Riziko únosů, teroristických útoků, krádeží a dalších rizik spojených s cestováním. Lidé mohou být v nebezpečí při cestování do konfliktních oblastí, nestabilních zemí nebo při cestování sami.
- Zdravotní bezpečnost: Riziko nákaz a epidemie, včetně pandemií. Lidé se mohou nakazit infekčními chorobami, jako je COVID-19, nebo se vystavit nebezpečným látkám a podmínkám, které ohrožují jejich zdraví.

Je důležité být si těchto rizik vědom a přijmout opatření k ochraně své bezpečnosti. To může zahrnovat používání silných hesel, aktualizaci softwaru a antivirového programu na počítači, opatrnost při sdílení osobních údajů online, monitorování zpravodajství a cestovních doporučení a dodržování bezpečnostních opatření ve veřejných prostorech.

2.2 Metody analýzy rizika

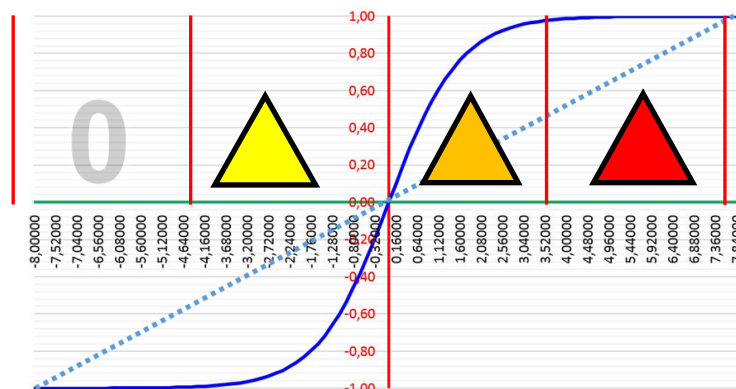
Jako praktický příklad je zvolen jednoduchý přístup k určení stupně ohrožení, přičemž za základ je brán současný stav, tedy **nejnižší stupeň ohrožení, který je označen nulou**, představuje „ideální“ klidový stav, při němž není žádná hrozba útoku na českém území. Při tomto stavu nejsou

vydávána žádná zvláštní doporučení nebo varování ve vztahu k veřejnosti. **První stupeň** bude označen žlutým trojúhelníkem, který upozorní na existenci obecného ohrožení terorismem. Při tomto stavu je třeba dbát obecné všímavosti. Za této situace platí některá vytipovaná zvýšená *bezpečnostní* opatření. **Druhý stupeň** bude znázorňovat oranžový trojúhelník. Tento stav upozorní na existenci zvýšené pravděpodobnosti ohrožení terorismem a vyhláší se v návaznosti na předchozí události či informace o hrozbě projevů terorismu. **Třetí stupeň** bude představovat červený trojúhelník. Tento stav zavede vysoký stupeň bdělosti a pohotovosti, při nichž je teroristický útok očekáván s vysokou pravděpodobností nebo už se stal a je potřeba přijmout opatření k zamezení pokračování či opakování útoku a minimalizovat následné škody. Graficky lze situaci znázornit tak, jak je na obrázku (Obrázek 3).



Obrázek 3: Hrozby a rizika regionální bezpečnosti – lineární rozdělání ohrožení

Rozdělání předpokládá lineární stejnoměrné rozložení hrozeb. Ovšem je zřejmé, že hodnota například 0,749 odpovídá oranžovému trojúhelníku a „prakticky“ stejná hodnota 0,751 již červenému. Ve slovním hodnocení se jedná o dosti nezanedbatelný rozdíl, z pohledu matematiky nikoli. Není zanedbatelné ani psychologické hledisko. Může se zdát, že „je jedno zda 0,75 anebo 1,00 – vždy je to červená“. Pak se nabízí použití nelineárního vztahu, jak je uvedeno na obrázku (Obrázek 4):



Obrázek 4: Použití funkce tgh pro stanovení nelineárního průběhu hodnoty koeficientu.

Pokud budeme hodnotit rizika nelineárně (Obrázek 4), máme v oblasti „0“ i „červeného trojúhelníku“ takřka konstantní hodnotu rizikového zatížení, a naopak ve střední části grafu se odvíjí veškerý nárůst potenciačního nebezpečí. Prakticky došlo k eliminaci přechodu mezi například oranžovou a žlutou hodnotou při zanedbatelné změně matematické hodnoty.

Jinou otázkou je pak pořízení vstupních dat, nutných pro výpočet hodnot rizikového zatížení. U hybridních hrozeb to pro rozmanitost zdrojů bude velmi náročné.

Zdroje

1. SVOBODA, Ivo. Political extremism and terrorism as destabilizing element of internal security of the state. In. *European Science, Sciencific journal*. Podhájská: 5/2018, s. 66-71. ISSN 2585-7738, EV 5691/18.
2. Bezpečnostní expert Šándor: Představa, že stát řekne, co je pravda a co ne, je nesmyslná: <https://www.novinky.cz/clanek/domaci-bezpecnostni-expert-sandor-predstava-ze-stat-rekne-co-je-pravda-a-co-ne-je-nesmyslna-40019977>
3. SVOBODA, Ivo. Vzdělávání dospělých v oblasti krizového řízení při zajištění bezpečnosti obyvatel. In.: *Zborník príspevkov z 12. medzinárodnej vedeckej konferencie „Národná a medzinárodná bezpečnosť 2021“*, Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2021, s. 351-362. ISBN 978-80-8040-606-6.
4. KUBEČKA, Karel. *Rizika staveb, příčiny vzniku poruch, důsledky poruch a způsob hodnocení*: autoreferát habilitační práce pro jednání Vědecké rady FAST VŠB-TU Ostrava, dne 20. února 2009. In Vědecké publikace Fakulty stavební Vysoké školy báňské – Technické univerzity Ostrava. Doktorské disertační, habilitační a inaugurační spisy. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2009. 50 s. Vědecké publikace Fakulty stavební Vysoké školy báňské. ISBN 978-80-248-1800-9.
5. KUBEČKA, Karel. *Využití metod analýzy rizika ve forenzních vědách: aplikace metod analýzy rizik v oceňování nemovitostí a hodnocení škod a vad*. Vydání první. Brno: KEY Publishing s.r.o., 2017. 179 s. monografie. ISBN 978-80-7418-281-5.
6. JUŘÍČEK, Ludvík a Petr ROŽŇÁK. *Bezpečnost, hrozby a rizika v 21. století*. Ostrava: Key Publishing, 2014, 323 s. ISBN 978-80-7418-201-3.

VYUŽITIE TEÓRIE DIGITÁLNEJ STOPY PRI IDENTIFIKÁCII HYBRIDNÝCH HROZIEB

JUDr. Adam Kubelka

Akadémia Policajného zboru v Bratislave; Sklabinská 1, 835 17 Bratislava; adam.kubelka@akademiapz.sk

Abstrakt: Predkladaný príspevok prináša náhľad do problematiky teórie digitálnej stopy a jej využitia pri identifikácii hybridných hrozieb. Pri jeho spracovaní bol kladený dôraz na skúmanie vybraných aspektov digitálnej stopy a hybridných hrozieb. Cieľom príspevku je popísať digitálnu stopu ako súčasť kriminalistickej teórie stôp a jej využiteľnosť pri identifikácii hybridných hrozieb s dôrazom na atribúciu kybernetických incidentov ako nástrojov hybridného pôsobenia. Vybrané aspekty využiteľnosti teórie digitálnej stopy pri boji s hybridným pôsobením, najmä v kybernetickom priestore, sú obsiahnuté v poslednej časti príspevku, pričom prezentované poznanie bolo nadobudnuté predovšetkým prostredníctvom obsahovej analýzy odbornej literatúry.

Kľúčové slová: hybridná hrozba, digitálna stopa, kybernetická doména.

ÚVOD

Pokrok v informačných technológiách umožnil miliónom ľudí na svete prístup k nespočetnému množstvu informácií, pričom mnohé z nich sú často zavádzajúce a nepravdivé. Výskyt rôznych dezinformačných kampaní, ako jeden z prostriedkov vedenia tzv. hybridnej vojny, sa neustále zvyšuje. Hoci dezinformácie nie sú novým javom v spoločnosti, ich význam z hľadiska bezpečnosti štátu sa zvýšil najmä v súvislosti so vznikom nových a efektívnejších techník ich šírenia. Zahraniční štátni aktéri čoraz viac využívajú dezinformačné stratégie, aby mohli ovplyvňovať verejné diskusie, podnecovať polarizáciu spoločnosti a zasahovať do demokratického rozhodovania. Pre bezpečnosť Slovenskej republiky sú rizikom predovšetkým preto, že svojim pôsobením oslabujú dôveru spoločnosti v demokratické inštitúcie a procesy štátu, čo môže v extrémnych prípadoch viesť k prevratu alebo zmene režimu. Úlohou štátu a jeho kompetentných zložiek je brániť sa voči dezinformačným kampaniam a bojovať s nimi nastavením správnej strategickej komunikácie. Prvky hybridnej vojny alebo hybridné hrozby v Slovenskej republike patria do pôsobnosti Národného bezpečnostného analytického centra a vládneho Situačného centra Slovenskej republiky, ktoré je národným kontaktným bodom pre hybridné hrozby.

1. INTERPRETÁCIA VÝKLADU KĽÚČOVÝCH POJMOV

1.1 Hybridná hrozba

Pojem hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.

Používanie nástrojov hybridných aktivít môže slúžiť na dosiahnutie konkrétnych cieľov aj bez formálneho vyhlásenia vojny. V súčasnosti existujú desiatky nástrojov hybridných aktivít (napr. zneužívanie zraniteľností vo verejnej správe, dezinformácie, kybernetická či priemyselná špionáž, zneužívanie právnych pravidiel, procesov, inštitúcií a argumentov) a rôznych nátlakových a podvratných činností a konvenčných a nekonvenčných metód, napríklad diplomatických,

vojenských, ekonomických a technologických. Súčasťou hybridného spôsobu boja môžu byť masívne dezinformačné kampane a využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie priaznivcov.

Hybridné hrozby sú rôznorodé a pôsobia naprieč doménami infraštruktúry, kybernetického priestoru, vesmíru, ekonomiky, obrany, kultúry, spoločnosti, verejnej správy, práva, spravodajských služieb, diplomacie, politiky a informácií.

1.2 Kybernetická doména

Kybernetický priestor zohráva v súvislosti s hybridnými hrozbami výnimočnú a veľmi špecifickú úlohu. V prípade národných bezpečnostných plánov zahŕňa počítačovú kriminalitu, propagandu, špionáž, ovplyvňovanie, terorizmus a dokonca aj samotný boj. Poskytuje nové mechanizmy, ktorý môžu zvýšiť rýchlosť, šírenie a silu útoku a zabezpečiť anonymitu. Menší aktéri majú väčšie možnosti na presadenie svojej moci v kybernetickom priestore, než v mnohých tradičných oblastiach svetovej politiky.

Kybernetická doména sa týka informačného prostredia pozostávajúceho zo vzájomne prepojených sietí infraštruktúr informačných technológií (vrátane hardvéru, softvéru, údajov, protokolov) a informácií vrátane internetu, telekomunikačných sietí, počítačových systémov a zabudovaných procesorov a kontrolných mechanizmov. Kybernetická doména sa v súčasnosti pomerne rýchlo mení. Nástroje, ktoré môže protivník uplatniť, sú zamerané na spôsobenie degradácie, narušenia alebo zničenia sietí alebo na prístup k údajom a informáciám. Prístup k informáciám môže byť tiež cieľom protivníka s cieľom zhromažďovať spravodajské informácie a znižovať možnosť detekcie. Digitálna transformácia môže umožniť použitie kybernetických nástrojov v mnohých ďalších doménach.

1.3 Digitálna stopa

Každé technologické zariadenie informačnej techniky, ktoré získava, uchováva, poskytuje alebo rôznym iným spôsobom spracováva elektronický údaj (dáta) zanecháva záznamy o svojej činnosti. Takéto záznamy sú s kriminalistického hľadiska stopami. V súvislosti s informačnou technikou a s informačnými technológiami môžeme hovoriť o stopách digitálnych. Tieto vznikajú na všetkých informačných zariadeniach a technológiách. Ich vypovedajúca sila je omnoho vyššia ako ľudská pamäť, lebo zaznamenávajú informácie oveľa presnejšie a zaznamenávajú dlhodobé informácie, ktoré už boli vykonané.

Pre termíny „digitálna a stopa“ a „digitálny dôkaz“ existuje v angličtine len jeden termín „digital evidence“, kde slovo „evidence“ má význam ako „dôkaz“. Naproti tomu slovenské slovo „stopa“ v súvislosti s modernými technológiami v zahraničnej literatúre nenájde. Je to z toho dôvodu, že teória a prax sú orientované predovšetkým na výsledok trestného procesu. Každá stopa musí byť súdom akceptovaná, čím dochádza k automatickému stotožneniu pojmov „stopa“ a „dôkaz“.

K definovaniu digitálnej stopy sa v súčasnosti vo väčšine vyspelých štátoch akceptuje definícia, ktorá bola navrhnutá v roku 1999 pracovnou skupinou SWGDE Scientific Working Group on Digital Evidence:

„Digitálna stopa je akákoľvek informácia s vypovedajúcou hodnotou uložená alebo prenášaná v digitálnej podobe“.²²⁹

Táto definícia je vo všeobecnosti platná pre akúkoľvek digitálnu technológiu a zahŕňa nielen oblasť počítačov a počítačovej komunikácie, ale i oblasť digitálnych prenosov, mobilných telefónov, digitálnych TV, audia, videa, digitálnych fotografií kamerových systémov, elektronických zabezpečovacích systémov a mnoho ďalších informačných technológií. V niektorých zahraničných publikáciách sa definujú digitálne stopy, ako dáta spojené vždy so spáchaním trestného činu, čo predstavuje nie vždy pravdivý a veľmi zúžený výklad definície.

V oblasti informačných technológií sú informácie označované ako kódované dáta, ktoré možno vysielat', prijímať, uchovávať a spracovávať ich prostredníctvom technologických prostriedkov. V odborných informačno-technologických textoch sa používajú obidva pojmy, niekedy ako synonymum podľa logického zmyslu textu, alebo aby sa slová zbytočne neopakovali v jednej vete. Informácie majú skôr širší význam, ktorý presahuje hranice oblasti informačných technológií. Obidva pojmy sa nedajú úplne stotožniť, ale v odbornom texte informačných technológií sa nerozlišujú, vždy sa používa ten, ktorý je výrazovo bližší k všeobecnému pochopeniu. Digitálna stopa nemusí byť vždy spojená s trestným činom. V tejto definícii sa rozumie digitálna stopa celkovo vo všeobecnosti, teda aj z pohľadu legálnej činnosti užívateľov. Digitálna stopa sa stáva kriminalistickou stopou dokazujúcou spáchanie trestného činu, až keď sa nájde súvislosť digitálnej stopy s trestnou činnosťou páchatel'a.

1.4 Zdroje digitálnych stôp

Vzhľadom na existujúce veľké množstvo rozmanitých zdrojov digitálnych stôp, ktorých množstvo a typová rôznorodosť sa neustále zvyšuje, bolo potrebné dátové zdroje rozdeliť do niekoľko skupín. Sú to skupiny, v ktorých digitálne stopy majú podobný charakter, a tiež aj rovnaký spôsob ich vyhľadávania, zaist'ovania, spracovania, ako aj podobný spôsob ich využitia. Každá z týchto skupín je orientovaná na špecifické nároky, na technické vybavenie a znalosti potrebné na prácu s digitálnymi stopami. Najčastejšie využívané zdroje, ktoré produkujú digitálne stopy, boli logicky usporiadané do troch skupín:

1. Otvorené počítačové systémy – tu patria napr. počítače, notebooky, hard-disky, klávesnice, monitory, servery.
2. Komunikačný systém – do tejto skupiny patria klasicky pevné telefóny, bezdrôtové telekomunikačné systémy, počítačové siete, internet atď. Prostredníctvom týchto zdrojov sú informácie prenášané do celého sveta. Ako dôležité digitálne stopy tu vystupujú ich autor, čas, ktoré prenášajú, e-mail, atď.
3. Zariadenia s integrovaným počítačovým čipom – sú zariadenia, ktoré sú cenným zdrojom dát vhodných pre kriminalistické vyšetrovanie, ako mobilné telefóny, čipové platobné karty, navigačné technológie GPS (Global Positioning System), čierne skrinky v lietadlách, diagnostické moduly počítačových riadiacich jednotiek automobilových motorov, taktiež platobná elektronická databáza v obchodoch, atď.

V tejto súvislosti možno konštatovať, že na základe všade prítomných digitálnych stôp je dnes veľmi málo trestných činov, ktoré by neboli spojené s uloženými alebo prenášanými informáciami.

²²⁹ PORADA, V., RAK, R. 2006. Digitální stopy v kriminalistice a forenzních vědách, s. 5.

Aj tieto skutočnosti predstavujú pre orgány presadzujúce právo určitú výhodu na úseku odhaľovania, objasňovania a dokazovania trestných činov.

1.5 Zaistenie digitálnych stôp

Najdôležitejšie úkony pri vyšetrovaní informačnej kriminality²³⁰ alebo iných trestných činov, v ktorých majú dôležitú úlohu digitálne dáta, sú úkony zaist'ovania digitálnych stôp. Zaistenie digitálnych stôp je úkon, ktorý začína okamihom, kedy dáta obsahujúce relevantné informácie, alebo zariadenia, na ktorých sú také dáta uložené, sú zaistené alebo uložené pre znalecké skúmanie.

Proces zaistenia digitálnych stôp sa vykonáva za predpokladu, že tieto stopy budú súdnymi orgánmi akceptované ako dôkaz, preto celý proces musí byť primeraný a legálny pre ďalšiu prácu s nimi ako s dôkazovým materiálom. Digitálne stopy pre ďalšie znalecké skúmanie sú zaist'ované viacerými spôsobmi, podľa okolností vyskytnutých sa pri zistení trestnej činnosti. Zaist'ujú ich orgány činné v trestnom konaní, prípadne za účasti súdneho znalca, vykonávaním činností vyplývajúcich z Trestného poriadku, alebo inými legálnymi spôsobmi, ktoré vedú k zaisteniu digitálnych stôp. Sú to najmä tieto úkony:

- domová prehliadka²³¹,
- osobná prehliadka,
- prehliadka iných priestorov a pozemkov,
- odňatie a vydanie vecí,
- obhliadka miesta činu,
- zaistenie dát z internetu,
- ďalšie úkony.

Pri zaist'ovaní digitálnych stôp pre účely ďalšieho skúmania resp. forenznú analýzu, ktoré nemajú súvislosť s trestným konaním, sa musia dodržiavať zákony a právne predpisy danej krajiny a úkony sa môžu vykonávať len so súhlasom vydávajúceho digitálne stopy alebo na jeho objednávku (napr. vykonanie podnikových auditov a pod.).

Zaistenie digitálnych stôp je v prvom rade procesom zaist'ovania dát. Zaistenie nosičov dát vykonávajú väčšinou dvaja príslušníci polície, za prítomnosti súdneho znalca, poprípade nezúčastnenej osoby. Tieto úkony vyžadujú vysokú odbornosť osoby, ktorá vykonáva zaistenie dát pre účely trestného konania. Táto osoba musí mať osvedčenie o odbornej spôsobilosti vykonávať kriminalisticko-technické úkony pri zaist'ovaní zariadení obsahujúcich digitálne stopy, resp. samotných digitálnych dát na mieste.

²³⁰ Trestná činnosť, pri ktorej sa využívajú informačné a komunikačné technológie (IKT), alebo ktorej cieľom sú IKT. Rozdeľuje sa na trestnú činnosť, ktorá súvisí s obsahom (porušovanie autorských práv, detská pornografia), tradičná trestná činnosť vykonávaná pomocou IKT (vydieranie, krádež, sprenevera), útoky na IKT (narušenie dát a systémov, rasnomware, DDoS útoky)

²³¹ §99 a nasledujúce zákona č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov.

Zaist'ovanie digitálnych dát a technológie obsahujúcej digitálne dáta sa vykonávajú v prípade, že:

- nie je možné vytvorenie bitových kópií digitálnych dát (presná kópia disku),
- pokiaľ ide o dobrovoľné vydanie dát,
- pri získavaní digitálnych dát z verejných zdrojov, napr. z internetu.

V prípade priameho zaistenia digitálnych dát je najčastejším úkonom kopírovanie dát (napr. zo serveru). Vykonáva sa to za účasti správcu alebo nezúčastnenej osoby špecialistu, ktorý rozhodne, aký spôsob zaistenia bude vykonaný. V prípade verejne dostupných zdrojov sa prítomnosť nezúčastnenej osoby nevyžaduje. Pri zaist'ovaní dát vždy záleží na okolnostiach a použitej technológii, pretože niektoré postupy sa môžu v praxi líšiť ale v princípe môžu byť rovnaké.

V rámci úkonov v trestnom konaní, reálne zaistenie digitálnych stôp môžeme rozdeliť podľa druhu na :

1. Zaistenie techniky obsahujúcej digitálne stopy :

- osobné počítače, servery, notebooky, netbooky, tablety a iné,
- dátové médiá – pevné disky, flash disky (USB kľúče), výmenné médiá, pamäťové karty, diskety, CD a DVD nosiče a pod.,
- mobilné telefóny a komunikátory, vreckové počítače, diáre, atď.,
- aktívne sieťové prvky – routery, firewally, sieťové servery a pod.,
- ostatná elektronika, ktorá môže obsahovať digitálne stopy.

2. Zaistenie dát:

- e-mailovej komunikácie,
- www stránok a serverov,
- databázy,
- účtovných dát,
- ostatných dát podľa špecifickosti spáchaného trestného činu,
- zaistenie tlačенých a obrazových výstupov, prípadne zaistenie písomnej dokumentácie, ktorá má vzťah k digitálnym stopám.

2. IDENTIFIKÁCIA HYBRIDNÉHO PÔSOBENIA POMOCOU DIGITÁLNYCH STÔP

Zatiaľ čo väčšina prvkov hybridných hrozieb nie je nová, digitálna sféra v skutočnosti predstavuje nové impozantné výzvy. Ruské zasahovanie do volieb v USA v roku 2016 bolo založené na dvoch primárnych zraniteľnostiach, ktoré digitálna sféra vytvára – znížené vstupné náklady na informačné operácie a kybernetickú špionáž s útokmi.²³² Vplyv Ruska počas volieb bol zosilnený koordinovanou informačnou operáciou na sociálnych médiách, ale aj na rafinovanejšími útokmi v kyberpriestore. Verejný charakter informačných operácií prostredníctvom sociálnych médií však otvára priestor na ich detekciu. Väčšina kybernetických útokov je navrhnutá tak, aby zostala neodhalená, alebo prinajmenšom zakryla páchatel'a vrstvami nejasností. Efektívna atribúcia kybernetických incidentov je preto rozhodujúca pre reakciu na hybridné hrozby.

Keď v kybernetickom priestore vznikajú nové zraniteľné miesta, otvárajú sa aj nové príležitosti na detekciu prípadných útokov a na náležitú reakciu na ne. Detekcia škodlivej kybernetickej aktivity

²³² LEWIS, J. A. 2018. Rethinking Cybersecurity: Strategy, Mass Effect, and States. In: Center for Strategic and International Studies.

môže indikovať, že ide o hybridnú operáciu v skoršom štádiu. Situácia je však podobná ako pri identifikácii iných hybridných operácií – prítomnosť jedného hybridného nástroja nezaručuje použitie iných hybridných nástrojov.

Prvým krokom vo všetkých prípadoch kybernetickej atribúcie je stiahnutie všetkých technických údajov o narušení systému alebo útoku. V ďalšom kroku prebieha identifikácia povahy útoku, cieľa útoku a jeho všeobecnej sofistikovanosti. Potom, prebieha analýza digitálnych stôp so zameraním sa na nasledovné kritériá:²³³

- Zdrojové údaje: Metadáta, ako napríklad „zdrojové IP adresy, názvy domén, informácie o registrácii názvu domény, údaje tretích strán zo zdrojov, ako Crowdsourc alebo VirusTotal, e-mailové adresy, hash a hostiteľské platformy môžu pomôcť pri atribúcii; tieto údaje sa však dajú ľahko sfalšovať.
- Nástroje, skripty a programy: V útočníkovom softvéri možno nájsť ďalšie dátové body, ako sú phishingové balíky (súbory a odkazy, ktoré po aktivácii zámerne odosielajú informácie späť hostiteľovi), jazyk kompilátora, programovací jazyk, čas kompilácie a ďalšie.
- Taktiky, techniky a postupy (TTP): Páchatelia majú niekedy svoj vlastný „štýl“. To môže siahať od spôsobu vykonania útoku až po spôsob, akým zakrývajú svoje stopy. Užitočné môže byť sledovanie online aktivity sociálnych médií v súvislosti s útokom. Páchateľ sa môže tiež pokúsiť označiť falošné dokumenty geotagom alebo phishingovými odkazmi na zakrytie skutočných miest,
- Snaha dostať sa útočníkovi do hlavy: Pochopenie ich cieľov môže poskytnúť kriticky dôležité informácie, potrebné na jeho odhalenie. V tomto bode je žiadúca spolupráca so spravodajskými službami, prípadne so špecializovanými pracoviskami Policajného zboru.
- Geopolitika: Táto analýza sa pokúša určiť identitu útočníka s ohľadom na súčasné udalosti. Analýza so zameraním na geopolitiku spája rôzne predpoklady nad motiváciou zainteresovaných strán s technickou forenznou analýzou kybernetického útoku. V tomto druhu analýzy sa tiež začína atribúcia posúvať od forenznej analýzy smerom k strategickejšiemu a komplexnejšiemu chápaniu hrozby.

Keď sa prípad atribúcie stáva zložitejším a útok je sofistikovanejší, možno prijať ďalšie opatrenia na určenie totožnosti útočníkov. Medzi dodatočné techniky atribúcie kybernetického útoku možno zaradiť: využitie vopred nasadených systémov na detekciu narušenia (IDS); nútená, resp. zneužitá sebaidentifikácia útočníka (napr. majáky, webové chyby, súbory cookie, vodoznaky); prekonfigurovanie a sledovanie siete; využitie bezpečného hostiteľa/smerovača alebo kombinovať súbory techník.²³⁴

Nielen štátne inštitúcie ochraňujúce kyberpriestor, ale aj všetky súkromné spoločnosti musia efektívnejšie zabezpečiť svoje vlastné údaje a údaje svojich zákazníkov. Keďže hybridné techniky znemožňujú jednoznačné určenie hranice medzi hybridnými aktérmi a bežnými občanmi, jednotlivci by tiež mali podniknúť kroky na zabezpečenie svojich účtov a svojich zariadení a rovnako by sa mali mať na pozore pred inými prvkami hybridného pôsobenia, najmä pred informačnými operáciami vykonávanými na sociálnych sieťach.

²³³ HARVEY, J. 2017: The Shadowy – and Vital – Role Attribution Plays in Cybersecurity. In: Accenture.

²³⁴ WHEELER, D. A., LARSEN, G. N. 2019. *Techniques for Cyber Attack Attribution*. In: *Institute for Defense Analyses, ES – 1*.

ZÁVER

Cieľom tohto príspevku bolo, v kontexte digitálnych stôp, priblížiť určité aspekty teórie digitálnych stôp a jej využiteľnosti pri odhaľovaní hybridných hrozieb. K naplneniu tohto cieľa došlo použitím vybraných metód skúmania, predovšetkým využitím obsahovej analýzy a následnej syntézy týchto poznatkov. V úvode tohto odborného článku sme priblížili niektoré pojmy súvisiace s našou témou, hlavne hybridné hrozby, doménu kyberpriestoru, digitálne stopy, ich zdroje a ich zaisťovanie. V ďalšej časti sme sa zamerali na aplikačnú prax, kde sme poukázali na možné využitie teórie digitálnej stopy pri odhaľovaní hybridného pôsobenia, pričom sme bližšie špecifikovali najmä hybridné operácie v kyberpriestore a ich atribúciu. Z prezentovaného poznania je zrejmé, že digitálne stopy sa stávajú veľmi cenným nástrojom odhaľovania, objasňovania a dokazovania trestnej činnosti. V tomto kontexte vidíme aj ich očividné benefity v procese identifikácie hybridných hrozieb, čo nepriamo poukazuje aj na potrebu zefektívnenia procesov zisťovania a zaisťovania digitálnych stôp operatívnymi a spravodajskými zložkami štátu a v neskoršom štádiu aj orgánmi činnými v trestnom konaní, osobitne v prípadoch, ak takéto konania naplňajú znaky skutkovej podstaty niektorého trestného činu uvedeného v osobitnej časti Trestného zákona. Sme si vedomí toho, že problematika identifikácie a fixácie digitálnych stôp je pomerne zložitá a má svoje špecifické prieniky do rôznych vedných disciplín, osobitne v tomto ohľade právnych, technických a forenzných vied. Tieto skutočnosti logicky akceptujeme a sú pre nás výzvou, ktorá inhibuje ďalšie vedecké skúmanie.

Zdroje

1. HARVEY, J. 2017: The Shadowy – and Vital – Role Attribution Plays in Cybersecurity. In: *Accenture, May 2017*. [cit. 19.3. 2023]. Dostupné na internete: <https://www.accenture.com/us-en/blogs/blogs-shadowy-vital-role-attribution.cybersecurity>
2. JIRKOVSKÝ, V. *Kybernetická kriminalita: nejen o hacinu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007. 284 s. ISBN 80-247-186-19.
3. LEWIS, J. A. 2018: Rethinking Cybersecurity: Stragy, Mass Effect, and States. In: *Center for Strategic and International Studies, January 2018*. [cit. 19.3.2023]. Dostupné na internete: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_Reconsidering_Cybersecurity_Web.pdf
4. MAISNER M., a kol.. *Základy práva informatických technológií*. Bratislava: IURAEdition, 2013. s. 289, ISBN 978-80-8708-594-9.
5. METĚNKO, J. a kol.: *Kriminalistické metody a možnosti kontroly sofistikované kriminality*. Katedra kriminalistiky a forenzných disciplín, Akadémia PZv Bratislave. Bratislava 2004. s. 356, ISBN 80-8054-336-4.
6. PORADA, V. - RAK, R. *Digitální stopy v kriminalistice a forenzních vědách*. Praha: Policejní akademie České republiky, 2006, s. 365.
7. WHEELER, D. A., LARSEN, G. N. 2019. Techniques for Cyber Attack Attribution. In: *Institute for Defense Analyses, ES – I* [cit. 19.3.2023]. Dostupné na internete: <https://apps.dtic.mil/sti/citations/ADA468859>
8. *Zákon Národnej rady Slovenskej republiky č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov*.
9. *Zákon Slovenskej národnej rady č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov*.

ON SEARCHING FOR NATURAL AND LEGAL PERSONS WITH AN UNFAVORABLE REPUTATION

Richard Marko, Michal Ries, Antonín Korauš, Stanislav Šišulák

Faculty of Informatics and Information Technologies, Slovak University of Technology, Bratislava, Slovakia 0000-0002-5911-1448, 0000-0002-9233-7123, Academy of the Police Force in Bratislava, Bratislava, Slovakia, 0000-0003-2384-9106, 0000-0003-4727-9582

Abstract: The goal of this study is to create a web platform that facilitates the identification of individuals or entities with a negative reputation through online sources. It seeks to assist companies and employers in evaluating potential associates and staff for potential connections to criminal offenses like money laundering, bribery, and fraud (e.g., hoax). A significant challenge is filtering and organizing pertinent articles related to these offenses and establishing an accessible index for efficient information retrieval. Additionally, the solution being developed accommodates various European languages by considering the language used in the articles.

Keywords: compliance, AML, anti-money laundering, adverse media screening.

INTRODUCTION

Adverse Media Screening (AMS) involves examining individuals or entities, whether natural or legal (like potential clients, employees, or business associates), against negative information sourced from various public domain sources [15], [4]. This process is crucial in uncovering potential allegations or charges, ultimately averting future problems. Inadequate AMS has resulted in significant financial losses for numerous companies, both financial and non-financial, during 2018 and 2019 [8]. Typically integrated into anti-money laundering procedures [2], [15], [8], AMS can divulge information indicating a heightened risk of money laundering activities or individuals engaging in deceitful actions.

As part of its directives to combat money laundering, the European Parliament has mandated the adoption of AMS measures, which EU member states are required to incorporate into their domestic legislation [13]. These directives necessitate screening against international media (reputable newspapers) and the utilization of automated adverse media screening technology. In this research, we've developed a system that autonomously updates its database of publicly accessible articles from international media sources daily, aligning with these requirements. However, continuous screening encounters significant challenges, including the extensive and varied publicly available information, media pertinence, and accuracy of named entities [8].

Given the immense volume of internet-based information, identifying pertinent articles and useful data points for recognizing potential risks can be arduous. Furthermore, much of the information available online may lack reliability or accuracy, potentially resulting in false positives or false negatives in the screening process. Another challenge in implementing AMS through a web portal is the necessity for advanced search and filtering capabilities. Effective adverse media screening mandates search capabilities that can refine information based on specific criteria such as time frame, relevance, and media type. Additionally, the screening process should proficiently detect and classify various media types, including news articles, social media posts, and other online content.

Privacy concerns represent a significant hurdle in the AMS process. Conducting the screening requires the collection and analysis of personal information about individuals or entities, raising valid concerns regarding data privacy and security. Organizations must implement robust data protection measures to ensure sensitive information is safeguarded and unauthorized access is prevented. Implementing AMS through a web portal necessitates ongoing monitoring and updating to maintain the efficacy and currency of the screening process. This can prove time and resource-intensive, particularly for large organizations tasked with screening a substantial volume of individuals or entities on an ongoing basis.

We propose solutions to address these challenges in the "Future Work" section of this article.

1. MOTIVATION

The main goal of this study is to devise a remedy for the aforementioned challenges. Our objective is to aid companies and governmental entities in ensuring secure and trustworthy operations. We plan to achieve this by creating a web application that empowers users to validate the credibility of potential employees or business associates through article searches pertaining to criminal activities associated with them. Our solution offers added features like enabling users to search for articles specifying certain crimes or those originating from the USA, UK, and European Union countries within specified timeframes, resulting in more precise outcomes. Moreover, this software includes supplementary functions, such as generating PDF reports based on selected articles and maintaining an archive to exhibit articles that have become inaccessible on their original domains, all while retaining fundamental search capabilities.

2. SOLUTION DESIGN

The main advantage of our solution is its simplicity for the end-users, who only need to enter the name of the person they want to investigate. However, from a technical perspective, our solution is complex and consists of several modules, each with its own use and challenges, all integrated into a single working unit as shown in Fig. 1. This represents our first step, the creation of the high-level architecture that unites all individual modules.

The Scraper module is the most critical part of our system, implemented using the Scrapy framework [9], responsible for obtaining the data. In the next phase, we identify a suitable source of data, which provides a vast volume of freely available articles from various sources, countries, and languages. We use the MongoDB database to store all scraped articles, and Elasticsearch is integrated into the scraper-mongo-elastic pipeline to store the indexed data.

The web application is a significant component of our solution, comprising a client application in ReactJS, an application server in NodeJS, and a PostgreSQL database that stores user-related data. It is crucial to design a simple, minimalist, and user-friendly interface, offering various basic and advanced functionalities, such as access to archived pages and generating PDF reports from selected articles.

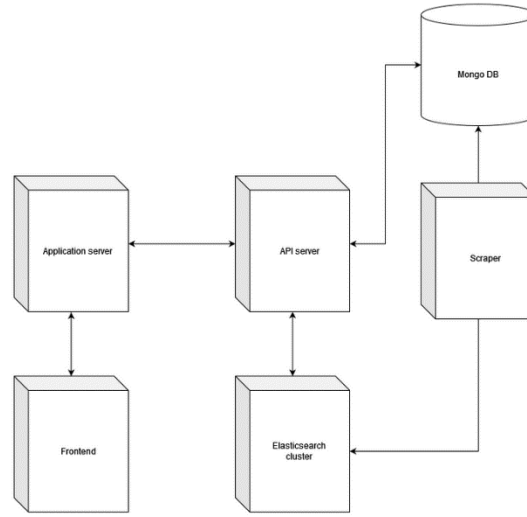


Fig. 1. High-level architecture diagram.

The basis of our proposed solution is an API server, which is developed using the Flask framework. The server acts as a provider of the accumulated and indexed data, and therefore, it necessitates communication with the MongoDB database and Elasticsearch for querying and retrieving articles.

3. IMPLEMENTATION

This section aims to provide a detailed account of the implementation of our solution, with a particular emphasis on the challenges associated with processing large volumes of data. We will describe the functionality of different components of our system and highlight some of the key techniques employed for obtaining and managing data.

A. Scraping the data

The advent of the internet and digital technologies has led to the exponential growth of data, including news articles. Data scraping is the process of collecting data from various sources, including news articles, for analysis and other purposes. However, scraping data from news articles is not always an easy task due to various challenges that arise during the process. We faced various challenges of data scraping from news articles:

1) *Volume and Diversity of Data*: One of the most significant challenges in data scraping from news articles is the volume and diversity of data. News articles come in various formats, including HTML, XML, and JSON, making it difficult to extract the relevant data accurately. Additionally, the sheer volume of news articles makes it impossible to manually collect and analyze the data, requiring automated data scraping tools.

2) *Web page structure*: Web pages containing news articles are structured differently, making it difficult to identify the relevant data. The structure of web pages varies based on the website, leading to inconsistencies in data scraping, and requiring different scraping techniques for different websites.

3) *Content Protection*: Many news websites have implemented measures to protect their content, such as CAPTCHAs, which require users to prove they are human before accessing the content. This can prevent automated data scraping tools from accessing the content, leading to incomplete or inaccurate data.

4) *Dynamic Web Pages*: Some websites use dynamic web pages, which are generated in real-time, and require interaction with the user to load content. This can pose a significant challenge to data scraping tools as they require additional effort to scrape data from these web pages.

5) *Data Quality*: Data scraped from news articles may not always be accurate, leading to poor quality data. News articles often contain biased or misleading information, which can affect the accuracy of the data collected.

6) *Legal Issues*: Data scraping from news articles may also lead to legal issues, such as copyright infringement, if the data is used without permission from the content owners. Additionally, some websites may have terms of service that prohibit data scraping, leading to legal repercussions if the terms are violated.

In order to extract only articles related to criminal activity, we utilize a dictionary of various crimes in multiple languages, which serve as keywords. The Scraper module iterates through this dictionary and collects all relevant articles published during a specified time period for each keyword. The subsequent step involves parsing the HTML source page by extracting only the heading and paragraph tags, thereby reducing the amount of stored data. Furthermore, we enhance the metadata of collected articles by searching for other crime-related keywords in addition to the initial search term. The article's title, language, region, link, date of publication, and identified keywords are stored in the MongoDB database after this step.

B. Use of Elasticsearch

Elasticsearch is a distributed, RESTful search and analytics engine based on Apache Lucene. It is designed to be scalable, reliable, and easy to use, making it a popular choice for search and analytics applications. Elasticsearch is used in a wide range of industries, including finance, healthcare, e-commerce, and more.

In order to ensure that our solution is efficient in finding relevant articles, we have incorporated the Elasticsearch software for data indexing. All fields, including the body of the article, are indexed, and this is done immediately after insertion into the MongoDB database as part of the scraper-mongo-elastic pipeline. When searching for results, Elasticsearch is used to modify queries to obtain results containing specific keywords, originating from specific countries, etc. However, these results only consist of IDs, and not the complete documents, which are retrieved from the database. While it would have been possible to store everything in Elasticsearch, we opted not to due to limited disk space. To conserve storage space, we used a database with compression functionality.

C. Web portal

We have developed and deployed a user-friendly interface that provides an effortless and intuitive user experience. The interface features a primary text field where users can enter their queries, as well as additional filter options, including a checklist of keywords, language preferences, country-

specific articles, and article age restrictions. These options enable users to refine their searches and obtain the most relevant results for their needs. Upon submitting a search request, the Flask API processes the query and returns the requested articles, along with any related criminal activity. The resulting articles are displayed to the user in a clear and comprehensible format, ensuring ease of use and optimal user engagement.

D. Containers

Docker containerization has become increasingly popular in recent years due to its numerous advantages. One of the main benefits of using Docker is its ability to create consistent, portable environments across different machines and platforms. Docker containers are lightweight and self-contained, which means that developers can easily package their applications and dependencies together, making it easier to deploy and scale applications. Another advantage of Docker is its flexibility. With Docker, developers can easily spin up new containers or scale up existing ones to meet changing demand, without having to worry about complex infrastructure setups or configurations. Docker also provides isolation and security for applications. Containers run in their own isolated environments, meaning that issues with one container do not affect others. This makes it easier to manage and maintain applications, especially in large-scale deployments. There are a wide range of pre-built Docker images available on the Docker Hub, which can save developers time and effort when building new applications.

In this research project, we have prioritized the use of containerization to ensure efficient deployment and management of our codebase. All the services in our codebase have been containerized and are composed of one or more modules, each present as a separate docker container. These modules are declared in a docker-compose file that manages the entire ecosystem and controls the state of each module.

To ensure consistency and ease of deployment, all container images are pulled from Dockerhub. Some of the modules are official images of widely used software that have been modified using environmental variables (e.g. Elasticsearch, NGINX), while others are custom-built Docker images (e.g. the Flask API server or the application server). For every module that uses a custom image, there is a GitHub repository containing the source code and a Dockerfile used to create the image.

To streamline the deployment process, we have implemented a CI/CD pipeline using Github actions. This pipeline builds a docker image on Github's servers and publishes it to our Dockerhub account. After the image is published, another automated action refreshes the running service using the docker-compose file present on our machine. As a result, manual deployment is unnecessary, saving us significant time and effort. Furthermore, deployment on multiple platforms is easily feasible using this approach.

The web application possesses several ways of representing the output data.

- Graphs and Charts (Fig. 2).
- List (Fig. 3).

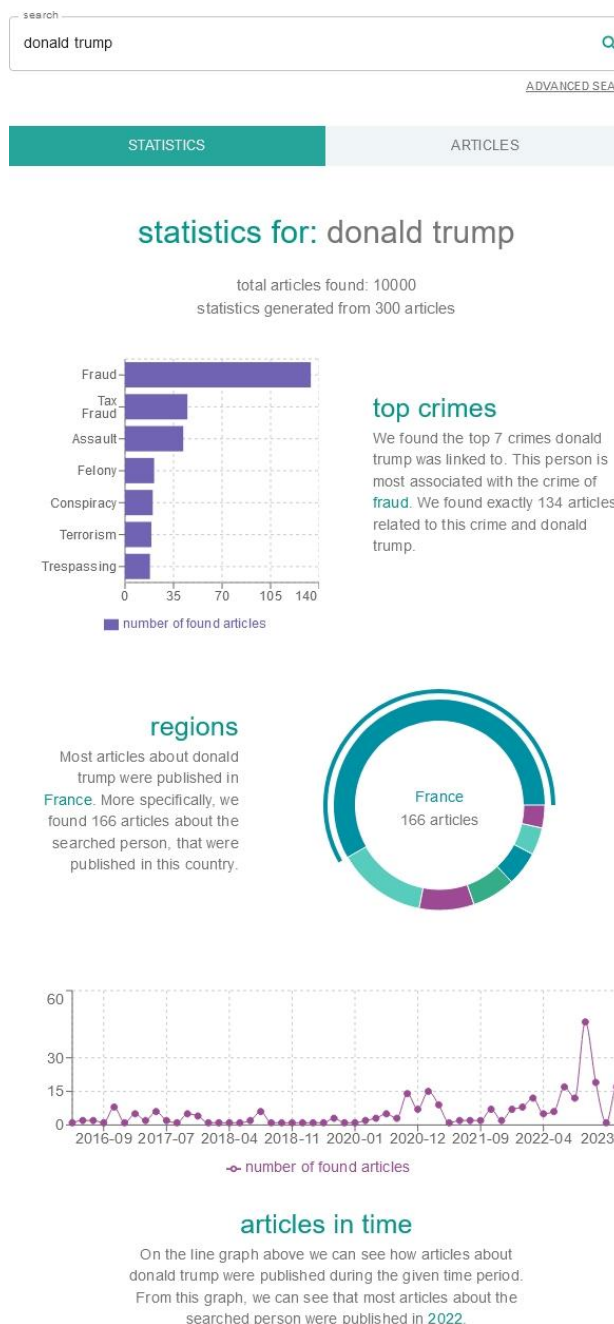


Fig. 2. Graph and chart representation of the output data.

4. EVALUATION

At present, our database contains a total of 4,319,480 articles pertaining to various forms of criminal activity. The storage used by these articles amounts to 104.2GiB in Elasticsearch and 35.4GiB in MongoDB. The comparatively smaller storage usage in MongoDB is due to the implementation of Huffman compression prior to the actual storage of articles in the database [1]. Our database is updated on a daily basis through the utilization of cron jobs [12], allowing us to scrape a minimum of 15,000 articles each day.

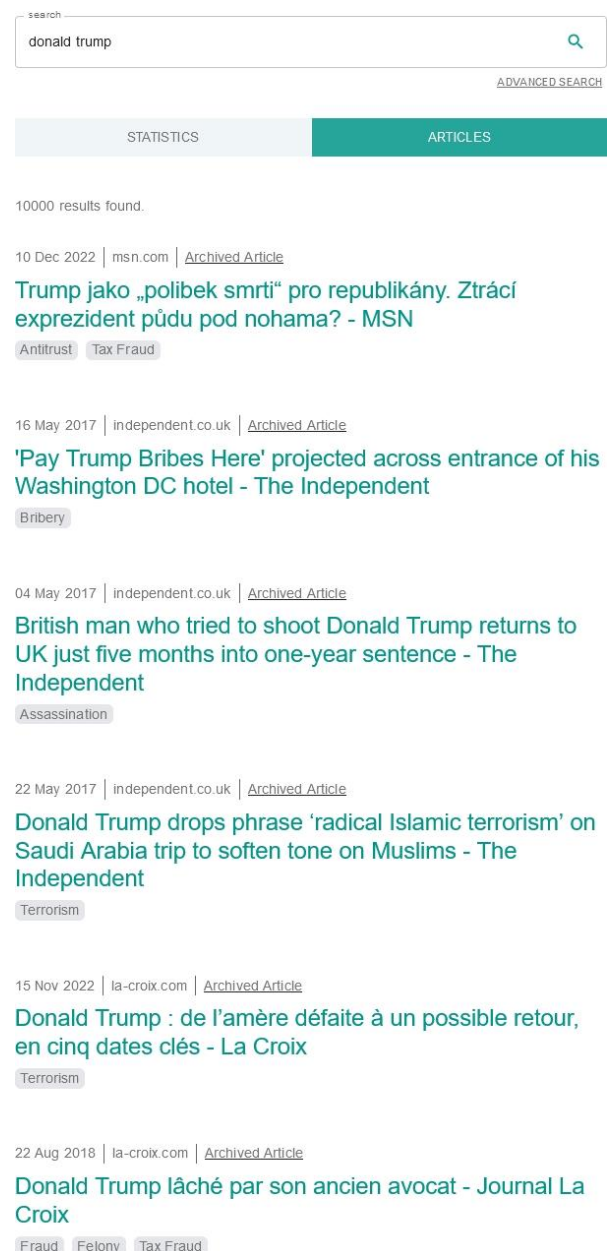


Fig. 3. Article list representation of the output data.

Our focus is primarily on the European market, with our web scraping efforts centered on publicly available media from countries within the European Union, United Kingdom and the United States. As of now, our system does not perform any verification of the accuracy of information obtained from the media sources. This is due to our initial goal of scraping and presenting users with as many articles about criminal activities as possible. Further evaluation of the system's performance is currently being conducted during the third-party testing phase, and we will provide additional results in due course.

5. FUTURE WORK

Our work is built upon a modular architecture that enables us to continuously improve and expand the functionality of our system. To achieve this, we plan to develop new modules and enhance existing ones in the future. Our immediate focus is on improving the web scraping module and enriching our data through a more comprehensive analysis pipeline. Additionally, we aim to broaden the functionality available to our users. In the long term, we plan to incorporate auditory layers in our data pipeline, leveraging machine learning to ensure the accuracy and relevance of our obtained data.

To enhance our data analysis capabilities, we are currently working on expanding our data's knowledge base by training and implementing a custom recursive neural network model for named entity recognition. This technique involves identifying specific names in texts and categorizing them based on different categories, such as people, companies, and geographical locations. This information can then be used to create complex relationship graphs. However, the challenge we are facing is the insufficient variety of data in different languages. Our current network provides promising results with a validation accuracy of over 95% in our internal tests for English texts. Following this, we plan to create even more complex solutions for relationship graphs by representing edges between entities using the articles.

Regarding user experience and functionality, we are currently planning two new features. First, we aim to integrate a translation engine to unify the user experience for articles in different languages. Second, we plan to implement a continuous monitoring feature, which will allow users to set specific entities under a watchlist and be notified if our system discovers new articles related to those entities. This feature is commonly found in other AMS implementations and will be implemented as a separate module between our application and data layers.

6. RELATED WORK

A. Robotic process automation of AMS in Deutsche Bank

Various studies [2], [8], [15] have demonstrated the widespread use of adverse media screening (AMS) in the banking sector. Many tasks in this industry require considerable time and effort, making them prone to human error [15]. To address these challenges, Deutsche Bank has leveraged Robotic Process Automation (RPA) and Artificial Intelligence (AI) technologies [5], [7], [15] to automate their AMS processes. The integration of these technologies was motivated by the bank's large volume of unstructured data, which is difficult to manage without advanced AI capabilities [15]. Consequently, Deutsche Bank has adopted the BluePrism commercial system [14] to facilitate their AMS activities [15].

B. Deep Learning-based Watchdog for Anti Money Laundering

Screening a large number of related documents for continuous monitoring of a single person can be a time-consuming and inefficient process, despite its effectiveness in identifying hidden criminal activities [2]. In order to improve the efficiency of this process, the authors propose a distributed architecture batch system based on natural language processing [3] techniques for organizing daily negative news [2]. The proposed system takes a set of documents from one watchlist and preprocesses the text, followed by paragraph embedding construction, resulting in a set of clusters containing all documents from the watchlist, grouped based on similarities [2]. The results are presented using a graphical interface to enhance user experience [2]. The proposed approach aims to reduce the time and effort required for continuous monitoring by improving the organization and presentation of related documents.

C. Adverse Media Mining for KYC and ESG Compliance

In response to issues with real-time updating and labor-intensive manual searches for adverse media screening (AMS), another representative of the AMS system has proposed a solution that involves both batch and real-time updating of negative news [8]. The updating process utilizes machine learning (ML) techniques and is driven by user-written queries [8]. Additionally, ML models are used for various perspectives in the AMS system, including Risk Relevance, Adverse Scoring, Entity Relevance, Risk Categorization, and Risk Stage Identification [8]. These ML models are integrated into the adverse news filtering pipeline, which has been shown to provide high-precision results for the AMS process [8].

D. Discussion

The objective of our system, as well as the other systems discussed in this chapter, is to filter negative news efficiently. However, unlike the other systems that employ AI or ML, our solution does not use these technologies yet. Our primary focus was to gather and process crime-related news from various countries. Nevertheless, the studies [8], [2], [15] reveal that going through all the collected articles, which may be unrelated, is a tedious and time-consuming process. Our research has provided us with valuable insights, and we intend to incorporate ML models for article relevance assessment in the future.

CONCLUSIONS

Within this paper, we introduced an innovative search engine crafted for organizations and employers aiming to assess the reputation and potential criminal involvement of natural and legal individuals through online media sources. Our system provides a user-friendly interface, where users can input a person's name to retrieve crime-related articles with pertinent keywords. Furthermore, our system is equipped to handle various European languages, enabling users to access information about criminal activities in countries where the language may pose a barrier. Nevertheless, there exists an opportunity for additional refinements.

References

1. R.A. Bedruz and A.R.F. Quiros, "Comparison of Huffman algorithm and Lempel-Ziv algorithm for audio, image, and text compression," in 2015 International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), pp. 1–6, IEEE, 2015.

2. H.Y. Chen, S.X. Zou, and C.L. Sung, "Pluto: A deep learning-based watchdog for anti-money laundering," in *Proceedings of the First Workshop on Financial Technology and Natural Language Processing*, pp. 93–95, 2019.
3. K. Chowdhary, "Natural language processing," in *Fundamentals of Artificial Intelligence*, pp. 603–649, 2020.
4. N. Corp, "Adverse media screening best practices guide," Web: <https://visit.dowjones.com/risk/content/adverse-media-best-practices/>.
5. S. Dick, "Artificial intelligence," 2019.
6. I. El Naqa and M.J. Murphy, "What is machine learning?" in *Machine Learning in Radiation Oncology*, pp. 3–11, Springer, 2015.
7. P. Hofmann, C. Samp, and N. Urbach, "Robotic process automation," *Electronic Markets*, vol. 30, no. 1, pp. 99–106, 2020.
8. R.P. Khandpur, A.A. Nanda, M. Davis, C. Li, D. Nurmanbetov, S. Gaur, and A. Talukder, "Adverse media mining for KYC and ESG compliance," *arXiv preprint arXiv:2110.11542*, 2021.
9. D. Kouzis-Loukas, "Learning Scrapy," Packt Publishing Ltd, 2016.
10. P.H. Li, R.P. Dong, Y.S. Wang, J.C. Chou, and W.Y. Ma, "Leveraging linguistic structures for named entity recognition with bidirectional recursive neural networks," in *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pp. 2664–2669, 2017.
11. Y. Li, "Implementation of Anti-Money Laundering Information Systems," Author-House, 2016.
12. R. Peters, "cron," in *Expert Shell Scripting*, pp. 81–85, 2009.
13. Ripjar, "Adverse media screening requirements around the world," Web: <https://ripjar.com/adverse-media-screening-requirements-around-the-world/>.
14. SS&C, "The future of RPA and intelligent automation," Web: <https://www.blueprism.com/>.
15. A.S. Villar and N. Khan, "Robotic process automation in the banking industry: a case study on Deutsche Bank," *Journal of Banking and Financial Technology*, vol. 5, no. 1, pp. 71–86, 2021.

SLOVO AKO “ZBRAŇ” – NEHODNÉ OCHRANY GARANTOVANEJ SLOBODOU PREJAVU

JUDr. Vladislav Marko, PhD., Mgr. Ivana Rubisová, PhD., JUDr. Veronika Hegedúšová

Katedra súkromnoprávných vied, Katedra verejnoprávných vied, Akadémia Policajného zboru v Bratislave, vladislav.marko@akademiapz.sk, ivana.rubisova@akademiapz.sk, veronika.hegedusova@akademiapz.sk

Abstrakt: Sloboda prejavu ako jeden z determinantov demokracie, ako jedno zo základných politických práv každého z nás, ako *condition sine qua non* skutočnej pluralitnej, tolerantnej spoločnosti sa dnes čoraz častejšie stáva obeťou zneužívania (nekorektnou interpretáciou svojej povahy, poslania, účelu) na odstránenie demokratických princípov spoločnosti, zastrasovanie verejnosti, oslabovanie jej hodnotovej orientácie, či politickú destabilizáciu. Vytváranie a šírenie dezinformácií ako jeden z najvýraznejších prejavov hybridného pôsobenia v našich podmienkach, (spochybňujúci, odmietajúci niektoré zo základných princípov demokratického právneho štátu), nenávistné, extrémistické prejavy polarizujúce spoločnosť, (ktorá má tak zvýšenú tendenciu sa radikalizovať), sú svojimi autormi a šíriteľmi mylne obhajované slobodou prejavu. Autori príspevku, analýzou vnútroštátnych ústavnoprávných ustanovení, ako aj obsahu článkov ľudskoprávných dokumentov nadnárodného významu garantujúcich slobodu prejavu, pojednávajú o subjektoch, ktoré informácie a myšlienky šíria alebo prijímajú, forme v akej ich šíri a napokon obsahu týchto informácií a myšlienok, nakoľko je nimi rozsah slobody prejavu vymedzený. Podmienky (dôvody) obmedzenia slobody prejavu stanovujú hranice, ktoré pri zasahovaní do slobody prejavu nemožno prekročiť, ako aj limity pre nositeľov predmetného práva, nerešpektovanie ktorých má za následok nedovoľanie sa ochrany predmetného práva pred súdnymi autoritami. Analýzou tzv. limitačnej klauzuly majúcej svoju vlastnú (aj keď povahou veľmi podobnú) textáciu v rámci jednotlivých právnych úprav (vnútroštátnej aj nadnárodnej) na pozadí rozhodnutí súdnych autorít autori sprehľadňujú charakter relatívnej povahy slobody prejavu, ktorej uplatňovanie nemôže byť a ani nie je bezbrehé.

Kľúčové slová: sloboda prejavu, hybridné hrozby, relatívna povaha slobody prejavu, prípustnosť obmedzenia slobody prejavu, prejavy nepoživajúce ochranu zákona, koncept „brániacej sa demokracie“.

1. K MEDZINÁRODNOPRÁVNYM A ÚSTAVNOPRÁVNYM VÝCHODISKÁM GARANCIE SLOBODY PREJAVU

Univerzálnosť prirodzenej povahy slobody prejavu umožňuje jej uplatňovanie naprieč celým spektrom ľudských práv a slobôd ako v rovine horizontálnej (na úrovni štátu), tak v rovine vertikálnej (na úrovni medzinárodného spoločenstva). K svojej realizácii nepotrebuje žiadny podporný právny predpis a s ohľadom na jednu zo základných charakteristík prirodzených práv existuje nezávisle od štátu, nepochádza od žiadnej moci, ale zo samotnej podstaty a jedinečnosti jedinca ako ľudskej bytosti, a naopak akúkoľvek moc, štátnu nevynímajúc, zaväzuje.²³⁵ Slovom I. Macejkovej, bývalej predsedníčky Ústavného súdu Slovenskej republiky „*Sloboda prejavu predstavuje jeden zo základov demokratickej spoločnosti, je jedným zo základných, ale i najstarších politických práv človeka. Jej význam je pritom v zásade možné rozdeliť do niekoľkých základných okruhov – sloboda prejavu umožňuje hľadanie pravdy, je prostriedkom súťaže a konfrontácie rôznych myšlienok a názorov, je nevyhnutná*²³⁶*na tvorbu slobodnej verejnej mienky, je prostriedkom naplňovania politickej účasti a formovania politickej vôle a je zároveň aj jednou zo základných podmienok pokroku (a vôbec existencie) demokratickej spoločnosti a sebarealizácie (rozvoja) každého jednotlivca.*“. Z ústavnoprávneho hľadiska je, ako uvádza K. Klíma, sloboda prejavu ústavnou kategóriou aj

²³⁵ OROSZ, L., SVÁK, J. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021. s. 331.

²³⁶ MACEJKOVÁ, I. Sloboda prejavu a súdna moc. In MAJERČÁK, T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 7.

ústavnou koncepciou plniacou funkciu objektívnej ústavnej hodnoty. Myšlienka slobody prejavu je podľa jeho slov už tradične chápaná ako politická a právna kategória, rovnako ako aj kategória sociálno-psychologická, ktorá „apriorně znamená možnosť svobodného vnějšího jednání jako projevu vůle osoby.“²³⁷ K. Klíma sa tak prikláňa k názoru M. Bartoňa v tom zmysle, že, „ačkoli je svoboda projevu podřazena rubrice F., politická práva“ „... , lze ji spíše řadit do kategorie politických svobod neboť ji lze jako svobodu podřadit pod „status negativus“, tedy pod sféru osobní autonomie, do které stát nemůže zasahovat.“²³⁸

Ústavnou garanciou slobody prejavu začína v texte Ústavy Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov (ďalej aj „Ústava“, „Ústava SR“) nová skupina základných práv a slobôd podľa predmetu ochrany subsumujúca práva politické. Slovanmi A. Krunkovej, „Ako uvádza P. Molek, skupinu politických práv začína právo, ktoré je z nich najmenej politické, pretože politické prejavy sú z hľadiska obsahu len jedným z druhov slobody prejavu. Pretože politické prejavy sú z hľadiska obsahu len jedným z druhov slobody prejavu.“²³⁹ Sloboda prejavu individuálneho charakteru môže a rovnako býva v spojení s inými právami uplatňovaná rovnako kolektívne, keďže nemožno opomenúť prepojenie slobody prejavu na ďalšie slobody (myslenia, svedomia, náboženského vyznania a viery, vedeckého bádania) a práva, tie politické nevynímajúc, (petičné, zhromažďovacie, združovacie). „Ojedinelým však nie je ani názor, keď sloboda prejavu býva charakterizovaná aj ako priama súčasť iných práv, resp. iné práva ju v sebe môžu zahŕňať, na základe čoho vznikla tzv. teória zložených práv.“²⁴⁰ V kontexte slobody prejavu Ústavný súd Slovenskej republiky konštantne judikuje „Ochrana slobody prejavu je nevyhnutná z viacerých dôvodov. Sloboda prejavu je nevyhnutná pre demokraciu a pre tvorbu slobodnej verejnej mienky v otvorenej spoločnosti. Sloboda prejavu je taktiež nástrojom hľadania pravdy, nástrojom súťaže a konfrontácie rôznych myšlienok a názorov... sloboda prejavu je základným pilierom demokratickej spoločnosti, v ktorej je každému dovolené vyjadrovať sa k verejným veciam a vynášať o nich hodnotové sudy. K veciam verejným pritom nepochybne patrí činnosť orgánov verejnej moci vrátane rozhodovacej činnosti súdov a taktiež činnosť osôb pôsobiacich vo verejnom živote. Tieto činnosti môžu byť verejne posudzované, pričom pri ich kritike platí z princípu demokracie vyplývajúca ústavná prezumpcia, že ide o kritiku dovolenú.“²⁴¹ Ústavný súd Českej republiky považuje slobodu prejavu rovnako za jednu z najdôležitejších hodnôt každej demokratickej spoločnosti a opakovane trvá na tom, že „Základní právo na svobodný projev třeba považovat za konstitutivní znak demokratické pluralitní společnosti a za jednu ze základních podmínek pro její chod a sebeuplatnění jednotlivce. V rámci demokratické pluralitní společnosti je každému dovoleno vyjadřovat se k věcem veřejným a vynášet o nich hodnotící soudy... V podmínkách liberálně demokratického politického zřízení je samozřejmé, že "tyto veřejné

²³⁷ Táto vonkajšia činnosť sa môže podľa K. Klímu uskutočniť v rôznych formách, „jednání nebo i nečinnosti, - otevřeného, prosloveného, napsaného či jinak projeveného vyjádření, - svobodného vyznání a náboženského projevu, - svobodného vyjádření politického názoru, - uměleckého projevu, - vědecko - odborného názoru, - v rámci činnosti v prostoru svobody tiskové, - svobodné kritiky.“ Bližšie: KLÍMA, K. Svoboda projevu a její ústavní limitace. In MAJERČÁK, T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 92.

²³⁸ Tamtiež.

²³⁹ MOLEK, P. Politická práva. Praha: Wolters Kluwer, 2014. s. 29. Citované podľa: OROSZ, L. SVÁK, K. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021, s. 333.

²⁴⁰ OROSZ, L. SVÁK, K. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021, s. 334. Porovnaj s: FILIP, J. Dogmatika slobody prejavu z hľadiska teórie, legislatívy a súdnej praxe. In Časopis pro právní vědu a praxi. 1998, roč. 6, č. 4, s. 619; FILIP, J. Vybrané kapitoly ke studiu ústavního práva. Brno: Masarykova univerzita, 2001. s. 126.

²⁴¹ Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 152/08 zo dňa 15. decembra 2009. Porovnaj s nálezom Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 326/09 zo dňa 4. marca 2010, nálezom Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 439/2016 zo dňa 27. októbra 2016.

záležitosti, resp. veřejná činnost jednotlivých osob mohou být veřejně posuzovány. Při kritice veřejné záležitosti vykonávané veřejně působícími osobami platí z hlediska ústavního presumpce o tom, že jde o kritiku dovolenou. Jde o výraz demokratického principu, o výraz participace občanské společnosti na věcech veřejných.“.²⁴² Bývalý předseda Ústavního soudu České republiky P. Rychetský k povaze slobody projevu, osobitne vo vzťahu k orgánom verejnej moci uvádza „*Svoboda projevu se rozhodně nekryje s hledáním pravdy a stát zde není od toho, aby určoval vítěze pomyslných soutěží o nejsprávnější či nejpravdivější výrok. Naopak. Svoboda projevu je svojí povahou typickou součástí tzv. negativního statusu v rámci veřejného subjektivního práva, takže veřejná moc nemá uloženu povinnost nějaký projev šířit anebo mu tleskat, ale musí jedince chránit do té míry, aby svůj názor mohl nerušeně vyjádřit. Této ochrany může jedinec využít, ale stejně tak může využít i reverzního aspektu tohoto práva a hledat u státu ochranu kvůli tomu, že jej k projevu někdo nutí.*“.²⁴³

Vychádzajúc z kategorizácie ľudských práv s ohľadom na historický prístup, uplatňujúc tzv. generačný princíp, patrí sloboda prejavu, podľa obdobia, v ktorom sa stala všeobecne uznávanou, minimálne, potreba jej deklaratórnej garancie, k právam prvej generácie. Právne zakotvenie slobody prejavu nachádzame už v texte Deklarácie práv človeka a občana (z 26. augusta 1789), v rámci ktorej článok XI ustanovuje, „*Slobodná komunikácia myšlienok a názorov je jedným z najvzácnejších ľudských práv; v dôsledku toho môže každý občan slobodne hovoriť, písať a tlačiť, výmenou za reakciu na zneužívanie tejto slobody v prípadoch určených zákonom.*“. Všeobecná deklarácia ľudských práv, prijatá Valným zhromaždením OSN dňa 10. decembra 1948, ako kľúčový ľudskoprávny dokument programového charakteru, vyhlasujúc všeobecné princípy medzinárodného štandardu ľudských práv, zakotvila slobodu prejavu článkom 19 v znení „*Každý má právo na slobodu presvedčenia a prejavu; toto právo nepripúšťa, aby niekto trpel ujmu za svoje presvedčenie a zahrňuje právo vyhľadávať, prijímať a rozširovať informácie a myšlienky akýmikoľvek prostriedkami a bez ohľadu na hranice.*“. Dňa 19. decembra 1966 bol v New Yorku otvorený na podpis Medzinárodný pakt o hospodárskych, sociálnych a kultúrnych právach a Medzinárodný pakt o občianskych a politických právach,²⁴⁴ ktorý (zhodne) v článku 19 garantuje slobodu prejavu každému, pričom toto právo „*zahrňa slobodu vyhľadávať, prijímať a rozširovať informácie a myšlienky každého druhu, bez ohľadu na hranice, či už ústne, písomne alebo tlačou, prostredníctvom umenia alebo akýmikoľvek inými prostriedkami podľa vlastnej voľby.*“. Predmetný článok 19 ods. 3 rovnako reflektuje relatívnu povahu slobody prejavu formuláciou „*Užívanie práv uvedených v odseku 2 tohto článku nesie so sebou osobitné povinnosti a zodpovednosť. Môže preto podliehať určitým obmedzeniam, tieto obmedzenia však budú len také, aké ustanovuje zákon a ktoré sú nevyhnutné: a) na rešpektovanie práv alebo povestí iných; b) na ochranu národnej bezpečnosti alebo verejného poriadku alebo verejného zdravia alebo morálky.*“

²⁴² „*O tom, co lze považovat za věc veřejnou, se Ústavní soud vyjádřil v nálezu sp. zn. I. ÚS 453/03 ze dne 11. 11. 2005 (N 209/39 SbNU 215), podle něhož jsou věci veřejnou veškeré agendy státních institucí, jakož i činnost osob působících ve veřejném životě, ale i umění včetně showbyznysu, a dále vše, co na sebe upoutává veřejnou pozornost.*“ Bližšie: Nález Ústavního soudu České republiky sp. zn. I. ÚS 823/11 zo dňa 6. marca 2012.

²⁴³ RYCHETSKÝ, P. Svoboda projevu a její ochrana před Ústavním soudem. In MAJERČÁK, T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 42.

²⁴⁴ V mene Československej socialistickej republiky boli oba pakty podpísané v New Yorku 7. októbra 1968. Federálne zhromaždenie Československej socialistickej republiky k nim vyslovilo súhlas dňa 11. novembra 1975. Pre Československú socialistickú republiku nadobudli platnosť dňa 23. marca 1976. Bližšie: Vyhláška ministra zahraničných vecí č. 120/1976 Zb. o Medzinárodnom pakte o občianskych a politických právach a Medzinárodnom pakte o hospodárskych, sociálnych a kultúrnych právach.

V rámci výpočtu dokumentov nadnárodného významu svojím obsahom garantujúcich slobodu prejavu, upriamujeme pozornosť osobitne na obsah článku 10 Dohovoru o ochrane ľudských práv a základných slobôd (ďalej aj „Dohovor“), ako kľúčovej ľudskoprávnej doktríny (kreovanej už ako súčasť európskeho regionálneho systému ochrany ľudských práv) podpísaného 4. novembra 1950 v Ríme (s platnosťou od 3. septembra 1953), v zmysle ktorého, „Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice...“. Súčasťou predmetného článku je rovnako tzv. limitačná klauzula, ktorá svojím obsahom predznamenaáva legitímne obmedzenie slobody prejavu, vyjadrená odsekom 2 v znení „Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci.“. Na tomto mieste si dovoľíme krátku poznámku smerom k inštitucionálnemu mechanizmu ochrany práv a slobôd, ktoré sú garantované textom Dohovoru, s cieľom domáhania sa ich reálnej ochrany, ako aj nápravy v prípade ich porušenia. Nezastupiteľný význam na predmetnom úseku zohráva činnosť Európskeho súdu pre ľudské práva, ktorého judikatúra je prameňom práva s potenciálnou prednosťou pred zákonmi Slovenskej republiky. Slovanmi I. Macejkovej, „Praktický význam judikatúry ESHP je o to väčší, že množstvo významných otázok nedostalo dosiaľ vnútroštátnu interpretáciu v rozhodnutiach ústavného súdu, a tak judikatúra ESHP vyplňa „vákuum“ v domácom právnom poriadku.“.²⁴⁵

Na regionálnej európskej úrovni je právo na slobodu prejavu garantované rovnako textom Charty základných práv Európskej únie zo dňa 7. decembra 2000 (ďalej aj ako „Charta“).²⁴⁶ Článok 11 Charty ustanovuje, že „Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice. Rešpektuje sa sloboda a pluralita médií.“. Je na mieste poukázať na absenciu zmienky (v predmetnom článku) o možných obmedzeniach slobody prejavu, vyjadrenej napr. ods. 2 článku 10 Dohovoru o ochrane ľudských práv a základných slobôd, ods. 3 článku 19 Medzinárodného paktu o občianskych a politických právach, ako aj (zatiaľ nezmeneným) ods. 4 článku 26 Ústavy SR. Ako uvádzajú (o.i.) autorky G. Dobrovičová, M. Jánošíková, „Je to dôsledok inej koncepcie Charty, ktorá má možnosť obmedzení upravenú spoločne pre všetky práva a zásady v čl. 52 Charty v rámci hlavy VIII týkajúcej sa všeobecných ustanovení upravujúcich výklad a uplatňovanie Charty.“.²⁴⁷ V zmysle ods. 1 až 3 článku 52 Charty, musí byť akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. „Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú

²⁴⁵ MACEJKOVÁ, I. Sloboda prejavu a súdna moc. In MAJERČÁK, T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 9.

²⁴⁶ „...Charta bola slávnostne vyhlásená Parlamentom, Radou a Komisiou v Nice v roku 2000, zatiaľ ako právne nezáväzná deklarácia. Po tom, čo bola zmenená, bola opäť vyhlásená v roku 2007. Až prijatím Lisabonskej zmluvy 1. decembra 2009 však Charta ZP nadobudla priamu účinnosť, ako sa uvádza v čl. 6 ods. 1 ZEÚ, čím sa stala záväzným zdrojom primárneho práva, rovnocenným so zakladajúcimi zmluvami.“ Bližšie: CHRENŠT, J. NESVADBA, A. 2020. Právo Európskej únie. Bratislava: Akadémia Policajného zboru v Bratislave, 2020. s. 149.

²⁴⁷ DOBROVIČOVÁ, G. JÁNOŠIKOVÁ, M. Sloboda prejavu v Charte základných práv Európskej únie. In MAJERČÁK, T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 86.

uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných. Práva uznané v tejto charte, ktoré sú predmetom ustanovení zmlúv, sa vykonávajú za podmienok a v medziach vymedzených týmito zmluvami. V rozsahu, v akom táto charta obsahuje práva, ktoré zodpovedajú právam zaručeným v Európskom dohovore o ochrane ľudských práv a základných slobôd, zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom dohovore. Toto ustanovenie nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany týchto práv.²⁴⁸ Charta základných práv Európskej únie nerozširuje rozsah pôsobnosti práva Európskej únie nad rámec jej právomocí,²⁴⁹ rovnako nezakladá žiadnu novú právomoc ani úlohu pre Európsku úniu, a svojím obsahom nemení právomoci a úlohy vymedzené v zmluvách.²⁵⁰ Európska únia v kontexte významu pri vykonávaní, dodržiavaní obsahu Charty základných práv Európskej únie sústreďuje pozornosť na vnútroštátne subjekty, Európsky parlament zdôrazňuje, že práve súdne orgány, orgány presadzovania práva a správne orgány vo vnútri štátov zohrávajú kľúčovú úlohu pri zabezpečovaní účinku práv a slobôd deklarovaných v Charte. „Rada Európskej únie zdôrazňuje, že vo vnútroštátnom kontexte je potrebné uplatňovať chartu ako súčasť širšieho súboru uplatniteľných zdrojov základných práv ... s cieľom účinne uplatňovať chartu je potrebné, aby vnútroštátne orgány venovali osobitnú pozornosť tým ustanoveniam charty, ktorých význam a rozsah pôsobnosti neurčujú zodpovedajúce ustanovenia Európskeho dohovoru o ľudských právach...“²⁵¹ V tomto ohľade ustanovenie článku 52 ods. 3 Charty podnecuje, resp. nevylučuje extenzívny výklad práv normovaných obsahom medzinárodných alebo iných európskych dokumentov.

2. K RELATÍVNEJ POVAHE SLOBODY PREJAVU

Nemožnosť interpretácie slobody prejavu ako slobody absolútnej povahy bez možnosti jej obmedzenia za zákonom stanovených dôvodov bola už predznamenaná poukazom na tzv. limitačné klauzuly, ktoré sú predmetom úprav jednotlivých článkov garantujúcich slobodu prejavu. Rovnako z konštantnej judikatúry súdnych autorít vyplýva, že v niektorých situáciách musí sloboda prejavu ustúpiť v zmysle obsahu predmetnej tzv. limitačnej klauzuly. Zúžime pozornosť na jej vyjadrenie v textoch dokumentov, ktoré sú pre rozhodovaciu prax orgánov súdnej moci Slovenskej republiky prioritné, a sice ods. 4 článku 26 Ústavy SR a ods. 2 článku 10 Dohovoru o ochrane ľudských práv a základných slobôd. Ich znenie explicitne uvádza dôvody obmedzenia slobody prejavu, pričom takéto obmedzenie musí byť stále v súlade s demokratickým charakterom spoločnosti.²⁵² Vyjadrením relatívnej povahy článku 26 Ústavy SR v ods. 4 ústavodarca počíta s obmedzujúcimi zásahmi do slobody prejavu. Naopak (zakázané) zásahy do slobody prejavu a sice zákaz cenzúry, v zmysle článku 26 ods. 3 nemožno vykonať, ide o zákaz v absolútnom zmysle slova bez prípustnosti obmedzenia. Vykonať možno jedine obmedzujúce zásahy do slobody prejavu za splnenia materiálnych a formálnych

²⁴⁸ Charta základných práv Európskej únie, článok 52, ods. 1-3

²⁴⁹ „Rešpektujúc právomoci a úlohy Únie, ako aj dodržiavanie zásady subsidiarity, táto charta opätovne potvrdzuje práva vyplývajúce najmä z ústavných tradícií a medzinárodných záväzkov spoločných pre členské štáty, Európskeho dohovoru o ochrane ľudských práv a základných slobôd, sociálnych chart prijatých Úniou a Radou Európy, ako aj judikatúry Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva.“ Charta základných práv Európskej únie, Preambula

²⁵⁰ Charta základných práv Európskej únie, článok 51, odsek 2

²⁵¹ Agentúra Európskej únie pre základné práva, 2020. Uplatňovanie Charty základných práv Európskej únie v práve a pri tvorbe politik na vnútroštátnej úrovni. Usmernenie. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2020. s. 12. Dostupné na: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_sk.pdf

²⁵² Napr. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 152/08 zo dňa 15. decembra 2009

podmienok vyjadrených v článku 26 ods. 4 Ústavy SR, rešpektujúc pre Slovenskú republiku záväzný obsah ods. 2 článku 10 Dohovoru o ochrane ľudských práv a základných slobôd.²⁵³

Pri určovaní **rozsahu obmedzenia slobody prejavu** sa posudzuje, či obmedzujúce podmienky, sú založené na základe zákona, sledujú legitímny cieľ, ako aj to, či ich uplatnenie bolo nevyhnutné v demokratickej spoločnosti.²⁵⁴ Ako uvádza J. Svák, je rozsah slobody prejavu vymedzený „**subjektom**, ktorý informácie a myšlienky šíru alebo prijíma, **formou** v akej ich šíri a napokon **obsahom** týchto informácií a myšlienok. Preto vymedzenie rozsahu slobody prejavu znamená určiť a) subjekt prejavu, b) obsah prejavu, c) formu prejavu.“²⁵⁵ V kontexte subjektu možno konštatovať, že sa sloboda prejavu vzťahuje ako na fyzickú, tak aj právnickú osobu, čo konštantne judikuje Európsky súd pre ľudské práva interpretujúc slobodu prejavu garantovanú článkom 10 Dohovoru o ochrane ľudských práv a slobôd, z ktorého teda profitujú všetky fyzické a právnické osoby, avšak nie v rovnakom rozsahu, pričom sú rozdiely podmienené (aj) postavením subjektu, či je šíriteľom / prijímateľom informácií, myšlienok, resp. sám je predmetom týchto informácií. V nadväznosti na uvedené je pri subjektoch slobody prejavu potrebné rozlišovať a) šíriteľa informácií a myšlienok, b) prijímateľa informácií a myšlienok, c) subjekt ako predmet informácií. Rozsah a spôsob obmedzenia slobody prejavu (vymedzujúc subjekt prejavu) je determinovaný „**povinnosťou a zodpovednosťou**“ **subjektu šíriaceho informácie a myšlienky**. Obmedzenie slobody prejavu vyplývajúce z „povinnosti a zodpovednosti“ spravidla vyplývajú z (osobitného) postavenia subjektu. Rozhodnutia Európskeho súdu pre ľudské práva vo veciach, ktorých predmetom bolo obmedzenie slobody prejavu pre šíriteľov informácií a myšlienok spojených v duchu myšlienky „povinnosť a zodpovednosť“ sa týkajú predovšetkým príslušníkov ozbrojených síl, štátnych zamestnancov, sudcov, advokátov, novinárov. Subjekt ako šíriteľ informácií a myšlienok, je pri aplikácii slobody prejavu limitovaný jednak „*obmedzením rozsahu informácií, ktoré môže šíriť, z dôvodu, že sú osobitne chránené a šíriteľ sa ich dozvedel v súvislosti s výkonom svojej funkcie,*“ ako aj „*možnosťami šírenia informácií, ktoré sú limitované spoločenským postavením ši charakterom funkcie, alebo práce šíriteľa informácií.*“²⁵⁶

Na ilustráciu skupiny **prípádov obmedzujúcich slobodu prejavu šíriteľov informácií z dôvodu, že sú osobitne chránené a šíriteľ sa ich dozvedel v súvislosti s výkonom svojej funkcie** z judikatúry Európskeho súdu pre ľudské práva vyberáme rozhodnutie Európskeho súdu pre ľudské práva vo veci Hadjianastassious proti Grécku zo dňa 16. decembra 1992, sťažnosť č. 12945/87. „*Sťažovateľ slúžil ako kapitán gréckeho vojenského letectva. V roku 1982 predložil Leteckému vojenskému, technickému, výskumnému stredisku (KETA) správu o vývoji riadenej strely, na ktorom sa zúčastnil. V roku 1983 predal súkromnej spoločnosti ELFON Ltd. Inú technickú štúdiu o riadených strelách, ktorú vypracoval sám. Za to bol odsúdený na dva a pol roka trestu odňatia slobody pre trestný čin vyzradenie vojenského tajomstva. Odvolacie súdy tento trest zmiernili. V sťažnosti zaslanej do Štrasburgu uviedol, že jeho trest za vyzradenie vojenského tajomstva menšieho významu znamenal porušenie jeho práva na slobodu prejavu garantovaného článkom 10 Európskeho dohovoru. Sťažovateľ popieral, že jeho zásah do práva na slobodu prejavu bol nevyhnutný. Pritom argumentoval tým, že bežnú štúdiu, spočívajúcu výlučne na jeho vlastnej dokumentácii, nemožno považovať za*

²⁵³ Porovnaj s: OROSZ, L., SVÁK, J. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021. s. 355.

²⁵⁴ Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 174/17 zo dňa 4. januára 2018

²⁵⁵ SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s.r.o., 2006. s. 729.

²⁵⁶ Bližšie: SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s.r.o., 2006. s. 731 – 732.

poškodujúcu národnú bezpečnosť. Aby tomu tak mohlo byť, museli by existovať pravidlá zakazujúce alebo povoľujúce gréckym vojakom pracovať pre súkromné firmy – takého pravidlá však neexistovali. Uvedený vojenský projekt bol síce kvalifikovaný ako predmet vojenského tajomstva, ale vojenský súd obvinil sťažovateľa za vyzradenie „všeobecných informácií“, ktoré by mali byť v záujme armády uchované v tajnosti. Experti menovaní vojenským súdom sa vyslovili v tom zmysle, že aj keď v oboch štúdiách boli aplikované rôzne metódy, napriek tomu došlo k určitému transferu technického know-how. Zhodne s gréckou vládou Súd konštatoval, že odhalenie štátneho záujmu na určitej zbrani a zodpovedajúceho know-how, ktoré môže byť indikáciou o stave pokročilosti jeho vývoja, môže do značnej miery poškodiť štátnu bezpečnosť. Vzal tiež do úvahy zvláštne podmienky vojenského života a špecifické „povinnosti“ a „zodpovednosť“ členov ozbrojených síl... Sťažovateľ ako vojenský dôstojník poverený experimentálnym vývojom v oblasti riadených striel bol viazaný povinnosťou mlčanlivosti. Podľa názoru Súdu nebolo možné tvrdiť, že by grécke vojenské súdy prekročili hranicu voľnej úvahy, ktorá je vnútroštátnym orgánom priznaná v oblasti národnej bezpečnosti. Neexistoval ani dôkaz o tom, že by bol porušený rozumný vzťah primeranosti medzi použitými prostriedkami a sledovaným legitímnym účelom.“ V predmetnej veci Európsky súd pre ľudské práva formuloval záver, že konaním vnútroštátnych súdov, ktoré namietal sťažovateľ, článok 10 Dohovoru nebol porušený.

Na ilustráciu skupiny **prípadov obmedzujúcich slobodu šíriteľov informácií z dôvodu ich osobitného postavenia** poslúži rozhodnutie Európskeho súdu pre ľudské práva vo veci Rekvenyi proti Maďarsku zo dňa 20. mája 1999, sťažnosť č. 25390/94. Sťažovateľ v predmetnej veci, štátny príslušník Maďarskej republiky, policajt, generálny tajomník nezávislých policajných odborov, podal v roku 1994 v mene policajných odborov ústavnú sťažnosť na Ústavný súd Maďarskej republiky proti novelizovanému zneniu maďarskej Ústavy, v dôsledku ktorého sa zakázalo policajtom členstvo v politickej strane a politická činnosť vôbec. V ústavnej sťažnosti policajné odbory zastúpené sťažovateľom tvrdili, že novelizovaný článok Ústavy je nezlučiteľný so všeobecne uznávanými princípmi medzinárodného práva, rovnako namietali jeho prijatie v rozpore s ústavou. Ústavný súd Maďarskej republiky predmetnú sťažnosť odmietol s poukazom na to, že nemá právomoc zrušiť ustanovenie Ústavy. Sťažovateľ sa v predmetnej veci obrátil so sťažnosťou na Európsky súd pre ľudské práva, namietajúc, že novelizované články Ústavy porušujú jeho právo na slobodu prejavu garantovanú článkom 10 Dohovoru o ochrane ľudských práv a základných slobôd, ako aj to, že sú príliš všeobecné a neurčité, v dôsledku čoho svojvoľne interpretovateľné. Zásah do slobody prejavu mal podľa sťažovateľa spočívať v tom, že jeho príslušnosť k policajnému zboru, nemôže zakladať právo štátu na tak široký zásah do jeho práva na slobodu prejavu, v podobe znemožnenia jeho podielu na akejkoľvek politickej diskusii. Neurčitosť novelizovaných ustanovení mala podľa sťažovateľa spočívať v tom, že z predmetných ustanovení nie je celkom zrejmé, aké aktivity spadajú pod pojem politická činnosť, čo podľa sťažovateľa vedie nevyhnutne k možnosti určitej svojvôle pri interpretácii. Vláda Maďarskej republiky k predmetnej sťažnosti v rámci svojej argumentácie uviedla, že zákon o polícii z roku 1994 a vyhláška z roku 1995 s predmetnou novelou Ústavy spoločne vytvorili dostatočne podrobný rámec upresňujúci obmedzenia uvalené na policajtov, čo sa ich výkonu politickej činnosti týka, čím spĺňali stupeň predvídateľnosti požadovaný ods. 2 článku 10 Dohovoru o ochrane ľudských práv a základných slobôd. Pokiaľ ide o legitímny cieľ, vláda Maďarskej republiky tvrdila, že predmetný zásah sledoval predovšetkým depolitizáciu polície, a to v dobe, kedy Maďarsko prechádzalo od totalitného režimu k pluralitnej demokracii a teda bol nevyhnutný v záujme národnej bezpečnosti a verejnej bezpečnosti, ako aj na ochranu verejného poriadku, aby sa obnovila dôvera občanov v nezávislú a apolitickú políciu. Európsky súd pre ľudské práva pri posudzovaní toho, či došlo k zásahu do sťažovateľovho práva na slobodu prejavu, ktorá je

garantovaná článkom 10 Dohovoru, jednoznačne konštatoval, že výkon činností politického charakteru spadá pod predmetný článok, a to v miere, v akej sloboda politickej diskusie predstavuje konkrétny aspekt slobody prejavu. „Sloboda politickej diskusie vskutku leží v samotnom jadre pojmu demokratická spoločnosť. ... Súd konštatoval, že policajti sú v službách štátu. Občania od nich môžu oprávnené očakávať, že pri vybavovaní ich osobných záležitostí na polícii im budú radiť politicky neutrálni zamestnanci, ktorí stoja úplne stranou od politického boja. Čo sa týka posúdenia nevyhnutnosti zásahu v demokratickej spoločnosti, Súd dospel k záveru, že vzhľadom na postavenie verejných činiteľov – v tomto prípade policajtov, aj keď je legitímne, aby im štát vzhľadom na ich postavenie uložil povinnosť diskretnosti, predsa len ide o osoby, ktoré tiež majú právo na slobodu prejavu podľa článku 10 Európskeho dohovoru. Súd preto musí v každom prípade posudzovať, či bola dodržaná spravodlivá rovnováha medzi základným právom jednotlivca na slobodu prejavu a legitímnym právom štátu bdieť nad tým, aby jeho inštitúcie pracovali pre účely uvedené v článku 10 ods. 2 Európskeho dohovoru. Súd uznal, že pokiaľ ide o právo štátnych zamestnancov na slobodu prejavu, povinnosti a zodpovednosť z ods. 2 článku 10 Európskeho dohovoru nadobúdajú zvláštny význam, ktorý ospravedlňuje ponechanie určitého priestoru žalovanému štátu na posúdenie, či inkriminovaný zásah je primeraný vyššie uvedenému cieľu. Súd záverom uviedol, že s ohľadom na posudzovaný priestor v danom historickom kontexte mohli byť príslušné opatrenia prijaté Maďarskom na ochranu policajných síl pred priamym vplyvom politických strán pokladané za zodpovedajúce naliehavej spoločenskej potrebe v demokratickej spoločnosti a rozhodol, že nedošlo k porušeniu článku 10 Európskeho dohovoru.“²⁵⁷

Z konštantnej judikatúry Európskeho súdu pre ľudské práva v kontexte interpretácie článku 10 Dohovoru z hľadiska jeho **obsahu** vyplýva prioritná ochrana prejavov týkajúcich sa otázok verejného záujmu zabezpečujúc politický pluralizmus. „Pojem verejný záujem sa však v rozhodovacej činnosti štrasburských orgánov ochrany práva stal veľmi flexibilným a ... aj veľmi extenzívne vykladaným.“²⁵⁸ S ohľadom na obsah prejavu je na základe ich materiálnej príbuznosti možno vyabstrahovať viacero kategorizácií prejavov. Jedným z prístupov k diferenciacii prejavov podľa priznania intenzity ochrany je členenie prejavov na politické, umelecké a komerčné. Prejavy prispievajúce k spoločenskej debate, k politickému diskurzu, teda prejavy politické požívajú vyššiu mieru ochrany, prejavy komerčné a umelecké sú slobodou prejavu chránené menej. Uvedené je dôkazom existencie a všeobecnej akceptácie, potvrdenej aj rozhodovacou súdnou praxou, **hierarchickej kategorizácie prejavov**. Aj rozhodnutie Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, č. sťažnosti 29032/95 s ohľadom na použitú argumentáciu súdu dokazuje, že politické prejavy, ktoré sa týkajú otázok verejného záujmu, požívajú vyššiu mieru ochrany a najnižšiu mieru voľnej úvahy uplatnenej zo strany zmluvného štátu Dohovoru pri ich obmedzovaní. „Súd vyjadruje názor, že podpora slobodnej politickej diskusie je veľmi dôležitým znakom demokratickej spoločnosti. Prikladá najvyššiu dôležitosť slobode prejavu v kontexte politickej diskusie a je názoru, že sa vyžadujú veľmi silné dôvody na to, aby sa ospravedlnilo obmedzenie politického prejavu. V dotknutom štáte by pripustenie širokých obmedzení na politický prejav v konkrétnych prípadoch nepochybne všeobecne postihlo rešpektovanie slobody prejavu.“²⁵⁹ Zvýšená miera ochrany politických prejavov sa neodvíja len od obsahu, ktorý je prezentovaný, ale je rovnako v tomto prípade viazaná na subjekt.

²⁵⁷ Citované podľa: <https://www.epi.sk/rozhodnutie-sudu/Rekvenyi-proti-Madarsku-Politicka-angazovanost-policajtov.html>

²⁵⁸ SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s r.o., 2006. s. 752.

²⁵⁹ Rozhodnutie Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, sťažnosť č. 29032/95.

V predmetnom prípade Európsky súd pre ľudské práva ďalej pripomína, „že existuje len malý priestor podľa článku 10 ods. 2 Dohovoru na obmedzenie politických prejavov alebo diskusie o otázkach verejného záujmu...“. Na druhej strane súd ale dodáva, že rovnako „hranica prijateľného kriticismu je širšia pokiaľ ide o politika ako takého ako v prípade súkromnej osoby. Na rozdiel od súkromnej osoby, politik sa otvára podrobnému skúmaniu jeho slov a činov zo strany novinárov a verejnosti, a preto musí prejavovať väčší stupeň tolerancie.“ Na tomto mieste ale nemožno neuviesť, že **nie každý prejav politika, je zároveň prejavom politickým**, teda prejavom požívajúcim zvýšenú ochranu garantovanú slobodou prejavu, ide napr. o prejavy extrémistické. „V tomto prípade nezohráva politický presah prejavu žiadnu úlohu, vylúčené z ochrany sú tak politické extrémistické prejavy, ako aj tzv. nenávistné prejavy či prejavy spojené s pornografiou, resp. blasfemiou (rúhaním).“²⁶⁰

Na ilustráciu z judikatúry Európskeho súdu pre ľudské práva v súvislosti s prejavmi nepožívajúcimi ochranu podľa článku 10 Dohovoru uvádzame rozhodnutie Európskeho súdu pre ľudské práva vo veci Pavel Ivanov proti Rusku zo dňa 20. februára 2007. „*Sťažovateľ, majiteľ a editor novín, bol odsúdený za verejné podnecovanie k etnickej, rasovej a náboženskej nenávisti prostredníctvom masmédií. Je autorom a vydavateľom série článkov znázorňujúcich Židov ako zdroj zla v Rusku, požadujúcich ich vylúčenie zo spoločenského života. Obviňoval celú etnickú skupinu z prípravy sprisahania proti ruskému ľudu a pripísal fašistickú ideológiu židovským čelným predstaviteľom. Sťažovateľ vo svojich publikáciách, ako aj vo svojich ústnych vyjadreniach na súde sústavne upieral Židom právo na národnú hrdosť, tvrdiac, že netvorí národ. Sťažovateľ sa sťažoval najmä na to, že jeho odsúdenie za podnecovanie k rasovej nenávisti bolo neodôvodnené. EŠLP vyhlásil sťažnosť za neprijateľnú (nezlučiteľnú ratione materiae). Nemal pochyb o výrazne antisemitskom charaktere názorov sťažovateľa a súhlasil s posúdením zo strany vnútroštátnych súdov, že prostredníctvom svojich publikácií sa snažil podnecovať nenávisť voči židovskému obyvateľstvu. Takýto všeobecný a prudký útok na jednu etnickú skupinu je namierený proti základným hodnotám Dohovoru, predovšetkým proti tolerancii, sociálnemu zmieru a nediskriminácii. Preto podľa článku 17 Dohovoru (zákaz zneužitia práv), sťažovateľ nemohol požívať ochranu v zmysle článku 10 Dohovoru (sloboda prejavu).*“²⁶¹ Rovnako nezlučiteľný s obsahom Dohovoru, s hodnotami v ňom zaručenými, ním hlásanými, bol prejav sťažovateľa, ktorý vo svojom okne umiestnil plagát Britskej národnej strany, ktorej bol členom, znázorňujúci budovu Twin Towers v plameni. Plagát bol doplnený slovami: "Islam z Británie - chráňte britský národ". V dôsledku toho bol sťažovateľ odsúdený za nepriateľstvo voči náboženskej skupine s prítážujúcimi okolnosťami. Predmetnú sťažnosť (Norwood proti Spojenému kráľovstvu) EŠLP vyhlásil rozhodnutím o prijateľnosti zo 16. novembra 2004 za neprijateľnú. „*Konštatoval, že vo všeobecnosti platí, že takýto prudký útok proti náboženskej skupine, spájajúcej skupinu ako celok s vážnym teroristickým činom, bol nezlučiteľný ... najmä s toleranciou, sociálnym zmierom a nediskrimináciou. EŠLP preto rozhodol, že umiestnenie plagátu sťažovateľom v jeho okne predstavovalo skutok v zmysle článku 17 Dohovoru (zákaz zneužitia práv), a že sťažovateľ teda nemôže požadovať ochranu v zmysle článku 10 Dohovoru (sloboda prejavu).*“²⁶²

²⁶⁰ Bližšie: OROSZ, L., SVÁK, J. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021. s. 336.

²⁶¹ Citované podľa: Factsheet — Hate Speech. 2017. Štrasburg : Európsky súd pre ľudské práva, 2017. Dostupné na: [FS_Hate_speech_SLK \(coe.int\)](https://www.echr.europa.eu/en/cases-and-decisions/other/key-ecj-and-echr-cases/key-ecj-cases/fs_hate_speech_slk_coe_int) Preklad: Kancelária zástupcu Slovenskej republiky pred Európskym súdom pre ľudské práva.

²⁶² Citované podľa: Factsheet — Hate Speech. 2017. Štrasburg : Európsky súd pre ľudské práva, 2017. Dostupné na: [FS_Hate_speech_SLK \(coe.int\)](https://www.echr.europa.eu/en/cases-and-decisions/other/key-ecj-and-echr-cases/key-ecj-cases/fs_hate_speech_slk_coe_int) Preklad: Kancelária zástupcu Slovenskej republiky pred Európskym súdom pre ľudské práva.

S ohľadom na ods. 2 článku 10 Dohovoru o ochrane ľudských práv a základných slobôd²⁶³ stanovujúceho podmienky, za ktorých možno obmedziť slobodu prejavu je pre rozhodovaciu prax súdnych autorít dôležité špecifikovať **a) druhy (spôsoby) obmedzení slobody prejavu**, ako aj **b) podmienky (dôvody) týchto obmedzení**. Druhy obmedzení, sankcií možno vo všeobecnosti rozdeliť na a) preventívne, b) represívne, pričom Európsky súd pre ľudské práva konštantne posudzuje aj primeranosť sankcie z hľadiska jej nevyhnutnosti v demokratickej spoločnosti, s preferenciou (v závislosti od prípadu) občianskoprávných sankcií pred trestnoprávnymi. Uvedené potvrdil rovnako rozhodnutím vo veci Lehideux a Isorni proti Francúzsku zo dňa 23. septembra 1998, č. sťažnosti 24662/94, kedy k porušeniu článku 10 Dohovoru došlo práve uložením trestnoprávnej sankcie voči sťažovateľom zo strany zmluvného štátu, ktorá bola po dôslednom posúdení okolností prípadu Európskym súdom pre ľudské práva vyhodnotená ako neprimeraná a v demokratickej spoločnosti nie nevyhnutná. Neprimeraná výška občianskoprávnej sankcie bola v ďalšom prípade (rozhodnutie Európskeho súdu pre ľudské práva vo veci Steel a Morris proti Spojenému kráľovstvu zo dňa 15. februára 2005, č. sťažnosti 68416/01) rovnako dôvodom pre porušenie článku 10 Dohovoru o ochrane ľudských práv a základných slobôd.

Podmienky (dôvody) obmedzení slobody prejavu diferencované na všeobecné a konkrétne stanovujú pre zmluvné strany Dohovoru o ochrane ľudských práv a základných slobôd hranice, ktoré pri zasahovaní do slobody vyjadrenej článkom 10 Dohovoru nemožno prekročiť, ako aj limity pre nositeľov predmetného práva, nerešpektovanie ktorých má za následok nedovolenie sa ochrany predmetného práva pred súdnymi autoritami.

Medzi **všeobecné podmienky obmedzenia slobody prejavu**, ktoré vychádzajú zo spoločných ustanovení Dohovoru o ochrane ľudských práv a základných slobôd vzťahujúce sa na výkon každého ľudského práva chráneného štrasburskými orgánmi ochrany práva, patrí a) možnosť odstúpenia od nich v prípade vojny alebo iného verejného ohrozenia (vyjadrená článkom 15 Dohovoru²⁶⁴), b) možnosť uvaliť obmedzenia na politickú činnosť cudzincov (vyjadrená článkom 16 Dohovoru²⁶⁵), c) možnosť obmedzenia slobody prejavu v prípade jej zneužívania (vyjadrená článkom 17 Dohovoru, pojednávajúcom a zákaze zneužitia práv všeobecne, v znení „Nič v tomto dohovore sa nesmie vykladať ako oprávnenie pre štát, skupinu alebo osobu vykonávať činnosť alebo uskutočniť skutok s cieľom narušiť práva alebo slobody v dohovore zakotvené, alebo na obmedzovanie týchto práv a slobôd vo väčšom rozsahu, než je stanovené v dohovore“).²⁶⁶ K poslednej všeobecnej podmienke obmedzenia slobody prejavu v prípade jeho zneužívania z rozhodovacej činnosti Európskeho súdu pre ľudské práva na ilustráciu uvádzame rozhodnutie vo veci Glimmerveen a Hagenbeek proti Holandsku, kedy „sťažovateľ

²⁶³ „Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinom, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenie úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci.“ Dohovor o ochrane ľudských práv a základných slobôd, článok 10, ods. 2

²⁶⁴ „V prípade vojny alebo akéhokoľvek iného verejného ohrozenia existencie štátu, môže ktorákoľvek Vysoká zmluvná strana prijať opatrenia smerujúce k odstúpeniu od záväzkov vyplývajúcich z tohto dohovoru v rozsahu, v akom to bezprostredne vyžaduje naliehavosť situácie a za predpokladu, že tieto opatrenia sú zlučiteľné s jej inými záväzkami podľa medzinárodného práva.“ Dohovor o ochrane ľudských práv a základných slobôd, článok 15, ods. 1

²⁶⁵ „Nič v článkoch 10, 11 a 14 sa nemôže považovať za brániace Vysokým zmluvným stranám uvaliť obmedzenia na politickú činnosť cudzincov.“ Dohovor o ochrane ľudských práv a základných slobôd, článok 16

²⁶⁶ Bližšie: SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľ'a, spol. s r.o., 2006. s. 778.

J. Glimmerveen bol predsedom politickej strany Nederlandse Volks Unie, ktorej základnými princípmi, ako ich opísal sám sťažovateľ, bola svetová koncepcia, ktorá každému národu priznáva vlastný štát, ako aj presvedčenie, že všeobecný záujem štátu sa najlepšie dosiahne etnicky homogénnou populáciou, a nie rasovým miešaním. V roku 1977 bol sťažovateľ odsúdený na dvojtyždňový trest odňatia slobody za to, že vlastnil letáky určené na ďalšiu distribúciu a rozširovanie, ktoré podnecovali k rasovej diskriminácii. Komisia pre ľudské práva odmietla sťažnosť sťažovateľov ako neprijateľnú z dôvodu zneužitia práv v zmysle čl. 17 Dohovoru a v rozsudku uviedla: „Leták, ktorý viedol k odsúdeniu sťažovateľov, sa sám v nadpise obracia k „bielym holandským ľuďom“. Obsahuje vyhlásenia ako „väčšia časť našej populácie už dlhý čas má dosť prítomnosti stoviek tisíc Surinamčanov, Turkov a ďalších tzv. hosťujúcich pracovníkov v našej krajine, ktorí tu navyše vôbec nie sú potrební, a ... úrady sa musia iba postarať o to, aby títo nežiadúci cudzinci odišli z našej krajiny čo najskôr“. Leták ďalej oznamuje, že strana Nederlandse Volks Unie bude pokračovať v boji za bielych ľudí Holandska, kým nebude politická moc (určitých politických strán) a ostatných spriaznených strán definitívne zlomená. Hneď ako by Nederlandse Volk Unie získala v našej krajine politickú moc, zavedie poriadok a začne s : 1) odstránením Surinamčanov, Turkov a ďalších takzvaných „hosťujúcich pracovníkov“ z Holandska...“ Politika, ktorú zastávajú sťažovatelia, je inšpirovaná celkovým cieľom odstrániť všetkých nebielych ľudí z holandského územia, úplne bez ohľadu na ich štátnu príslušnosť, dobu pobytu, rodinné väzby a sociálne, ekonomické, humanitné alebo iné dôvody. Komisia zastáva názor, že táto politika jasne obsahuje prvky rasovej diskriminácie, ktorá je zakázaná podľa Dohovoru a iných medzinárodných zmlúv.“²⁶⁷

Zásahy do práva na slobodu prejavu sa pri uplatňovaní **konkrétnych** podmienok obmedzenia slobody prejavu vychádzajú z článku 10 ods. 2 Dohovoru o ochrane ľudských práv a základných slobôd posudzujú z týchto troch hľadísk, či „a) sú založené na základe zákona, b) sledujú legitímny cieľ, c) ich uplatnenie bolo nevyhnutné v demokratickej spoločnosti.“²⁶⁸ Čo teda znamená, že zásah do slobody prejavu by bol v rozpore s článkom 10 Dohovoru o ochrane ľudských práv a základných slobôd vtedy, ak by nebol upravený zákonom (prescribed by law), ak by nesledoval jeden alebo viaceré legitímne ciele uvedené v ods. 2 článku 10 predmetného dohovoru, a ak by nebol „nevyhnutný v demokratickej spoločnosti“ na dosiahnutie takéhoto cieľa alebo cieľov. Európsky súd pre ľudské práva v sťažnostiach namietajúcich porušenie článku 10 Dohovoru o ochrane ľudských práv a základných slobôd postupne preskúmava každé z týchto kritérií. Posudzovanie prvého kritéria priblížime na už zmieňovanom rozhodnutí Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, sťažnosť č. 29032/95. „Sťažovateľ tvrdil, že právny základ pre obmedzenie jeho slobody prejavu nebol dostatočne predvídateľný tak ako to vyžaduje judikatúra Súdu. Uviedol najmä, že slovenské právo, tak ako je vykladané a používané vnútroštátnymi súdmi, nedefinuje primerane urážku (defamáciu) v tom, že nerozlišuje medzi hodnotiacimi výrokmi a skutočnosťami a medzi verejnými činiteľmi a súkromnými osobami... Vláda nesúhlasila a trvala na tom, že zásah bol upravený zákonom, konkrétne § 11 a n. Občianskeho zákonníka... Pokiaľ sťažovateľ namieta, že nebolo možné dostatočne predvídať príslušný zákon, Súd pripomína, že jedna z požiadaviek vyplývajúca z pojmu „upravený zákonom“ je predvídateľnosť predmetného opatrenia. Normu nemožno považovať za „zákon“, pokiaľ nie je formulovaná dostatočne presne, aby umožnila občanovi regulovať jeho správanie: musí byť schopný – v prípade potreby s primeraným poučením – predvídať, v miere primeranej

²⁶⁷ Bližšie: Rozhodnutie Európskeho súdu pre ľudské práva vo veci Glimmerveen a Hagenbeek proti Holandsku zo dňa 11. októbra 1979, sťažnosť č. 8348/78 a 8406/78. Citované podľa: WILFLING, P. Nenávistné prejavy a extrémizmus v rozhodnutiach Európskeho súdu pre ľudské práva. Banská Bystrica: VIA IURIS, 2017. s. 20.

²⁶⁸ SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s r.o., 2006. s. 782.

okolnostiam, následky... Dôsledky nemusia byť predvídateľné s absolútnou istotou, skúsenosť ukazuje, že toto nie je dosiahnuteľné. Hoci je istota v oblasti práva vysoko želateľná, mohla by viesť k prehnanej tvrdosti a právo musí byť v stave držať krok s okolnosťami. Preto, mnohé zákony sú zjavne formulované v pojmoch, ktoré sú viac alebo menej široké, a ktorých interpretácia a použitie sú otázkou praxe... Namietaný zásah má právny základ, konkrétne § 11 a 13 ods. 1 Občianskeho zákonníka. Podľa posledného spomenutého ustanovenia, každá fyzická osoba môže požadovať, aby sa zastavilo neodôvodnené zasahovanie do jej osobných práv v zmysle § 11 Občianskeho zákonníka, aby sa odstránili dôsledky takéhoto zásahu, a aby jej bolo priznané primerané zadostučinenie. Je vecou vnútroštátnych súdov, aby posúdili osobitné sťažnosti o údajnom zásahu a rozhodli o primeranom zadostučinení. V súlade so zaužívanou praxou, žalobca v konaniach o ochranu osobnosti musí preukázať, že tvrdenia odporcu boli objektívne v stave poškodiť jeho práva podľa § 11 Občianskeho zákonníka, pričom ak obrana má mať úspech, od odporcu sa v takom prípade vyžaduje, aby predložil dôkazy dokazujúce pravdivosť jeho tvrdení. Súd s uspokojením konštatuje, že použitie týchto zákonných ustanovení a prax neprekročili vo veci sťažovateľa to, čo mohlo byť primerane predvídateľné v daných okolnostiach. Vzhľadom na to, zásah bol upravený zákonom v zmysle článku 10 ods. 2 Dohovoru.²⁶⁹

K podmienke zákonnosti Európsky súd pre ľudské práva konštantne judikuje, že slová "stanovuje zákon" použité v článku 10 ods. 2 Dohovoru znamenajú jednak to, že inkriminované opatrenie musí mať podklad vo vnútroštátnom práve, ale taktiež sa vzťahujú ku kvalite príslušného zákona. Vyžaduje sa, aby bol dotknutej osobe prístupný, teda aby táto osoba mohla predvídať dôsledky z predmetnej právnej úpravy. Z argumentácie súdu uplatnenej v rámci odôvodnenia súvisiaceho rozhodnutia Európskeho súdu pre ľudské práva vo veci Združenie Ekin proti Francúzsku zo dňa 17. júla 2001, sťažnosť č. 39288/98, čo sa zákonnosti zásahu do predmetného práva zo strany štátu týka, vyberáme „Otázka, zda je splněna první podmínka, není v daném případě sporná. Právním podkladem byl vskutku § 14 zákona z roku 1881, ve znění pozdějších úprav. Zbývá otázka, zda příslušná norma splňovala také požadavky přístupnosti a předvídatelnosti důsledků. Vláda je toho názoru, že podmínky přístupnosti a předvídatelnosti jsou zákonem z roku 1881, ve znění pozdějších úprav, splněny s přihlédnutím k jeho výkladu, jaký dává judikatura Státní rady. Soud připomíná, že podle jeho judikatury musí být pojem "zákon" chápán v "materiálním", a nikoli "formálním" smyslu. V důsledku toho pod něj zahrnuje veškeré psané právo, včetně podzákonných norem (viz zejm. De Wilde, Ooms a Versyp, 1971), jakož i judikaturu, jež ho vykládá (viz, mutatis mutandis, výše cit. Kruslin). Otázkou, která v daném případě vyvstává, je, zda v okamžiku, kdy byla vydána vyhláška ministra vnitra ze dne 29. 4. 1988, existovala ustálená, jasná a přesná judikatura francouzských soudů, která doplnila § 14 zákona z roku 1881 způsobem, jenž sdružení Ekin umožňoval přizpůsobit chování v záležitosti vydávání literárních děl. S ohledem na omezenou kontrolu vykonávanou v těchto záležitostech Státní radou v době inkriminovaných událostí se Soud přiklání spíše k tomu, že omezení kritizované sdružením Ekin nesplňovalo podmínku předvídatelnosti.“²⁷⁰

Približiac účel posudzovania druhej podmienky vyžadujúcej od zásahu do slobody prejavu legitímny cieľ, prinášame **výpočet podmienok umožňujúcich (legitimujúcich) zásah do**

²⁶⁹ Rozhodnutie Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, sťažnosť č. 29032/95.

²⁷⁰ Bližšie: Rozhodnutie Európskeho súdu pre ľudské práva vo veci Združenie Ekin proti Francúzsku zo dňa 17. júla 2001, sťažnosť č. 39288/98. Citované podľa: [http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/44FE015F41498F37C125844800395D07/\\$file/Sdru%C5%BEE n%C3%AD%20Ekin%20proti%20Francii_rozsudek.pdf?open&](http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/44FE015F41498F37C125844800395D07/$file/Sdru%C5%BEE n%C3%AD%20Ekin%20proti%20Francii_rozsudek.pdf?open&)

slobody prejavu vykonať, medzi ktoré, reflektujúc obsah článku 10 ods. 2 Dohovoru o ochrane ľudských práv slobôd, patrí: záujem národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, predchádzanie nepokojom alebo zločinnosti, ochrana zdravia alebo morálky, ochrana povesti alebo práv iných, zabránenie úniku dôverných informácií alebo zachovanie autority a nestrannosti súdnej moci. „Každý z týchto dôvodov, z ktorých aj jeden stačí na to, aby bola dodržaná podmienka legitímnosti cieľa je doplnený o imperatívnu podmienku, že zásah musí byť nevyhnutný v demokratickej spoločnosti...“,²⁷¹ pričom práve tretie kritérium je vo väčšine prípadov prejednávanych Európskym súdom pre ľudské práva rozhodujúcim pre určenie legitimacy obmedzenia slobody prejavu.

Na ilustráciu obhajoby obmedzenia slobody prejavu v záujme predchádzania nepokojom a ochrany práv iných uvádzame rozhodnutie Európskeho súdu pre ľudské práva vo veci *Féret proti Belgicku* zo 16. júla 2009, č. sťažnosti 15615/07, kedy sťažovateľ ako poslanec belgického parlamentu a predseda politickej strany Front National (Národný front) v Belgicku počas volebnej kampane bol za distribuovanie letákov obsahujúcich slogany ako napríklad: „*Postavte sa proti islamizácii Belgicka*“, „*Zastavte falošnú integračnú politiku*“ a „*Pošlite neeurópskych uchádzačov o prácu naspäť domov*“ odsúdený za podnecovanie k rasovej diskriminácii. Sťažovateľ bol odsúdený na verejné práce, rovnako mu bol uložený zákaz vykonávania poslaneckého mandátu po dobu 10 rokov. Sťažovateľ namietal, že týmto postupom štátnych orgánov došlo k porušeniu jeho práva na slobodu prejavu. Európsky súd pre ľudské práva v predmetnej veci rozhodol, že nedošlo k porušeniu článku 10 Dohovoru o ochrane základných práv a slobôd, nakoľko boli podľa záverov súdu komentáre sťažovateľa zjavne spôsobilé vyvolávať pocity nedôvery, odmietnutia alebo dokonca nenávisť voči cudzincom, najmä medzi menej informovanými občanmi. „*Jeho poslanstvo, vyslané vo volebnom kontexte, prinieslo zvýšenú rezonanciu a jasne predstavovalo podnecovanie rasovej nenávisť. Odsúdenie sťažovateľa bolo opodstatnené...*“.²⁷²

Pri posudzovaní toho, či sa jedná o prejav prípustný, požívajúci ochranu v zmysle článku 10 Dohovoru, chránený slobodou prejavu, je vhodné reflektovať rovnako **konceptiu „brániacej sa demokracie“**, ako označenie stavu demokracie, keď je ohrozená jej samotná podstata či dokonca existencia. K predmetnému pojmovému označeniu S. Cibík uvádza, „*Z hľadiska štátneho režimu však pojem brániaca sa demokracia ako samostatný pojem neexistuje. Štátny režim je jednou z troch zložiek formy štátu, pričom možno hovoriť o demokratickom alebo nedemokratickom štátnom režime. Takéto striktné delenie však môže pôsobiť problematicky práve pri koncepte brániacej sa demokracie, vo vedeckej a odbornej literatúre, predovšetkým politologickej, častejšie označovanom ako o koncepte militantnej demokracie. Je to tak z dôvodu, že kým sa demokracia snaží ochrániť samu seba, a teda obmedzuje činnosť, ktorá by mohla viesť k jej postupnému odstráneniu, mali by sa v zásade demokratické princípy vytratiť úplne.*“²⁷³ Uvedené nachádza vyjadrenie aj v už skloňovanom článku 17 Dohovoru o ochrane

²⁷¹ Uvedené potvrdzuje rovnako argumentácia Európskeho súdu pre ľudské práva uplatnená v už zmieňovanom rozhodnutí vo veci *Združenie Ekin proti Francúzsku* zo dňa 17. júla 2001, sťažnosť č. 39288/98. Porovnaj s: - SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s r.o., 2006. s. 784.

²⁷² Rozhodnutie Európskeho súdu pre ľudské práva vo veci *Féret proti Belgicku* zo 16. júla 2009, č. sťažnosti 15615/07. Citované podľa: Factsheet — Hate Speech. 2017. Štrasburg : Európsky súd pre ľudské práva, 2017. Dostupné na: [FS_Hate_speech_SLK \(coe.int\)](https://www.echr.europa.eu/en/cases-and-decisions/other/key-ecr-judgments/factsheet-hate-speech) Preklad: Kancelária zástupcu Slovenskej republiky pred Európskym súdom pre ľudské práva.

²⁷³ K pôvodu konceptu brániacej sa demokracie S. Cibík uvádza, že „*Koncept brániacej sa demokracie v dnešnom chápaní ako prvý formuloval Karl Loewenstein vo svojich článkoch *Militant Democracy and Fundamental Rights*, v ktorých upozornil na hrozbu nástupu fašizmu v Taliansku a národného socializmu v Nemecku. V týchto článkoch konštatoval, že úspech fašizmu a jeho techniky na získanie moci sa viaže na podmienky, ktoré sú vytvorené*

ľudských práv a základných slobôd. Ako v jednom zo súvisiacich rozhodnutí²⁷⁴ Európsky súd pre ľudské práva konštatuje, „všeobecným účelom čl. 17 je zabrániť skupinám vyznávajúcim totalitné ideológie, aby zneužívali princípy zakotvené v Dohovore vo svoj prospech“.²⁷⁵ P. Wilfling v tejto súvislosti uvádza, „Ak demokratický štát poskytne úplnú slobodu hnutiam a osobám, ktoré ho chcú zničiť, bude to viesť k skorému zničeniu a zániku demokratického štátu. Preto sa demokratický štát musí brániť proti svojim nepriateľom, ktorí ho chcú zničiť. V tom spočíva koncepcia tzv. brániacej sa demokracie („militant democracy“).“²⁷⁶ Reflexie konceptu brániacej sa demokracie možno rovnako nachádzať v rozhodovacej činnosti súdnych autorít demokratických krajín, pričom v našich podmienkach nachádzame relevantný odkaz k uvedenému v rozhodnutí ešte Ústavného súdu Českej a Slovenskej Federatívnej Republiky v znení „Bezpečnosť štátu a bezpečnosť občanov (verejná bezpečnosť) vyžadujú zabrániť podpore a propagácii hnutí, ktoré bezpečnosť štátu a občanov ohrozujú. Hnutia, ktoré preukázateľne smerujú k potlačeniu občianskych práv alebo k hlásaniu vymedzenej zášte, nech sú akokoľvek pomenované a zdôvodňované akýmikoľvek ideálmi alebo cieľmi, sú hnutiami, ktoré demokratický štát, jeho bezpečnosť a bezpečnosť jeho občanov ohrozujú. Ich postih je preto v plnom súlade s obmedzeniami, ktoré čl. 17 odst. 4 Listiny pripúšťa.“²⁷⁷

ZÁVER

V procese uplatňovania základných práv a slobôd, (osobnú slobodu nevynímajúc), platí vo všeobecnosti potreba nastolenia určitej rovnováhy pri ich realizácii. Ako konštantne judikuje Ústavný súd Slovenskej republiky „Všetky základné práva a slobody sa chránia len v takej miere a rozsahu, dokiaľ uplatnením jedného práva alebo slobody nedôjde k neprimeranému obmedzeniu, či dokonca popretiu iného práva alebo slobody. Rovnováha verejného a súkromného záujmu je dôležitým kritériom pre určovanie primeranosti obmedzenia každého základného práva a slobody.“²⁷⁸ Sloboda prejavu ako prerokovizita existencie každej pluralitnej spoločnosti budovanej na demokratických základoch s ohľadom na svoju relatívnu povahu predpokladá legitimitu obmedzenia za naplnenia kvalifikovaných okolností vyjadrených v znení vybraných ustanovení článkov garantujúcich slobodu prejavu na vnútroštátnej a nadnárodnej úrovni. S ohľadom na zložitosť posudzovania prípustnosti zásahov do slobody prejavu je práve judikatúra na tomto úseku prijímaná určitým návodom k jej náležitému zhodnoteniu, pričom je v každom prípade nutná interpretácia článkov garantujúcich slobodu prejavu v závislosti od konkrétnych osobitostí individuálne sledujúc povahu subjektov, obsahu a formy prejavu, ktorý sa šíri, nakoľko je dnes už nepopierateľné, že nie každý prejav je hodný ústavnoprávnej a medzinárodnoprávnej ochrany.

Skutočnosť, že extrémizmus ohrozuje základy a podstatu demokracie a nepriatelia demokracie využívajú na svoje aktivity nástroje a možnosti, ktoré im demokracia poskytuje, zakladá

demokratickými inštitúciami a na jeho schopnosť prispôbiť sa demokracii a využiť jej toleranciu na vlastné zničenie. Práve preto by mala demokracia pri snahe brániť sa voči svojmu vlastnému rozvratu a odstráneniu využívať aj mocenské prostriedky, a nielen demokratické prostriedky, ktoré sú zneužívané práve nepriateľmi demokracie. Vo svojej práci sa Loewenstein venoval napríklad jednotlivým legislatívnym opatreniam, ktoré by mohli zabrániť nepriateľom demokracie odstrániť tento režim a nastoliť režim nedemokratický.“ Bližšie: CIBIK, S. Vývoj konceptu brániacej sa demokracie v slovenskom právnom poriadku. In Právny obzor, 106, 2023, č. 3, s. 189 – 201.

²⁷⁴ napr. Rozhodnutie Európskeho súdu pre ľudské práva vo veci W.P. a ďalší proti Poľsku, č. sťažnosti 42264/98

²⁷⁵ Citované podľa: WILFLING, P. Nenávistné prejavy a extrémizmus v rozhodnutiach Európskeho súdu pre ľudské práva. Banská Bystrica: VIA IURIS, 2017. s. 14.

²⁷⁶ WILFLING, P. Nenávistné prejavy a extrémizmus v rozhodnutiach Európskeho súdu pre ľudské práva. Banská Bystrica: VIA IURIS, 2017. s. 13.

²⁷⁷ Nález Ústavného súdu Českej a Slovenskej Federatívnej Republiky, sp. zn. PL. ÚS 5/92

²⁷⁸ Nález Ústavného súdu Slovenskej republiky, sp. zn. PL. ÚS 7/96 zo dňa 27. februára 1997

v kontexte konceptu brániacej sa demokracie povinnosť obrany voči týmto pokusom o jej odstránenie. „*Obrana demokracie a jej základných atribútov by mala byť preto rovnako silná a efektívna ako odhodlanie jej nepriateľov zničiť ju.*“²⁷⁹ Ako vyplýva z koncepcie boja proti radikalizácii a extrémizmu do roku 2024 ako základného dokumentu definujúceho priority SR v oblasti predchádzania a boja proti radikalizácii, extrémizmu a s nimi spojenou protispoločenskou činnosťou ohrozujúcou základy demokratického právneho štátu, prijatej s cieľom „*podporiť rešpektovanie univerzálnych hodnôt a predchádzať vzniku predsudkov, stereotypov a nenávistných prejavov podmienených národnostnou, rasovou, etnickou, náboženskou alebo inou neznášanlivosťou, ako aj predchádzať vzniku a šíreniu postojov a aktivít smerujúcich k podpore a propagácii rasizmu, xenofóbie a ostatných foriem intolerancii v demokratickej spoločnosti,*“ priniesli uplynulé roky značný nárast online ako aj offline nenávistných prejavov mylne obhajovaných slobodou prejavu.

V texte príspevku analyzované rozhodnutia súdnych autorít spája apel sťažovateľov na ich slobodu slova, ktorý je ale sám o sebe nedostatočným spôsobom dokazovania čohokoľvek. „*Jednotlivec môže tvrdiť, že sloboda slova ho určitým spôsobom oslobodzuje od povinností a následkov spojených s jeho výrokmi. Môže sa brániť kritike svojich tvrdení tým, že obviňuje kritikov z narušovania slobody prejavu, prípadne argumentom o slobode prejavu vopred stavia svoje tvrdenia do pozície, ktorá kritiku nepripúšťa.*“²⁸⁰ Európska komisia v súčasnosti stále naliehavejšie poukazuje na potrebu efektívnejšieho boja proti ilegálnemu extrémistickému a nenávistnému obsahu prezentovanému online, „*nakoľko práve internet poskytuje priestor na uplatňovanie slobody prejavu, ktorú dokáže využívať aj extrémistická scéna okrem iného na tvorbu a šírenie zavádzajúcich informácií (dezinformácií) vrátane využívania falošných správ (z anglického jazyka „fake news“) či sprisahaneckých/konšpiračných „teórií*“.“²⁸¹ Rovnako prihodným je v tomto kontexte jedno z Murphyho pravidiel v znení „*Pravdivosť výrokov nemá nič spoločné s tým, ako vierohodne znejú a naopak*“. Uplatňovanie slobody prejavu nemôže a ani nie je bezbrehé a ako bolo úvodom príspevku konštatované je práve v súčasnosti sloboda prejavu čoraz častejšie obeťou zneužívania (nekorrektnou interpretáciou svojej povahy, poslania, účelu) na odstránenie demokratických princípov spoločnosti, zastrasovanie verejnosti, oslabovanie jej hodnotovej orientácie, či politickú destabilizáciu.

Zdroje

1. CIBIK, S. Vývoj konceptu brániacej sa demokracie v slovenskom právnom poriadku. In Právny obzor, 106, 2023. č. 3, s. 189 – 201. Dostupné na: <https://doi.org/10.31577/pravnyobzor.2023.3.02>
2. DOBROVIČOVÁ, G. JÁNOŠÍKOVÁ, M. Sloboda prejavu v Charte základných práv Európskej únie. In MAJERČÁK. T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 83 - 90. ISBN 978-80-8152-392-2.
3. CHRENŠŤ, J. NESVADBA, A. Právo Európskej únie. Bratislava: Akadémia Policajného zboru v Bratislave, 2020. 338 s. ISBN 978-80-8054-867-4.
4. KLÍMA, K. Svoboda projevu a její ústavní limitace. In MAJERČÁK. T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika

²⁷⁹ Koncepcia boja proti extrémizmu na roky 2015 – 2019. Dostupné na: [koncepcia extremizmus 2015-2019.pdf \(minv.sk\)](#)

²⁸⁰ Národný bezpečnostný úrad. Krátky slovník hybridných hrozieb. Dostupné na: [Krátky slovník hybridných hrozieb -NBU \(gov.sk\)](#)

²⁸¹ Koncepcia boja proti radikalizácii a extrémizmu do roku 2024. Dostupné na: [vlastny material.pdf](#)

- v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 91 - 100. ISBN 978-80-8152-392-2.
5. MACEJKOVÁ, I. Sloboda prejavu a súdna moc. In MAJERČÁK. T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 7 – 39. ISBN 978-80-8152-392-2.
 6. OROSZ, L. SVÁK, K. a kol. Ústava Slovenskej republiky. Komentár. Zväzok I. Bratislava: Wolters Kluwer SR s.r.o., 2021, s. 892. ISBN 978-80-571-0380-6.
 7. RYCHETSKÝ, P. Svoboda projevu a její ochrana před Ústavním soudem. In MAJERČÁK. T. Sloboda prejavu a jej limity - IV. ústavné dni Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016. s. 40 - 48. ISBN 978-80-8152-392-2.
 8. SVÁK, J. Ochrana ľudských práv (z pohľadu judikatúry a doktríny štrasburských orgánov ochrany práva). Žilina: Poradca podnikateľa, spol. s.r.o., 2006. 1116 s. ISBN 80-88931-51-7.
 9. WILFLING, P. Nenávistné prejavy a extrémizmus v rozhodnutiach Európskeho súdu pre ľudské práva. Banská Bystrica: VIA IURIS, 2017. 131 s. ISBN 978-80-89805-01-3.
 10. Všeobecná deklarácia ľudských práv
 11. Vyhláška ministra zahraničných vecí č. 120/1976 Zb. o Medzinárodnom pakte o občianskych a politických právach a Medzinárodnom pakte o hospodárskych, sociálnych a kultúrnych právach
 12. Dohovor o ochrane ľudských práv a základných slobôd
 13. Charta základných práv Európskej únie
 14. Rozhodnutie Európskeho súdu pre ľudské práva vo veci Féret proti Belgicku zo 16. júla 2009, č. sťažnosti 15615/07.
 15. Rozhodnutie Európskeho súdu pre ľudské práva vo veci W.P. a ďalší proti Poľsku, č. sťažnosti 42264/98.
 16. Rozhodnutie Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, sťažnosť č. 29032/95.
 17. Rozhodnutie Európskeho súdu pre ľudské práva vo veci Združenie Ekin proti Francúzsku zo dňa 17. júla 2001, sťažnosť č. 39288/98.
 18. Rozhodnutie Európskeho súdu pre ľudské práva vo veci Feldek proti Slovenskej republike zo dňa 12. júla 2001, sťažnosť č. 29032/95.
 19. Rozhodnutie Európskeho súdu pre ľudské práva vo veci Glimmerveen a Hagenbeek proti Holandsku zo dňa 11. októbra 1979, sťažnosť č. 8348/78 a 8406/78.
 20. Nález Ústavného súdu SR, sp. zn. II. ÚS 152/08 zo dňa 15. decembra 2009.
 21. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 174/17 zo dňa 4. januára 2018.
 22. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 152/08 zo dňa 15. decembra 2009.
 23. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 326/09 zo dňa 4. marca 2010.
 24. Nález Ústavného súdu Slovenskej republiky, sp. zn. II. ÚS 439/2016 zo dňa 27. októbra 2016.
 25. Nález Ústavného súdu Slovenskej republiky, sp. zn. PL. ÚS 7/96 zo dňa 27. februára 1997.
 26. Nález Ústavného súdu Českej a Slovenskej Federatívnej Republiky, sp. zn. PL. ÚS 5/92.
 27. Nález Ústavného súdu Českej republiky sp. zn. I. ÚS 823/11 zo dňa 6. marca 2012.
 28. Agentúra Európskej únie pre základné práva, 2020. Uplatňovanie Charty základných práv Európskej únie v práve a pri tvorbe politík na vnútroštátnej úrovni. Usmernenie. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2020. s. 12. Dostupné na internete: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-charter-guidance_sk.pdf

29. Factsheet — Hate Speech. 2017. Štrasburg : Európsky súd pre ľudské práva, 2017. Dostupné na: FS_Hate_speech_SLK (coe.int) Preklad: Kancelária zástupcu Slovenskej republiky pred Európskym súdom pre Slovenskú republiku.
30. Konceptia boja proti radikalizácii a extrémizmu do roku 2024. Dostupné na: vlastny material.pdf
31. Konceptia boja proti extrémizmu na roky 2015 – 2019. Dostupné na: konceptia extremizmus 2015-2019.pdf (minv.sk)
32. Národný bezpečnostný úrad. Krátky slovník hybridných hrozieb. Dostupné na: Krátky slovník hybridných hrozieb -NBU (gov.sk)
33. <https://www.epi.sk/rozhodnutie-sudu/Rekvenyi-proti-Madarsku-Politicka-angazovanost-policajtov.html>
34. [http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/44FE015F41498F37C125844800395D07/\\$file/Sdru%C5%BEen%C3%AD%20Ekin%20proti%20Francii_rozsudek.pdf?open&](http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/44FE015F41498F37C125844800395D07/$file/Sdru%C5%BEen%C3%AD%20Ekin%20proti%20Francii_rozsudek.pdf?open&)

ZVYŠOVANIE ÚROVNE VZDELÁVANIA V OBLASTI HYBRIDNÝCH HROZIEB

prof. Ing. Bohuslava Mihalčová, PhD. & PhD., EUR ING

Ekonomická univerzita v Bratislave, Podnikovohospodárska fakulta so sídlom v Košiciach, Tajovského 13, 040 01 Košice, e-mail: bohuslava.mihalcova@euba.sk

Abstrakt: Zmeny v bezpečnostnom prostredí s nízkou pravdepodobnosťou predpovedania kladú vysoké nároky nielen na analytikov a odborníkov v oblasti bezpečnosti, ale aj na zvyšovanie vedomostí a úrovne povedomia verejnosti o tejto problematike. V predložennom príspevku charakterizujeme pojmy z oblasti hybridných hrozieb, venujeme sa histórii dezinformácií a hoaxov a diskutujeme o záveroch našich analýz súčasného stavu inštitucionálneho vzdelávania o bezpečnostných otázkach na vybraných univerzitách.

Kľúčové slová: hybridné hrozby, bezpečnosť, vzdelávanie.

ÚVOD

Pojem bezpečnosť existuje už od staroveku. Vtedy sa však nepovažovala za vec verejného záujmu ale za niečo nevyhnutné, resp. za vôľu bohov. Moderné predstavy o bezpečnosti sa rozvinuli až v 19. storočí vďaka priemyselnej revolúcii, keď veľký počet nehôd v továrňach vzbudil záujem ľudí o prevenciu. Dnes je záujem o bezpečnosť globálny a je centrom pozornosti mnohých vládnych a súkromných agentúr na miestnej, národnej a medzinárodnej úrovni. (Britannica, 2023) Bezpečnosť je stav sociálneho, prírodného, technického, technologického alebo iného systému, ktorý za špecifických vnútorných a vonkajších podmienok umožňuje plnenie určených funkcií a ich rozvoj v záujme človeka a spoločnosti.

Vo všeobecnosti ho možno charakterizovať aj ako stav bez reálnej hrozby nebezpečenstva, prípadne stav protikladný k nebezpečenstvu. (Horáček, J. et al., (2006)

Nie všetko prebieha vo svete podľa plánu. Ustálený stav niektorých entít je často spochybnený. Tu nachádza svoje miesto bezpečnostná veda. Bezpečnosť sa tak stáva procesom alebo prostriedkom pre ochranu pred vonkajšími alebo vnútornými chybami, nebezpečenstvami, stratami, zločincami a inými jednotlivcami alebo akciami, ktoré ohrozujú, bránia alebo ničia „ustálený stav“ organizácie a zbavujú ju účelu, na ktorý je určená. (Oakes, 2009). S pojmom bezpečnosť je úzko spätý aj pojem hybridné hrozby.

Ide o činnosť, ktorú vykonávajú tak štátne, ako aj neštátne subjekty za účelom poškodzovať ovplyvňovaním rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.

1. POJMOLÓGIA A HISTORICKÉ VÝCHODISKÁ

Hybridné aktivity môžu fungovať aj bez formálneho vyhlásenia vojny. Medzi nástroje hybridných aktivít patria napr. dezinformácie, kybernetická a priemyselná špionáž, zneužívanie procedúr, ale aj podvrtné činnosti, či nekonvenčné metódy. Súčasťou hybridného spôsobu boja môžu byť masívne dezinformačné kampane a využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie priaznivcov. Tieto hrozby sa dotýkajú celého spektra aktivít, či už v politike, polícii, práve, ale aj v ekonomike, diplomacii, kyber priestoru a inde.

Ako sme už spomenuli, dezinformácie, predstavujú neoddeliteľnú súčasť hybridných hrozieb. Podľa NBS, pojem **dezinformácia** zatiaľ nebol v Slovenskej republike kodifikovaný. Väčšinou

sa preberajú definície uvádzané v odborných publikáciách či oficiálnych európskych dokumentoch. Dezinformácie sa tak stávajú súčasťou celého informačných operácií, ktoré sú známe pod niekoľkými pojmami týkajúcimi sa hybridných hrozieb, ako sú napr. už spomínané dezinformácie, hoaxy, propaganda, falošné správy, dokonca paródia, či satira. Povedzme si stručne základné definície týchto pojmov.

Dezinformácie sú nepravdivé informácie, ktoré sú vytvorené a zdieľané s cieľom úmyselne poškodiť. S týmto pojmom súvisia aj falošné správy („fake news“) a pojem propaganda.

Falošné správy sú spravodajstvom, ktoré nie je pravdivé. Môžu byť vo forme dezinformácií alebo nedostatku dezinformácií. Silverman (2016) dokonca tvrdí, že ide o spravodajstvo tvorené za účelom finančného zisku, pretože, ak by absentoval motív financií, išlo by len o propagandu. Výskumy v tejto súvislosti poukazujú na fakt, že až dve tretiny občanov EÚ uvádzajú, že sa s falošnými správami stretávajú aspoň raz týždenne (Flash Eurobarometer 464, 2018). Viac ako 80 % občanov EÚ tvrdí, že falošné správy vnímajú ako problém ich krajín a demokracie vo všeobecnosti. Polovica občanov EÚ vo veku 15 – 30 rokov tvrdí, že potrebujú kritické myslenie a informačné zručnosti, ktoré im pomôžu bojovať proti falošným správam a extrémizmu v spoločnosti (Flash Eurobarometer 455, 2018). Ivančík a Müllerová, 2022 uvádzajú, že „**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“.

Zopár príkladov na hybridné hrozby z histórie

Ramzes II.

Ramesse II. (Ramzes II.), nazývaný **Veľký** bol faraónom starovekého Egypta. Podľa análov sa narodil okolo roku 1303 pred n.l.p. faraónovi Sethimu I. a kráľovnej Tuje. Najznámejšia z Ramesseových manželiek bola Nefertari. Napriek tomu, že ide o najslávnejšieho faraóna vtedajších dôb, bol vystatovačný a veľmi márnomyseľný. Šíril dezinformácie a propagandu, preháňal svoje činy a vymýšľal si niektoré víťazstvá v boji. Spomeňme napr. bitku pri Kádeši z roku 1274 p.n.l., kde po jej skončení prostredníctvom papyrusových zvitkov rozšíril po celom Egypte, ako v tejto bitke vyhral proti Chetitom. Opak však bol pravdou. Faraón Ramesse II. musel uzatvoriť s Chetitským kráľom Muvatalli II. Aj keď neskôr obe strany označovali bitku za svoje víťazstvo, Ramesseho vojaci utrpeli veľké straty a Ramesse tak nebol schopný obsadiť žiadne nové územie. Ich nepriateľstvo skončilo až uzatvorením mierovej zmluvy 1258 p.n.l. s novým kráľom Chetitov. (Spracované podľa https://sk.wikipedia.org/wiki/Ramesse_II.)

Sun Tzu

Na využívanie dezinformácií v hybridnej vojne upozorňoval aj známy čínsky mysliteľ Sun Tzu v *Umení vojny*, keď napísal, že „*Skutočným tajomstvom je schopnosť zmiasť protivníka tak, že nie je schopný rozpoznať náš skutočný úmysel*“ (Sarvaš, 2021). Stovky rokov pred narodením Krista bolo v Číne obdobie známe ako vek bojujúcich štátov. Aby tieto štáty vyhrali, hľadali akýkoľvek spôsob, ako získať výhodu nad svojimi protivníkmi; vyhľadávaní boli najmä tí, ktorí majú znalosti o stratégii a vodcovstve. V tom čase povstal generál zo štátu Čchi známy ako Sun Tzu (približne 554 p.n.l.). Jeho kniha *Umenie vojny* sa stala dielom o stratégii v Číne. Podrobne opisuje kompletnú filozofiu, ako poraziť súpera. Sun Tzu zdôrazňuje umenie vojny bez boja, tzn. odporúča bojovníkom najprv stanoviť takú stratégiu, ktorá by bola obojstranne výhodná bez toho, aby „rinčali“ zbrane. Agresívne taktiky považuje za poslednú možnosť. Zdôrazňuje, že dlhé vojny spôsobujú zbytočné plytvanie zdrojov, ktoré je možné využiť pre rozvoj štátov a budovanie ich infraštruktúr. Vo svojej knihe *Umenie vojny* poukazuje na dezinformáciu, ako

na prostriedok hybridných hrozieb, kde uvádza, že *skutočným tajomstvom je schopnosť vojvodu zmiast' protivníka tak, že nebude schopný rozpoznať náš skutočný úmysel.*

Ptolemaios I. Sótér

Ptolemaios I. Sotér (367–283 pr. n. l.) bol macedonským generálom panovníka Alexandra Veľkého, jeho dôverným priateľom od detstva a neskôr zakladateľom ptolemaiovskej dynastie. Dokonca v r. 305 pr. n. l. prijal titul egyptského faraóna (spracované podľa wikipédie). Po krajine rozšíril dezinformáciu, že je Alexandrovým nevlastným bratom, aby si po Alexandrovej smrti zabezpečil miesto na tróne.

Octavius Augustus

Augustus (63 pr. n. l. – 19. n.l., vl. menom Gaius Octavius, neskôr Gaius Iulius Caesar Octavius bol prasynovcom Gaia Iulia Caesara, ktorý si ho obľúbil a vyhlásil neskôr za svojho dediča. To bolo neskôr jablko sváru medzi ním a Marcusom Antóniom. (spracované podľa wikipédia). Bol prvým a zároveň najväčším rímskym cisárom. Napriek množstvu kladných vlastností a rozmachu ríše, bol zároveň veľmi schopným manipulátorom. Zradu, korupciu a manipuláciu využíval vo svoj prospech. Známy je napríklad Augustov hoax a Kleopatrinej samovraždy, ktorá bola partnerkou Marcusa Aurélia.

Napoleon Bonaparte I. (1769 – 1821)

Charizmatický vodca a výborný francúzsky generál a stratég Napoleon Bonaparte bol jednou z najvýznamnejších postáv svetových dejín, napriek svojim pádom. Dá sa považovať jeho výška 168 cm za trpasličí vzhľad? Porovnaním jeho výšky s výškou iných politikov, napr. Josifa Visarionoviča Stalina – 163 cm, či Nicolasa Sarkozyho, resp. Silvia Berlusconiho – 165 cm môžeme povedať že nie. Napriek tomu ho nepriateľská anglická propaganda považovala za arogantného trpaslíka s ešte menším vzhľadom.

Mnoho ďalších príkladov propagandy a hoaxov nachádzame v tzv. nacistickej propagande, ktorá stála za rozpútaním 2. svetovej vojny.

Vráťme sa teraz opäť do súčasnosti. Koncom 20. storočia začali prevládať optimistické scenáre ďalšieho vývoja ľudstva aj napriek niekoľkým regionálnym a lokálnym konfliktom vo svete. Ekonomický rast mnohých krajín bol na vzostupe. Koniec prvého desaťročia však so sebou prináša hypotekárne, finančné a ekonomické krízy. Znalosti o ekonomickom raste a cykle však už boli na takej úrovni, že umožnili postupne konsolidovať ekonomickú situáciu. Žiaľ, ozbrojené konflikty národného a medzinárodného rozmeru neprestali. Boli to krajiny Afriky, Blízkeho východu, ale aj Afganistanu, Sýrie či bývalých republík Sovietskeho zväzu. Najmä v týchto republikách sa Ruská federácia postavila ako mierotvorná sila a po prevzatí moci Putinom v Rusku dosadila do čela týchto krajín svojich prívržencov. Ľudstvo potrápili nielen ozbrojené konflikty. Koncom dvadsiatych rokov 21. storočia vážne zasiahla epidémia COVID-19. Vysoko nákazlivý, rýchlo sa šíriaci vírus s častými mutáciami zabil v rokoch 2020 a 2021 približne 14,9 milióna ľudí. Svetová zdravotnícka organizácia (WHO) odhaduje, že pandémia svojim obetiam zničila celkovo 336,8 milióna ľudských životov vrátane post covidových ochorení. WHO vypočítala, že v priemere sa život jednej obete covidu skrátil zhruba o 22 rokov. Pandémia mala podľa štatistík organizácie negatívny vplyv aj na celosvetový boj s nádorovými a prenosnými chorobami, pretože akútne operácie, očkovanie a zdravotnícke služby boli pozastavené, nedostatočné, prípadne fungovali s nedostatkom personálu a materiálneho zdravotníckeho vybavenia. Nielen COVID-19 spôsobil pokles očkovania proti osýpkam, tetanu a iným ochoreniam. Príčinou boli aj proti vakcinačné hnutia. Spomedzi chorôb sa častejšie vyskytovala malária a tuberkulóza. (RTV.sk, 2023) Ekonomické, sociálne a politické dôsledky

spomínaných chorôb sú zatiaľ nekvantifikované. V celkovo komplikovanej situácii počas spomínaných rokov začala Ruská federácia 24. februára 2022 bezprecedentnú vojnu proti Ukrajine, Kremlom dlhodobo označovanú ako „Špeciálnu vojenskú operáciu“. Najväčšie obete tejto agresie sú na Ukrajine, no výrazné negatívne dôsledky dopadajú na väčšinu krajín sveta. Vyššie uvedené udalosti sa stali základom pre vznik asymetrického hybridu, energetických hrozieb, surovín a nedostatku potravín. Skúmanie celého spektra problémov je dôležité predovšetkým z hľadiska bezpečnostnej situácie. Bezpečnosť štátu je na poprednej úrovni celkovej bezpečnosti, pretože bez nej by neexistovala ekonomická ani osobná bezpečnosť, ani žiadna iná bezpečnosť.

2. INŠTITUCIONÁLNE VZDELÁVANIE V OBLASTI HYBRIDNÝCH HROZIEB

Rovnako ako na Slovensku, tak aj v Českej a Poľskej republike, ale aj v ďalších krajinách Európskej únie sa problematikou bezpečnosti zaoberá viacero inštitúcií, ktoré pripravujú a vykonávajú všeobecne záväzné nariadenia. Vzhľadom na vyššiu právnu silu nariadení Európskej komisie a Rady Európy tieto navzájom súvisia a rozdiely medzi nimi sú minimálne. Východiskom pre tvorbu ústavných zákonov, nariadení, uznesení, vyhlášok, smerníc a usmernení stanovujúcich dôsledné hodnotenie situácie a realizáciu potrebných opatrení v záujme bezpečnosti štátov sú Ústavy jednotlivých krajín. Napríklad v Slovenskej republike existujú zákony ako:

- Ústavný zákon o bezpečnosti Slovenskej republiky
- Zákon o fungovaní Bezpečnostnej rady SR v čase mieru
- Bezpečnostná stratégia SR
- Obranná stratégia SR
- Branný zákon
- Zákon o riadení štátu v krízových situáciách mimo vojnového a vojnového stavu
- Zákon o hospodárskej mobilizácii. (Úrad vlády Slovenskej republiky, 2022)

Komplexné bezpečnostné riešenie si žiada čoraz viac odborníkov rôzneho zamerania a vzdelávacie procesy, ktoré by pripravovali jedincov pre pochopenie bezpečnosti na každej úrovni a prevenciu proti hybridným vojnám. Ide tak o stredné školy, ktoré si pozývajú do vyučovacieho procesu odborníkov z praxe, ale najmä vysoké školy, v programoch ktorých čoraz viac dominujú otázky bezpečnosti.

Ak v poslednom desaťročí 20. storočia existovali najmä štátne vysoké školy, ktoré pripravovali vojakov, policajtov a odborníkov pre prácu v rezorte obrany. Do vzdelávania v oblasti bezpečnosti a ochrany v 21. storočí sa postupne zapája viacero verejných aj súkromných vysokých škôl v Európskej únii. Úlohou odborníkov je porovnávať parametre a študijné programy v oblasti bezpečnostných štúdií v záujme zjednotenia úsilia v bezpečnostných štúdiách. Viaceré študijné odbory sa tak po roku 2019 zjednotili do novo zaradených odborov „Bezpečnosť a bezpečnostné vedy“ a študijný odbor bol zaradený do skupiny „Bezpečnostné vedy, obrana a vojenstvo“. Vysoké školy, ktoré sa snažia ponúkať študijné programy pre študentov v tomto odbore, musia získať kladný výsledok úspešnej akreditácie na študijný program tohto odboru. Univerzity môžu poskytovať akreditované programy na prvom, druhom a treťom stupni štúdia. Študijné programy prvého stupňa a študijné programy druhého stupňa nie je možné spájať do jedného celku. Interdisciplinárne štúdium je prípustné. Hlavné témy vedomostného jadra študijného odboru bezpečnostná veda sú koncipované tak, aby absolventi získali poznatky umožňujúce komplexné hodnotenie, projektovanie a riadenie rizík a ohrození bezpečnosti osôb, materiálnych a nehmotných hodnôt a životného prostredia, technologických rizík, priemyselnej bezpečnosti a vykonávania preventívnych opatrení a efektívneho a účinného

riešenia protispoločenskej a trestnej činnosti, vznikajúcich bezpečnostných incidentov, mimoriadnych udalostí a krízových situácií. (PORTALVS.SK, 2019). Medzi nosné témy nosných poznatkov študijného odboru patrí ochrana osôb, majetku a informácií, bezpečnostný manažment, projektový manažment, civilná bezpečnosť a civilná ochrana, manažment rizík a krízový manažment, pohotovostná služba, súdne inžinierstvo, teória policajných vied, kriminalistika a kriminalistika, bezpečnostná služba verejnej správy, bezpečnosť a ochrana zdravia pri práci, požiarna ochrana, technologická bezpečnosť. Medzi hlavné témy jadra študijného odboru patria poznatky z relevantných právnych oblastí, najmä z oblasti trestného, policajného a správneho práva.

Pri analýze študijných odborov a študijných programov susedných krajín sme zistili ich podobnosť. To dovoľuje vysloviť záver, že úsilie o zjednotenie v bezpečnostných štúdiách je úspešné. Podobné črty štúdiá boli identifikované na Slovensku, kde univerzity ponúkajú 55 študijných programov v odbore: Bezpečnostné vedy, obrana a vojenstvo v týchto programoch, a to napr. na Policajnej akadémii v Bratislave, Vysokej škole bezpečnostného manažmentu v Košiciach, na Fakulte bezpečnostného manažmentu v Žiline, na Materiálovo technologickej fakulte STU so sídlom v Trnave, na Akadémii ozbrojených síl generála Milana Rastislava Štefánika, na Technickej univerzite vo Zvolene, ale aj ďalších fakultách. Podľa údajov webu VysokeSkoly.cz ponúka bezpečnostné štúdium v Českej republike 23 škôl a fakúlt. (VYSOKESKOLY.CZ, 2023). Podobne je to aj Maďarsku a Poľsku.

Od počiatku skúmania problematiky hybridných hrozieb a prevencii proti nim prostredníctvom vyučovacieho procesu sme sa orientovali na vyváženosť z hľadiska:

- súčasných poznatkov o hybridných hrozbách doma a v zahraničí
- aktuálnych cieľov v oblasti predchádzania a potenciálneho eliminovania hybridných hrozieb,
- voľby dostupných metód a postupov nadobudnutia východiskových podmienok na vypracovanie koncepcie vzdelávania v inštitucionálnych podmienkach SR,
- postupnej kolekcie analýzy a syntézy nadobudnutých výsledkov čiastkových a výsledných riešení s dôrazom na odporúčania v oblasti samotnej koncepcie.

Absorbovali sme poznatky o významnej asymetrickosti hybridných hrozieb a ich ďalekosiahlych dôsledkov na život jednotlivcov a fungovanie spoločnosti.

Zastrašovanie, vyhrážanie, manipulovanie, sebaopoškodenie, šikanovanie, obchod s ľudskými orgánmi a ľuďmi, ale aj krádež identity sa znásobujú. Popri tom sa hybridné hrozby implementovali do početných ozbrojených konfliktov v rôznych regiónoch sveta. V záujme získania východísk na riešenie danej problematiky sme vykonali rešerš študijných programov a vyučujúcu problematiku bezpečnosti s akcentom aj na hybridné hrozby. Koncentrovali sme sa na podklady o študijných plánoch a uskutočnili sme konzultačné stretnutia s osobnosťami takýchto škôl.

Ako príklad výskumu uvádzame významnú súkromnú vysokú školu v Poľskej republike, ktorá bola podrobená hĺbkovému skúmaniu. Jedná sa o Krakovskú akadémiu Andrzeja Frycza Modrzewskiego. Poľská republika je naším severným susedom. Jej popredné relevantné vládne, vedecké a vysokoškolské inštitúcie sa venujú problematike hybridných hrozieb s vysokou intenzitou. V ostatných desaťročiach je svet a jednotlivé krajiny vystavené nesymetrickým nie len ohrozeniam, ale žiaľ i vojnám. Kybernetický priestor priniesol popri mnohých pozitívnych vkladoch do rozvoja spoločenstva aj kybernetické hrozby a pomedzi nimi dominujúce informačné hrozby. Pomedzi informačnými hrozbami sa aj tam významne presadzujú hybridné

hrozby. Dôraz sme položili na študijné programy prvého a druhého stupňa vysokoškolského štúdia na Krakovskej akadémii Andrzeja Frycza Modrzewskiego (ang. Andrzej Frycz Modrzewski Krakow University). Univerzita je plnohodnotná, akreditovaná, neverejná (súkromná) vysoká škola. Aktuálne má škola 9283 študentov, ktorí sa vzdelávajú v anglickom alebo poľskom jazyku. Pomedzi 7 fakultami sú aj Fakulta práva, administrácie a medzinárodných vzťahov (Faculty of Law, Administration and International Relations) a Fakulta bezpečnostných vied (Faculty of Security Studies). Podľa vyjadrenia kompetentných zahraničných partnerov sa tieto programy stali základom na vytvorenie programov ďalších vysokých škôl. Fakulta bezpečnostných vied, vôbec ako prvá v Poľsku vypracovala a dala akreditovať študijný odbor národná bezpečnosť. Vďaka tomuto odboru sú študenti vzdelávaní v programoch:

- ✓ národná bezpečnosť - prvý stupeň / bakalárske štúdium (6 semestrov)
- ✓ vnútorná bezpečnosť - bakalárske / bakalárske štúdium (6 semestrov)
- ✓ národná bezpečnosť - druhý stupeň / magisterské štúdium (3 semestre).

Fakulta bezpečnostných vied organizuje aj doktorandské semináre, pretože získala oprávnenie udeľovať akademický titul doktor (dr) na Slovensku philosophie doctor PhD. vo vednej oblasti spoločenských vied v odbore bezpečnostné vedy. Popri uvedených nosných štúdiách fakulta ponúka aj postgraduálne štúdium a kurzy. Aktuálne na fakulte pôsobí 16 prednášajúcich riadnych a univerzitných profesorov a rad cvičiacich učiteľov. Medzi prednášajúcimi profesormi sú aj bývalí najvyšší velitelia ozbrojených síl i polície, ktorí dosiahli generálske hodnosti a následne aj tretí stupeň vysokoškolského vzdelania a viacerí sa habilitovali. Obohacujú tak teoretické základy a samotný obsah študijných programov vypracované profesormi, ktorí svoju kariéru budovali predovšetkým na akademickej pôde.

Konkrétne v Poľsku sa problematikou bezpečnosti zaoberá najmenej 2 desiatky vysokých škôl, a to tak štátnych, verejných, ale aj súkromných. Štúdium vytypovaných syllabov predmetov týkajúcich sa hybridných hrozieb potvrdzuje významnosť riešenej problematiky v rámci uvedenej oblasti skúmania, ktorá má pre spoločnosti veľký význam.

3. DISKUSIA

Súbor bezpečnostných učebných osnov predstavuje jeden pohľad na bezpečnostné vzdelávanie. Ak si uvedomíme, že bakalárske štúdium trvá 3-4 roky a štúdium na druhom stupni spravidla ďalšie 2 roky, je mimoriadne dôležité každoročne upravovať vyučovaný materiál tak, aby pokrýval najdôležitejšie zmeny v dynamicky sa rozvíjajúcom a zložitom bezpečnostnom prostredí. Starostlivým štúdiom celého spektra študijných odborov/vysokoškolských programov sme zistili, že prakticky každý z nich obsahuje aj otázky súvisiace s bezpečnostným prostredím. Ovplyvňujú bezpečnú funkciu strojov, zariadení, dopravných prostriedkov, systémov, prevádzok, laboratórií z pohľadu odborných zamestnancov, ale aj manažmentu s dôrazom na predchádzanie hrozbám, elimináciu rizík spojených so stále vyššou mierou autonómie logistiky. a následne aj výrobné, riadiace a často aj rozhodovacie procesy. Z tohto dôvodu by mali vysoké školy poskytovať študentom najnovšie poznatky v problematike bezpečnostných aspektov súčasného vývoja spoločnosti vo všetkých sférach života.

Osobitnú pozornosť treba venovať **príprave budúcich riadiacich funkcionárov** a príslušníkov obranných a bezpečnostných síl a zložiek na zvládanie čoraz závažnejších výziev a hrozieb. Bude to možné len vtedy, ak sa kvalitne rozvinie **príprava príslušníkov ozbrojených síl na vysokých vojenských školách a policajtov na policajných akadémiách**. Potrebný počet špecialistov v armáde a policajnom zbore z odborov, ktoré neuskutočňujú vojenské a policajné vysoké školy, je potrebné **prípraviť a zaškoliť v účelových kurzoch po**

ich prijatí do štátnej služby na plnenie úloh v náročných odbornostiach, bez ktorých nemožno zlepšiť obranný a bezpečnostný systém.

ZOPÁR SLOV NA ZÁVER

Vzhľadom na výsledky analýzy bezpečnostných študijných programov na univerzitách v susedných krajinách môžeme konštatovať, že vo všeobecnosti predstavujú celé spektrum bezpečnostných oblastí. Oproti stavu pred 30 rokmi ich ponúkajú desiatky fakúlt týchto univerzít. V rámci celého spektra študijných programov bez zanedbávania dôležitosti každého z nich je preukázateľné, že programy štátnych vysokých škôl v oblasti obrany a bezpečnosti sú rozvíjané s cieľom pripraviť personál, ktorý má prvoradý význam pre oblasť obrany a bezpečnosti. Periodická akreditácia všetkých študijných programov pripravujúcich odborníkov v širokom spektre bezpečnostného vzdelávania prostredníctvom nezávislých akreditačných agentúr pre vysoké školy v susedných krajinách je nástrojom na posilnenie úsilia vysokých škôl o skvalitnenie ponúkaných študijných programov.

Zdroje

1. BRITANNICA. Safety. The Editors of Encyclopaedia Britannica 2023. Online [Cit.: 2023-10-13]. Dostupné na: <https://www.britannica.com/topic/safety-condition>
2. HORÁČEK, J. et al. (2006), Terminologický slovník krízového manažmentu, Žilina:
3. Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, s. 5, ISBN 8088829755 Flash Eurobarometer 464 , 2018
4. IVANČÍK, R., MULLEROVÁ, J. (2022). Dezinformácie ako hybridná hrozba šírená prostredníctvom sociálnych sietí. Dostupné na: https://www.akademiapz.sk/sites/default/files/202209/32022/EDITED_003%20IVAN%204%208C%20C3%20DK%20C%20M%20C3%209CLLEROV%20C3%2081%20Dezinform%20C3%20A1cie%20ako%20hybridn%20C3%20A1%20hrozba%20C5%20A1%20C3%20ADren%20C3%20A1%20soci%20C3%20A1lnymi%20sie%20C5%20A5ami.pdf. Online [Cit.: 2023-10-12].
5. NBS.Dostupné na:(<https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html>). Online [Cit.: 2023-10-12].
6. OAKES, Ch. G. (2009). Blue Ember Technologies, LLC."Safety versus Security in Fire Protection Planning Archived 2012-03-13 at the Wayback Machine,"The American Institute of Architects: Knowledge Communities, May 2009. Online [Cit.: 2023-10-12]. Dostupné od júna 22, 2011.
7. PORTALVS.SK 2019. Bezpečnostné vedy Online [Cit.: 2023-10-11]. Dostupné na: <https://www.portalvs.sk/sk/studijne-odbory/zobrazit/bezpecnostne-vedy>
8. Ramesse II. Dostupné na: https://sk.wikipedia.org/wiki/Ramesse_II. Online [Cit.: 2023-10-13].
9. RTV.SK 2023. Pandémia skrátila životy obetí covidu o 22 rokov, tvrdí WHO. Mala negatívny dosah aj na boj proti iným ochoreniam. Online [Cit. 2023-10-14] According to ČTK from 19. 5. 2023. Dostupné na: <https://spravy.rtvsk.sk/2023/05/pandemia-skratila-zivoty-obeti-covidu-o-22-rokov-tvrdi-who/>
10. SARVAŠ, Š. (2021) Dezinformácie: cesta do pekiel nefunkčnej spoločnosti. Dostupné na: <https://infosecurity.sk/dezinfo/dezinformacie-cesta-do-pekiel-nefunkcnej-spolocnosti/>. Online [Cit.: 2023-10-13].
11. SILVERMAN, C. (2016). This analysis shows how viral fake election news stories outperformed real news on Facebook. In Buzzfeed, 2016.

12. ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY. 2022. Základné dokumenty riešiace bezpečnosť Slovenskej republiky. Online [Cit. 2023-10-12] Dostupné na: <https://www.vlada.gov.sk/zakladne-dokumenty-riesiace-bezpecnost-slovenskej-republiky/>
13. VYSOKESKOLY.CZ 2023. Bezpečnostní studia. Online [Cit.: 2023-10-11] Dostupné na: <https://www.vysokeskoly.cz/v/pravo-a-verejna-sprava/bezpecnostni-studia/>
14. [https://cs.wikipedia.org/wiki/Ptolemaios_I. S%C3%B3t%C3%A9r](https://cs.wikipedia.org/wiki/Ptolemaios_I._S%C3%B3t%C3%A9r). Online [Cit.: 2023-10-15]
15. https://sk.wikipedia.org/wiki/Octavius_Augustus. Online [Cit.: 2023-10-15]

MIMORIADNE UDALOSTI A ICH ZNEUŽITIE PRE HYBRIDNÉ PÔSOBNIE NA VEREJNÚ SPRÁVU SR

doc. Ing. Michal Orinčák, PhD.

Akadémia Policajného zboru v Bratislave, Katedra verejnej správy a krízového manažmentu; Sklabinská 1, 835 17 Bratislava 35; michal.orincak@minv.sk, michal.orincak@akademiapz.sk

Abstrakt: Príspevok rieši problematiku možného zneužitia mimoriadnych udalostí, ktoré môžu vzniknúť na území Slovenska pre hybridné pôsobenie na verejnú správu SR. V prvej časti príspevku je uvedená aktuálna štatistika početnosti vzniku vybraných mimoriadnych udalostí v SR. Druhá časť príspevku rozoberá možnosti zneužitia vybraných mimoriadnych udalostí pre hybridné pôsobenie v SR. Záverečná časť príspevku pojednáva o aktuálnom hoaxe o zhoršení radiačnej situácie na území SR.

Kľúčové slová: mimoriadne udalosti, hybridné pôsobenie, hoax, verejná správa.

ÚVOD

V krízovom riadení a civilnej ochrane obyvateľstva sa používajú nasledujúce tri dôležité pojmy, a to: *mimoriadna udalosť* (emergency event), *mimoriadna situácia* (extraordinary situation) a *krízová situácia* (crisis situation). Tieto základné pojmy predstavujú dôležitú súčasť novodobého problému možného zneužitia mimoriadnych udalostí pre hybridné pôsobenie na verejnú správu SR s cieľom narušiť rozhodovacie procesy v štátnom aparáte a tým vytvoriť priestor pre vznik chaosu a nedôvery k štátnej správe a samospráve.

Mimoriadna udalosť je závažná, časovo ťažko predvídateľná a priestorovo ohraničená príhoda spôsobená vplyvom živelnej pohromy, technickej alebo technologickej havárie, prevádzkovej poruchy prípadne úmyselného konania človeka, ktorá vyvolala narušenie stability systému, alebo prebiehajúcich dejov a činností, ohrozuje životy a zdravie osôb, hmotné a kultúrne statky, či životné prostredie. Je definovaná v zákone č. 42/1994 Z. z. Národnej rady Slovenskej republiky o civilnej ochrane obyvateľstva v znení neskorších predpisov.

Mimoriadna situácia je časovo a priestorovo determinované ohrozenie života, zdravia, majetku a životného prostredia, hospodárstva štátu, ako aj orgánov verejnej správy vyvolané pôsobením negatívnych následkov mimoriadnych udalostí, ktoré si vyžaduje použitie postupov, nástrojov, zdrojov, síl a prostriedkov krízového riadenia. Taktiež je definovaná v zákone č. 42/1994 Z. z. Národnej rady Slovenskej republiky o civilnej ochrane obyvateľstva v znení neskorších predpisov.

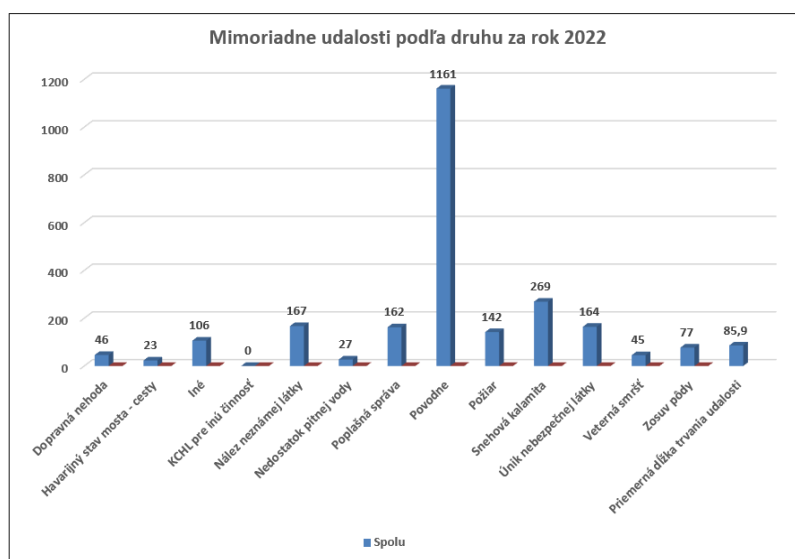
Krízová situácia je obdobie, počas ktorého je bezprostredne ohrozená alebo narušená bezpečnosť štátu a ústavné orgány môžu po splnení podmienok ustanovených v zákone NR SR č. 227/2002 Z. z. Ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu na jej riešenie vypovedať vojnu, vyhlásiť vojnový stav alebo výnimočný stav, alebo núdzový stav.

Krízovou situáciou mimo času vojny a vojnového stavu je obdobie, počas ktorého je bezprostredne ohrozená alebo narušená bezpečnosť štátu a ústavné orgány môžu po splnení podmienok ustanovených v ústavnom zákone (zákon NR SR č. 227/2002 Z. z. Ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu), alebo v osobitnom zákone (zákon NR SR č. 387/2002 Z. z. o riadení štátu v krízových situáciách

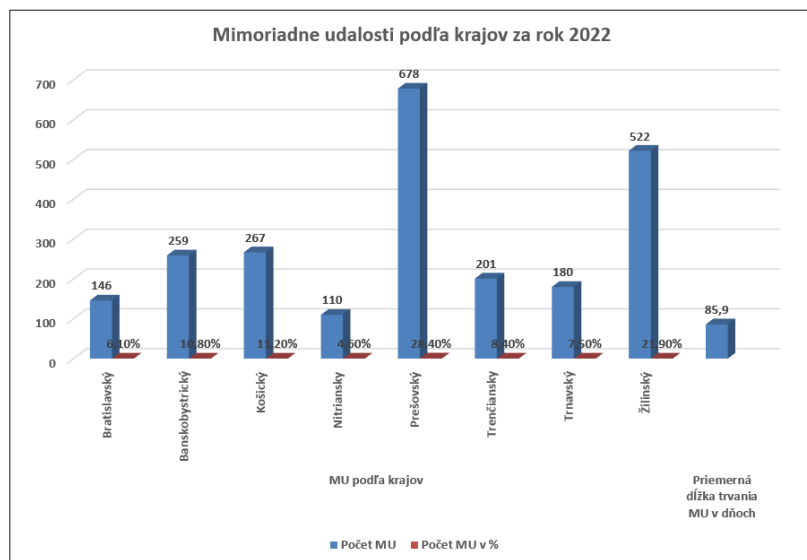
mimo času vojny a vojnového stavu) na jej riešenie vyhlásiť výnimočný stav, núdzový stav, alebo mimoriadnu situáciu.

1. ŠTATISTIKA POČETNOSTI VZNIKU VYBRATÝCH MIMORIADNYCH UDALOSTÍ V SR

Absolútna početnosť vybratých druhov mimoriadnych udalostí z celkového počtu vzniknutých mimoriadnych udalostí v SR za rok 2022 a ich významnosť v súvislosti so zaradením k hybridnej hrozbe je uvedená na nasledujúcich obr. 1, obr.2 a tab. 1, kde je uvedená aj priemerná dĺžka trvania mimoriadnej udalosti v dňoch.



Obr.1 Mimoriadne udalosti podľa druhu za rok 2022 (Zdroj: Štatistiky mimoriadnych udalostí za rok 2021-2022, Ministerstvo vnútra Slovenskej republiky, Sekcia krízového riadenia, Centrálné monitorovacie a riadiace stredisko, Bratislava, 2022)



Obr.2 Mimoriadne udalosti podľa krajov za rok 2022 (Zdroj: Štatistiky mimoriadnych udalostí za rok 2021-2022, Ministerstvo vnútra Slovenskej republiky, Sekcia krízového riadenia, Centrálné monitorovacie a riadiace stredisko, Bratislava, 2022)

	Spolu	MU podľa krajov v SR								Priemerná dĺžka trvania MU v dňoch
		Bratislavský	Banskobystrický	Košický	Nitriansky	Prešovský	Trenčiansky	Trnavský	Žilinský	
Počet MU	2389	146	259	267	110	678	201	180	522	85,9
Dopravná nehoda	46	6	3	5	2	11	7	7	5	0,0
Havarijný stav mosta - cesty	23	0	4	3	0	7	0	3	6	75,7
Iné	106	5	14	20	3	40	5	9	8	395,4
KCHL pre inú činnosť	0	0	0	0	0	0	0	0	0	261,2
Nález neznámej látky	167	27	12	26	32	24	16	25	5	0,0
Nedostatok pitnej vody	27	0	10	8	0	5	3	0	1	94,2
Poplašná správa	162	53	6	29	2	17	11	19	1	94,9
Povodne	1161	0	163	117	49	437	125	54	216	19,8
Požiar	142	30	13	33	12	20	7	17	10	74,2
Snehová kalamita	269	0	3	6	0	21	1	0	238	72,3
Únik nebezpečnej látky	164	22	18	13	9	37	17	45	3	5,8
Veterná smršť	45	1	4	4	1	29	0	0	6	79,9
Zosuv pôdy	77	2	9	3	0	30	9	1	23	11,2
Priemerná dĺžka trvania MU v dňoch	85,9	101,3	38,5	88,0	8,7	126,1	26,3	149,3	83,7	

Tab.1 Mimoriadne udalosti podľa krajov za rok 2022 a priemerná dĺžka ich trvania v dňoch (Zdroj: Štatistiky mimoriadnych udalostí za rok 2021-2022, Ministerstvo vnútra Slovenskej republiky, Sekcia krízového riadenia, Centrálné monitorovacie a riadiace stredisko, Bratislava, 2022)

V roku 2021 bolo na číslo tiesňového volania 112 na celom Slovensku prijatých 905 918 volaní. Z celkového počtu volaní na 112 bolo až 27 % volaní tzv. neidentifikovaných, to znamená, že tieto volania boli uskutočnené z mobilných zariadení bez SIM-karty alebo z oblastí, kde volajúci nemá signál svojej domovskej mobilnej siete. V roku 2021 bolo na 112 prijatých 19 904 SMS a 3 074 volaní e-Call [6].

V roku 2022 bolo na číslo tiesňového volania 112 na celom Slovensku prijatých 903 910 volaní. Z minuloročných volaní bolo oprávnených 617 546. To znamená, že takmer jedna tretina volaní (takmer 32 %) bola bez reálnej udalosti. Z celkového počtu volaní na 112 bolo 209 946 volaní tzv. neidentifikovaných. To znamená, že sa uskutočnili z mobilných zariadení bez vloženej SIM karty alebo z oblastí, kde volajúci nemal signál svojej domovskej mobilnej siete. V roku 2022 bolo na 112 prijatých 16 701 SMS a 4 002 volaní e-Call ako aj 787 automatických volaní e-Call pri nárazoch motorového vozidla [6].

2. ZNEUŽITIE MIMORIADNYCH UDALOSTÍ PRE HYBRIDNÉ PÔSOBENIE V SR

Vybraté mimoriadne udalosti SR, ktoré môžu byť zneužitú pre hybridné pôsobenie na verejnú správu (podľa zákona č. 42/1994 Z. z. Národnej rady Slovenskej republiky o civilnej ochrane obyvateľstva v znení neskorších predpisov a vyhlášky č. 523/2006 Z. z. Ministerstva vnútra Slovenskej republiky o podrobnostiach na zabezpečenie záchranných prác a organizovania jednotiek civilnej ochrany):

- a) Živelná pohroma.
- b) Havária.
- c) Katastrofa.
- d) Teroristický útok.
- e) Ohrozenie verejného zdravia II. stupňa.
- f) Hromadný prílev cudzincov na územie Slovenskej republiky.

Medzi ďalší možný druh mimoriadnej udalosti v SR, ktorý bude potrebné doplniť do zákona č. 42/1994 Z. z. Národnej rady Slovenskej republiky o civilnej ochrane obyvateľstva v znení neskorších predpisov môžeme v súčasnosti zaradiť aj tzv. **ohrozenie informačného systému CO** (hlásna služba a informačná služba CO) ako konkrétny negatívny účinok hybridného pôsobenia cudzieho aktéra (agresora) na verejnú správu SR.

Z hľadiska významnosti potenciálu možného zneužitia jednotlivých druhov mimoriadnych udalostí pre hybridné pôsobenie na verejnú správu v SR ich môžeme z pohľadu civilnej ochrany obyvateľstva a záchranných služieb rozdeliť na tzv. *primárne - hlavné* a *sekundárne – periférne (okrajové)* mimoriadne udalosti ako napríklad:

1. Živelné pohromy:

- 1.1 povodne a záplavy** (*primárne z hľadiska hybridných hrozieb*),
- 1.2 krupobitia (*periférne z hľadiska hybridných hrozieb*),
- 1.3 následky víchrice (*periférne z hľadiska hybridných hrozieb*),
- 1.4 zosuvy pôdy** (*primárne z hľadiska hybridných hrozieb*),
- 1.5 snehové kalamity a lavíny (*periférne z hľadiska hybridných hrozieb*),
- 1.6 rozsiahle námrazy (*periférne z hľadiska hybridných hrozieb*),
- 1.7 zemetrasenia** (*primárne z hľadiska hybridných hrozieb*),

2. Havárie:

2.1 požiare a výbuchy (primárne z hľadiska hybridných hrozieb),

2.2 úniky nebezpečných látok, prípravkov a odpadov, ropných produktov s následným kontaminovaním územia, ovzdušia, vodných tokov, zdrojov pitnej vody a podzemných vôd (primárne z hľadiska hybridných hrozieb),

2.3 poškodenie vedení rozvodných sietí, ich zariadení a diaľkovodov (primárne z hľadiska hybridných hrozieb),

3. Katastrofy:

3.1 veľké letecké, železničné, lodné a cestné nehody spojené s požiarmi prípadne s únikom nebezpečných látok (primárne z hľadiska hybridných hrozieb),

3.2 havárie jadrových zariadení (primárne z hľadiska hybridných hrozieb),

3.3 porušenie vodných stavieb (primárne z hľadiska hybridných hrozieb),

4. Teroristický útok: ako priamy tzv. „fyzický“ útok na verejnú správu a obyvateľstvo. Z hľadiska možného zneužitia pre hybridné pôsobenie na verejnú správu v SR ho môžeme zaradiť medzi tzv. *primárnu mimoriadnu udalosť*.

5. Ohrozenie verejného zdravia II. stupňa: z hľadiska možného zneužitia pre hybridné pôsobenie na verejnú správu v SR ho môžeme zaradiť medzi tzv. *sekundárnu mimoriadnu udalosť*.

6. Hromadný prílev cudzincov na územie Slovenskej republiky: z hľadiska možného zneužitia pre hybridné pôsobenie na verejnú správu v SR ho môžeme zaradiť medzi tzv. *primárnu mimoriadnu udalosť*.

Podrobnejšia charakteristika jednotlivých druhov mimoriadnych udalostí z hľadiska ich možného potenciálu zneužitia pre hybridné pôsobenie na verejnú správu v SR z pohľadu civilnej ochrany obyvateľstva a záchranných služieb je uvedená v záverečnej časti kapitoly tohto príspevku. V súčasnosti sú na Slovensku pripravené tzv. „**Plány typových činností a štandardizované operačné postupy**“, ktoré sú zamerané na hybridné hrozby, kde ich hlavným nástrojom pôsobenia sú tzv. *informačné operácie*, ktoré sú zámerne cielené na vytváranie chaosu a paniky v štáte.

Z hľadiska zneužitia mimoriadnych udalostí ako reálneho nástroja pre hybridné pôsobenie na subjekty a zamestnancov verejnej správy je potrebné vykonať tzv. *koncepciu a stratégiu boja proti hybridným hrozbám* ako základ pre účinnú prevenciu a represiu voči hybridným hrozbám. Taktiež je nutné určiť pre základné rozdelenie mimoriadnych udalostí v SR tzv. *primárnu a sekundárnu kategóriu* potencijnálneho zdroja hybridnej hrozby. Zároveň stanoviť tzv. *kritické prvky* jednotlivých druhov mimoriadnych udalostí, podľa ktorých budú zaradené do primárnej alebo sekundárnej kategórie. Na základe tejto kategorizácie je možné realizovať strategický plán prevencie a represie voči hybridným hrozbám vo verejnej správe.

Živelné pohromy ako tzv. sekundárna kategória, okrem vybratých druhov mimoriadnych udalostí (povodne, záplavy, zosuvy pôvody, zemetrasenia) najmä prostredníctvom narušenia tzv. kybernetickej bezpečnosti IZS a verejnej správy. Veľmi ťažké až nemožné plánovanie a riadenie samotného priebehu živelnej pohromy pre potreby naplnenia cieľov hybridnej hrozby – vojny. Viaceré druhy živelných pohrôm predstavujú tzv. lokálnu mimoriadnu udalosť vyskytujúcu sa na úrovni obcí, miest prípadne okresu.

Havárie ako tzv. primárna kategória, ktorých základným zdrojom sú najmä závažné priemyselné havárie, poškodenie vedení rozvodných sietí, ich zariadení, diaľkovodov a vybrané katastrofy, ktoré spôsobia naakumulovanie negatívnych účinkov na zasiahnutom území veľkého rozsahu (veľký počet mŕtvych a zranených, značné materiálne a environmentálne škody na rozsiahlom území a pod.) a tým umožnia ľahšiu aplikáciu nevojenských prostriedkov a činností za účelom dosiahnutia cieľa bez priameho vojnového konfliktu.

Teroristický útok ako tzv. primárna kategória pre ľahší prienik nežiadúcich *tzv. závadových činností* s cieľom narušiť a destabilizovať systém vybraného územia štátu (najmä orientácia na prihraničné regióny štátu) bez priameho použitia vojenských prostriedkov cudzieho štátu. Výrazne ľahšie plánovanie a riadenie samotného priebehu teroristického útoku pre potreby naplnenia cieľov hybridnej hrozby – vojny. Ide predovšetkým o priamy *tzv. „fyzický“* útok na verejnú správu a obyvateľstvo.

Ohrozenie verejného zdravia II. stupňa (epidémia, pandémia) ako tzv. sekundárna kategória – a to z dôvodu veľmi ťažkého riadenia a plánovania samotného priebehu epidémie (pandémie) a výskyt viacerých neočakávaných komplikácií. Možnosť využiť ochromené riadenie a činnosť štátu na narušenie a destabilizáciu postihnutej krajiny. Riešenie a prevencia spadá najmä do oblasti zdravotníctva a ochrany verejného zdravia (prierezová oblasť v rámci pôsobnosti ministerstiev).

Hromadný prílev cudzincov na územie SR ako tzv. primárna kategória - ľahší prienik nežiadúcich *tzv. závadových činností* najmä do oblasti zasahovania zahraničných aktérov do vnútorného chodu štátu a *polovojenských a extrémistických skupín* s cieľom narušiť najmä vnútornú bezpečnosť štátu. Je to *tzv. prierezová oblasť* v rámci pôsobnosti viacerých ministerstiev.

3. HOAX O ZHORŠENÍ RADIAČNEJ SITUÁCIE NA ÚZEMÍ SR

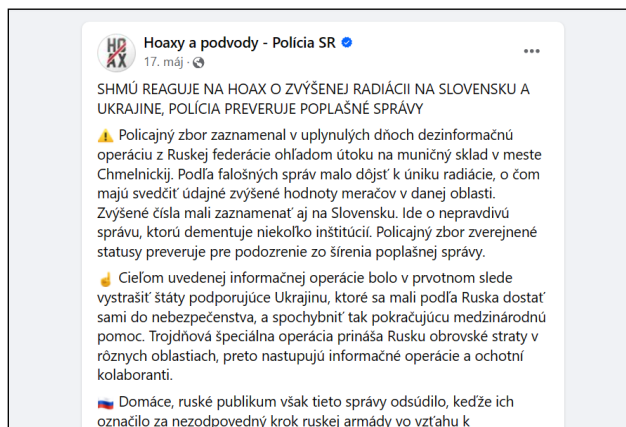
V rámci sociálnych sietí sa dňa 18.05.2023 vyskytol *hoax o zhoršení radiačnej situácie na území SR*, ktorí priamo súvisel s aktuálnym ozbrojeným konfliktom na území Ukrajiny. Samotný *hoax (zámerne vytvorený falošný obsah, ktorý sa snaží zmanipulovať a úmyselne oklamať príjemcu, aby ho preposielať a ďalej masovo šíril)* obsahoval nasledovné informácie [11], [12]:

- ruská armáda zničila muničný sklad v meste Chmelnickij,
- následkom útoku má byť únik radiácie tam uschovanej munície,
- dôkazom majú byť zvýšené hodnoty miestnych meračov,
- na Slovensku sa šíria hoaxy o tom, že táto radiácia prichádza na naše územie,
- slovenské hoaxy spomínajú zvýšené namerané hodnoty meračov,
- šíria sa návody o tom, ako sa vyhnúť žiareniu (napr. sprchovať sa 2-4-krát do dňa),
- tento hoax sa šíri masovo na Facebooku a cez WhatsApp.

Hlavným cieľom tohto konkrétneho hoaxu bolo najmä [11], [12]:

- vystrašiť obyvateľov Ukrajiny a okolitých krajín, spôsobiť chaos a paniku,
- vystrašiť susedné krajiny, spôsobiť chaos a paniku,
- znížiť podporu Ukrajiny zo strany spojencov,
- znížiť dôveryhodnosť ukrajinských orgánov v očiach spojencov.

Poľské štátne orgány zdôraznili, že prechodne zvýšené hodnoty prirodzeného radiačného pozadia nie sú ničím nezvyčajným a vyskytujú sa pravidelne, napr. počas zrážok. Cez európsky kontinent vrátane Poľska aktuálne prechádza atmosférický front, ktorý prináša aj výdatné zrážky. Práve tie podľa poľských odborníkov spôsobili tzv. „skoky“ v grafoch, na ktoré sa odvolávajú dezinformátori a autori hoaxy.



Obr.3 Hoax o zhoršení radiačnej situácie na území SR – facebook hoax PZ (Zdroj: <https://www.facebook.com/hoaxPZ/posts/1453250442169485/>, 2023)

Stanovisko Úradu verejného zdravotníctva Slovenskej republiky bolo k tomuto hoaxu nasledovné [11], [12]:

- Radiačná situácia na území Slovenskej republiky je aktuálne štandardná.
- Neboli zaznamenané žiadne odchýlky od bežne meraných hodnôt dávkových príkonov žiarenia gama. Na akékoľvek zmeny a prítomnosť umelých rádionuklidov v ovzduší sme pripravení promptne reagovať.
- K dnešnému dňu (18. mája 2023 k 12:00) neboli zaznamenané žiadne významné odchýlky sledovaných hodnôt dávkových príkonov na území Slovenskej republiky: <https://www.shmu.sk/sk/?page=1&id=radioaktivita>.

Stanovisko Slovenského hydrometeorologického ústavu (SHMÚ) bolo k tomuto hoaxu nasledovné [11], [12]:

- Na ukrajinských a slovenských staniciach neboli zaznamenané významne zvýšené hodnoty radiačie.
- Všetky dáta sú transparentné a verejnosť ich môže sledovať na stránke: <https://remap.jrc.ec.europa.eu/Advanced.aspx>.
- Celé stanovisko Slovenského hydrometeorologického ústavu (SHMÚ) k uvedenému hoaxu o zhoršení radiačnej situácie na území SR je uvedené na facebookovej stránke SHMÚ (<https://www.facebook.com/shmu.sk/posts/9373544316052391>).



Obr.4 Online mapy Spoločného výskumného centra EÚ - monitorovanie rádioaktivity životného prostredia (Zdroj: <https://remap.jrc.ec.europa.eu/Advanced.aspx>, 2023)

Okamžitým a jednotným postupom všetkých štátnych orgánov a inštitúcií Slovenskej republiky bol tento hoax *o zhoršení radiačnej situácie* obyvateľom SR vysvetlený a jeho ďalšie šírenie postupne behom týždňa zaniklo. Tento konkrétny prípad hoaxu ukázal v praxi, aká je veľmi dôležitá včasná a koordinovaná reakcia štátu na tieto typy dezinformácií a falošných správ, ktoré vznikajú na sociálnych sieťach.

ZÁVER

Hlavným cieľom tohto príspevku bolo objasniť a vysvetliť z pohľadu civilnej ochrany obyvateľstva a záchranných služieb, aké mimoriadne udalosti môžu vzniknúť na území Slovenska a zároveň akým spôsobom môžu byť zneužívané na hybridné pôsobenie cudzieho aktéra (agresora) na verejnú správu SR.

Hybridné nástroje a ich pôsobenie na verejnú správu prebieha zvyčajne skryté, a to najmä v čase mieru, kedy dochádza k narušeniu rozhodovacích procesov v štátnom aparáte, čím sa vytvára priestor pre vznik chaosu a nedôvery k štátnej správe a samospráve. Výsledkom takejto kumulácie až eskalácie hybridných útokov môže byť vyhlásenie krízového stavu – napr. vyhlásenie výnimočného stavu pre určité územie SR z dôvodu občianskych nepokojov alebo vyhlásenie núdzového stavu v dôsledku živeľnej pohromy, havárie, katastrofy, pandémie pričom môže dôjsť aj k tzv. ohrozeniu až znefunkčneniu informačného systému CO (hlásnej služby a informačnej služby CO).

Nástroj hybridného pôsobenia môže byť aj tzv. útok DDoS, čo v praxi znamená preťaženie informačného systému akýmkoľvek spôsobom a tým narušiť plynulý priebeh poskytovanej služby – napr. tiesňové linky záchranných zložiek, e-call a pod. Najčastejšie prostredníctvom tzv. zombie alebo bot systémom - botnet ako sieť botov.

Zdroje

1. Zákon NR SR č. 227/2002 Z. z. Ústavný zákon o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu.
2. Zákon NR SR č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov.
3. Zákon NR SR č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov.

4. Zákon NR SR č. 129/2002 Z. z. o integrovanom záchrannom systéme v znení neskorších predpisov.
5. Vyhláška č. 523/2006 Z. z. Ministerstva vnútra Slovenskej republiky o podrobnostiach na zabezpečenie záchranných prác a organizovania jednotiek civilnej ochrany.
6. Štatistiky mimoriadnych udalostí za rok 2021-2022, Ministerstvo vnútra Slovenskej republiky, Sekcia krízového riadenia, Centrálné monitorovacie a riadiace stredisko, Bratislava, 2022.
7. Koncepcia bezpečnostného systému SR, MV SR, Bratislava, 2022.
8. Koncepcia pre boj SR proti hybridným hrozbám, ÚVSR, Bratislava, 2018.
9. KLINGOVÁ, K. 2019. Hybridné hrozby na Slovensku. Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach GLOBSEC. Bratislava (<https://www.globsec.org/wpcontent/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnychhrozieb-web.pdf>).
10. LUŽÁK, J., KLAČKO, L. 2019. Audit bezpečnostného systému Slovenskej republiky v kontexte hybridných hrozieb, GLOBSEC. Bratislava (<https://www.globsec.org/what-we-do/publications/audit-bezpecnostneho-systemu-slovenskej-republiky-v-kontexte-hybridnych>).
11. Hoax o zhoršení radiačnej situácie na území SR – facebook hoax PZ. [online]. [cit. 27.06.2023]. Dostupné na: https://www.facebook.com/policiaslovakia/posts/6746457755384389?ref=embed_post.
12. Hoax o zhoršení radiačnej situácie na území SR – facebook hoax PZ. [online]. [cit. 27.06.2023]. <https://www.facebook.com/hoaxPZ/posts/1453250442169485>.
13. Online mapy Spoločného výskumného centra EÚ - monitorovanie rádioaktivity životného prostredia [online]. [cit. 29.10.2023]. <https://remap.jrc.ec.europa.eu/Advanced.aspx>.

DEZINFORMÁCIE V KRAJINÁCH EÚ

prof. RNDr. Beáta Stehlíková, CSc., prof. Ing. Antonín Korauš, PhD.

Slovenská technická univerzita, Vazovova 5, 812 43, Bratislava, beata.stehlikova@stuba.sk,
Akadémia Policajného zboru, Sklabinská 1, 835 17 Bratislava; antonin.koraus@akademiapz.sk

Abstrakt: Dezinformácie sú jedným z nástrojov hybridnej hrozby pre verejnú správu. Predstavujú nepresný alebo zmanipulovaný informačný obsah, ktorý sa šíri zámerné. Cieľom príspevku je zistiť, ktoré ukazovatele MLI najviac ovplyvňujú jeho výslednú hodnotu. Inými slovami, ktoré indikátory MLI najviac napomáhajú kriticky hodnotiť informácie z médií. Podľa typu použitých údajov ide o kvantitatívnu výskumnú štúdiu. Pomocou algoritmu supervised machine learning - random forest identifikujeme faktory, ktoré najviac ovplyvňujú schopnosť kriticky hodnotiť informácie z médií a tak znížiť účinnosť dezinformačných kampaní. Najdôležitejšie sa ukázali výsledky PISA v oblasti čitateľskej gramotnosti, v oblasti matematiky a Sloboda tlače. Úspešnosť dezinformačných kampaní môžeme znížiť aj zlepšením vzdelávacieho procesu a zvýšením slobody tlače.

Kľúčové slová: dezinformácie, index mediálnej gramotnosti MLI, random forest.

ÚVOD

Duberry (2022) uvádza, že dezinformácie sú zámerné, často strategické v tom zmysle, že sa zameriavajú na konkrétne demografické skupiny a vkladajú falošné príbehy a koordinované úsilie zo skutočných a falošných účtov s cieľom zaujať publikum (Bennett & Livingston, 2018). Facebook prijal nasledujúcu operačnú definíciu dezinformácií. Dezinformácie sú nepresný alebo zmanipulovaný informačný obsah, ktorý sa šíri zámerné. Môže to zahŕňať falošné správy alebo môže zahŕňať jemnejšie metódy, ako sú operácie pod falošnou vlajkou, poskytovanie nepresných citátov alebo príbehov nevinným sprostredkovateľom alebo vedomé rozširovanie zaujatých alebo zavádzajúcich informácií. Dezinformácie sa líšia od dezinformácií, čo je neúmyselné alebo neúmyselné šírenie nepresných informácií bez zlého úmyslu (Weedon, Nuland a Stamos, 2017, s. 5).

Dezinformačné kampane sú súčasť veľkej stratégie na spochybnenie spoločného chápania výhod, relevantnosti a odolnosti európskych liberálnych demokracií, a tým prispieť ku globálnej geopolitickej hre o moc (Duberry, 2022). Dezinformácie sú jedným z nástrojov hybridnej hrozby aj pre verejnú správu.

Dezinformačné taktiky na narušenie dôvery v demokratické inštitúcie. Krasodonski-Jones, Smith, Jones, Judson a Miller (2019) identifikovali niekoľko strategických cieľov.

Prvý strategický cieľ, ktorý identifikovali Krasodonski-Jones et al. (2019), sa týka ovplyvnenia prepojenia medzi politickými osobnosťami a občanmi, presnejšie toho, ako občania vnímajú politické vedenie. Zámerom je zvýšiť podporu verejnosti pre politickú stranu alebo politického lídra. Tieto stratégie sa vykonávajú prostredníctvom dvoch hlavných taktík - falošné zosilnenie (boty a falošné účty) a podvodný obsah (Wardle, 2017).

Druhý strategický cieľ dezinformačných kampaní, ktorý identifikovali Krasodonski-Jones et al. (2019), sa týka politickej participácie a konkrétnejšie zníženia účasti občanov na volebných procesoch s cieľom podporiť politických oponentov. Cieľom je podkopanie dôvery v demokraciu a volebné procesy, podporu polarizácie a potlačenie hlasov.

Tretím strategickým cieľom dezinformačných kampaní, ako ho identifikovali Krasodonski et al. (2019), je zamerať sa na integritu samotného komunikačného prostredia. Cieľom je narušiť komunikačné kanály a vytvoriť digitálne prostredie, ktorému občania už nedôverujú. Pokiaľ ide o taktiku, zahŕňa to zneužívanie moderovania obsahu, hranie na obe strany na podporu hnevu a zmätku, vymýšľanie a rozširovanie strašidelných príbehov, šokujúci obsah.

Posledný strategický cieľ dezinformačných kampaní, ktorý identifikovali Krasodonski et al. (2019), sa týka kvality informácií, ku ktorým majú občania prístup. Cieľom je vytvoriť informačný chaos, kde už nie je jasné, čo je pravda a čo nepravda. V dôsledku toho fakty strácajú svoju hodnotu. Stratégie spojené s týmto cieľom sa zameriavajú na podkopávanie dôvery v médiá a digitálne médiá a ovplyvňovanie vytváraného obsahu.

S nárastom falošných správ a dezinformačných kampaní sa kontrola faktov stala jedným z cieľov online platforiem, tlače a západných vlád. ReportersLab identifikoval asi 160 organizácií na overovanie faktov na svete (Lim, 2019). V Európe niektoré organizácie ako EUFactcheck.eu³ alebo EUvsDisinfo.eu⁴ sú hlavnými príkladmi úsilia tlače a inštitúcií EÚ bojovať proti šíreniu falošných správ (Duberry, 2022).

Perspektívy umelej inteligencie a analýzy údajov sú tiež veľmi dôležité, možno ich použiť na detekciu slov, alebo slovné vzory, ktoré by mohli naznačovať klamlivé príbehy“ (Iasiello 2017, 51-63).

Cieľom príspevku je zistiť, ktoré ukazovatele MLI najviac ovplyvňujú jeho výslednú hodnotu. Inými slovami, ktoré indikátory MLI najviac napomáhajú kriticky hodnotiť informácie z médií.

1. MATERIÁL A METÓDY

Dezinformačné kampane a propaganda patria medzi aktivity zamerané na ovplyvňovanie, destabilizáciu a rušenie výkonu verejnej správy. Odolnosť voči dezinformáciám môžeme merať pomocou Indexu mediálnej gramotnosti Media Literacy Index (MLI). Je to nástroj, ktorý sa používa na meranie schopnosti jednotlivcov porozumieť a kriticky hodnotiť informácie z médií. Je to dôležitá zručnosť v dnešnom svete, kde sme vystavení obrovskému množstvu informácií z rôznych zdrojov. Media Literacy Index, ktorý vyvinula organizácia European Policies Initiative (EuPI). Tento index meria mediálnu gramotnosť na základe kritérií, vrátane schopnosti jednotlivcov: rozpoznať rôzne druhy médií a ich účely, porozumieť tomu, ako média fungujú a aké sú ich predpoklady, kriticky hodnotiť informácie z médií, identifikovať zaujatosť a chyby v médiách, vytvoriť si vlastný názor na základe informácií z médií, porozumieť tomu, ako média ovplyvňujú spoločnosť, porozumieť tomu, ako sa môžeme angažovať v médiách, porozumieť tomu, ako sa môžeme chrániť pred škodlivými účinkami médií. Index transformuje údaje na štandardizované skóre (z-skóre) od 0 do 100 (od najnižšieho po najvyššie). MLI má štyri dimenzie obsahujúce indikátory nerovnakých váh uvedené v percentách. Pri indikátoroch je uvedený aj zdroj, z ktorých MLI čerpá údaje. V príspevku pracujeme s údajmi IML 2023.

Tabuľka 1 Štruktúra indexu MLI

<i>Indikátory slobody médií</i>	
Skóre Freedom of the Press od Freedom House	20 %
Index slobody tlače podľa Reportérov bez hraníc	20 %
<i>Ukazovatele vzdelania</i>	
Skóre PISA v čitateľskej gramotnosti (OECD)	30 %
Skóre PISA vo vedeckej gramotnosti (OECD)	5 %
Skóre PISA matematická gramotnosť (OECD)	5 %
Zápis do terciárneho vzdelávania (%) (Svetová banka)	5 %
<i>Dôvera</i>	
Dôvera v iných (Trust in others) (prieskum svetových hodnôt - OECD)	10 %
<i>Nové formy participácie</i>	
E-participation Index (OSN)	5 %

Sloboda tlače je nevyhnutná pre zdravú demokraciu. Umožňuje novinárom vyšetrovať a informovať o veciach verejného záujmu bez strachu z cenzúry alebo odvety. Umožňuje tiež občanom prístup k rôznym informáciám a názorom, ktoré sú potrebné na prijímanie informovaných rozhodnutí o ich živote a vláde.

Sloboda tlače nie je absolútna. Vo väčšine krajín existujú určité obmedzenia slobody tlače, ako napríklad zákony proti podnecovaniu násilia alebo prejavom nenávisti. Tieto obmedzenia však musia byť dôkladne odôvodnené a nemali by sa používať na umlčanie nesúhlasu alebo na zabránenie novinárom vykonávať ich prácu. Nárast falošných správ uprostred značne roztriešteného mediálneho prostredia alebo slabých a kontrolovaných médií v niektorých krajinách sprevádza zhoršenie kvality demokratického procesu. V modeli MLI sa na meranie médií používajú dva bežne akceptované indexy – Freedom House a Index Slobody tlače (Reportéri bez hraníc).

Freedom House je organizácia, ktorá vydáva výročnú správu o slobode tlače s názvom Freedom of the Press. Správa hodnotí mieru slobody tlače a zohľadňuje pri tom nasledovné faktory - právne prostredie pre médiá, politické tlaky, ktoré ovplyvňujú spravodajstvo a ekonomické faktory, ktoré ovplyvňujú prístup k správam a informáciám.

Cieľom Indexu slobody tlače (Reportéri bez hraníc) je posúdiť a zoradiť krajiny na základe slobody pre prácu novinárov a fungovanie médií. Index Slobody tlače hodnotí päť strategických oblastí – politickú, ekonomickú, socio-kultúrnu kontextovú, bezpečnostnú a právny rámec. . Najnovší Index slobody tlače z roku 2023 varuje pred nástrahami dezinformácií vytváraných pomocou umelej inteligencie.

Predpokladá sa, že ľudia, ktorí sú vzdelanejší, sú informovanejší, majú viac analytických schopností lepšie kriticky myslia a je menej pravdepodobné, že upadnú do pasce falošných správ. PISA (Programme for International Student Assessment) je štúdia, ktorá zisťuje a na medzinárodnej úrovni aj porovnáva výsledky vzdelávania z pohľadu požiadaviek trhu práce a poskytuje tak obraz o celkových výsledkoch vzdelávacieho systému v krajine. Zahrnuté ukazovatele pre vzdelávanie sú PISA čitateľský výkon, PISA veda (znanosti z oblasti prírodných vied) a PISA matematické znalosti .

Čítanie s porozumením je súčasťou rôznych gramotností, ktoré potrebujeme pre každodenný život. Čitateľská gramotnosť PISA (2006) je definovaná ako "schopnosť porozumieť a používať písané texty a uvažovať o nich pri dosahovaní osobných cieľov, rozvíjaní vlastných vedomostí a schopností a pri podieľaní sa na živote spoločnosti." PISA meria čitateľskú gramotnosť žiakov prostredníctvom testu, ktorý obsahuje úlohy z rôznych oblastí, ako sú: získavanie informácií z textov, interpretácia textov, uvažovanie a hodnotenie textov.

Prírodovedná gramotnosť je schopnosť používať vedecké poznatky, identifikovať otázky a vyvodzovať dôkazmi podložené závery na pochopenie a tvorbu rozhodnutí o svete prírody a zmenách, ktoré v ňom v dôsledku ľudskej aktivity nastali. Podľa PISA (2006) „Prírodovedne gramotný človek je schopný a ochotný zapojiť sa do logických diskusií na tému veda a technika, čo si vyžaduje nasledujúce kompetencie: vysvetliť javy vedeckým spôsobom, navrhnúť a vyhodnotiť prírodovedný výskum, interpretovať získané údaje a dôkazy vedeckým spôsobom.“

Termín matematická gramotnosť nemožno redukovať iba na znalosť terminológie, faktov, postupov a procedúr. Zahŕňa tvorivú kombináciu týchto prvkov na požiadavky vytvorené určitou situáciou. Kľúčovou schopnosťou je použiť matematiku v kontexte nielen čisto matematickom, ale aj v takých prípadoch, v ktorých nie je zrejmá žiadna matematická štruktúra a preto ju treba vytvoriť. Podľa PISA (2006) „Matematická gramotnosť je schopnosť človeka vyjadriť, použiť a interpretovať matematiku v rôznych súvislostiach. Zahŕňa matematické myslenie, používanie matematických pojmov, postupov, faktov a nástrojov na opis, vysvetlenie alebo predpovedanie javu. Pomáha uvedomiť si, akú úlohu má matematika v reálnom svete, a na tomto základe správne posudzovať a rozhodovať sa tak, ako sa to vyžaduje od konštruktívneho, zaangažovaného a rozmyšľajúceho občana.“

Konšpiračné teórie o fungovaní sveta odrážajú a zároveň prinášajú nízku mieru dôvery v existujúce inštitúcie. Súčasný model používa súvisiaci ukazovateľ – Dôvera v iných. Meria úroveň dôvery v spoločnosť a odráža, ako ľudia vnímajú spoľahlivosť iných, podľa definície OECD. Vysoká hodnota Dôvery v iných je spravidla znakom úspešných spoločností a zástupcom rozvoja občianskej spoločnosti.

E-participation Index je ukazovateľ na meranie využívania informačných a komunikačných technológií na zvýšenie politickej účasti, čo umožňuje občanom komunikovať medzi sebou, volenými predstaviteľmi a orgánmi.

Na identifikáciu vplyvných premenných sme použili metódu Náhodného lesa pre regresiu (Random forest regression). Náhodný les pre regresiu je metóda strojového učenia, ktorá sa používa na predpovedanie numerických hodnôt. Funguje tak, že vytvorí niekoľko rozhodovacích stromov na základe náhodne vybraných dát a premenných. To pomáha znižovať preučenie, pretože každý strom vidí iba časť dát a premenných. Náhodný les kombinuje výsledok viacerých predpovedí. (Guyon, Statnikov a Batu, 2019). Existuje niekoľko parametrov, ktoré je potrebné nastaviť pri vytváraní náhodných lesov pre regresiu. Medzi tieto parametre patrí aj počet stromov. Pracovali sme s hodnotou 250. Čím viac stromov je v lese, tým presnejšie sú predikcie. Avšak príliš veľa stromov môže viesť k predikciám, ktoré sú príliš hladké. IncNodePurity je celkový pokles nečistôt v uzloch z rozdelenia na premennej, spriemerovaný zo všetkých stromov. Čistota uzla Inc bola použitá ako miera dôležitosti indikátora.

Intenzitu závislosti sme merali pomocou neparametrického Spearmanovho korelačného koeficientu.

Výpočty sme realizovali v programovom prostredí R.

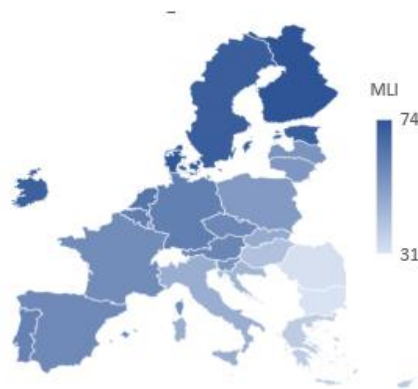
2. VÝSLEDKY A DISKUSIA

Tabuľka 2 obsahuje popisné charakteristiky indikátorov Indexu mediálnej gramotnosti. Najvyššiu hodnotu mediánu dosiahol indikátor Index slobody tlače, skóre pre Freedom of the Press a skóre pre PISA-matematická gramotnosť. Koeficient šikmosti je s výnimkou indikátora Dôvera v iných záporná, čo znamená, že väčšina hodnôt sa nachádza nad priemerom. Takmer symetrické pravdepodobnostné rozdelenie má indikátor kvantifikujúci podiel študentov zapísaných do terciárneho vzdelávania.

Tabuľka 2 Popisné charakteristiky indikátorov

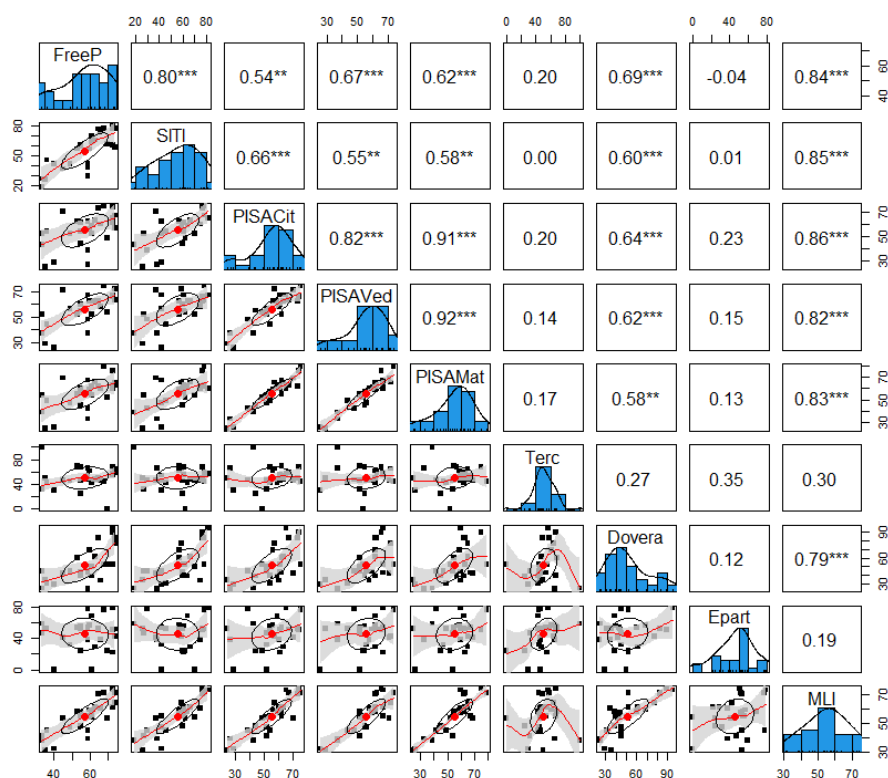
Indikátor	Acronym	Minimum	Maximum	Priemer	Medián	Standardná odchýlka	Šikmosť
Index MLI	MLI	31	74	54.6	55	11.9	-0.22
Skóre Freedom of the Press	FreeP	33	74	57.3	59	12.9	-0.55
Index slobody tlače	SITI	19	81	55.3	60	17.7	-0.37
Skóre PISA v čitateľskej gramotnosti	PISACit	25	75	55.0	57	13.3	-0.71
Skóre PISA vo vedeckej gramotnosti	PISAVed	26	74	55.9	58	12.3	-0.84
Skóre PISA matematická gramotnosť	PISAMat	25	79	55.1	59	13.2	-0.66
Zápis do terciárneho vzdelávania	Terc	0	100	50.3	48	17.6	-0.08
Dôvera v iných	Dovera	24	95	51.2	45	19.4	0.77
E-participation Index	Epart	0	79	45.7	52	20.0	-0.52

Z geografického hľadiska rozloženia hodnôt, najvyššie hodnoty sú v severských krajinách Fínsko (74), Švédsko (71), Estónsko (71). Tiež v Dánsku (73) a Írsku (70). Nižšie hodnoty sú v juhovýchodnej časti Európskej únie – Bulharsko (31), Rumunsko (32), Grécko (38), Cyprus (39), Maďarsko (41). Výsledky nám hovoria že viac kriticky hodnotia informácie z médií severské krajiny ako krajiny východnej časti územia Európskej únie.



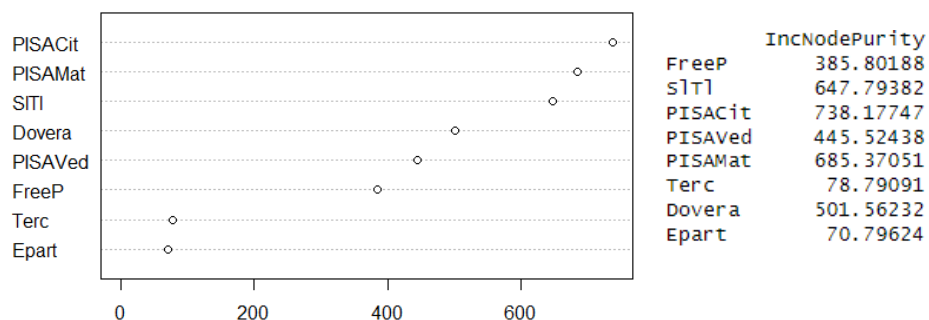
Obrázok 1 Kartogram z hodnôt indexu MLI

Obrázok 2 obsahuje okrem histogramov, jadrovej funkcie hustoty hodnôt jednotlivých ukazovateľov aj Spearmanove korelačné koeficienty medzi jednotlivými indikátormi a výsledným indikátorom MLI. Hodnota Indexu mediálnej gramotnosti štatisticky signifikantne a silne závisí od všetkých indikátorov okrem podielu študentov zapísaných do terciálneho vzdelávania a indikátora E-participation Index. Tieto dva indikátory nevykazujú signifikantnú závislosť nielen s MLI ale ani so žiadnymi ďalšími indikátormi. Prvé tri najsilnejšie sú závislosti s PISACit (0,86), SITl (0,85) a FreeP(0,84).



Obrázok 2 Kombinovaný graf pre index MLI a jeho indikátory

Koeficient determinácie pre Random forest regression je vysoký – 0,9564. Prediktorové premenné zaradeného do náhodného lesa veľmi dobre vysvetľujú odchýlky závisle premennej. O kvalite odhadu svedčí aj nízka hodnota strednej absolútnej chyby (MAE), ktorá meria priemer rezíduí v súbore údajov. Jeho hodnota je 1,298. Podľa Random forest regression sú tri najdôležitejšie indikátory PISACit (738,18), PISAMat(685,37) a SITl (647,79).



Obrázok 3 Poradie dôležitosti indikátorov a hodnoty IncNodePurity

Tabuľka 3 obsahuje poradia dôležitosti indikátorov MLI podľa dvoch metód – Random forest a Spearmanov korelačný koeficient medzi MLI a indikátormi. Môžeme konštatovať, že je zhoda na prvých a posledných dvoch miestach. Ostatné odchýlky vieme zdôvodniť pri pohľade na Obrázok 2, kde vidíme, že skúmané často závislosti nie sú monotónne. Spearmanov korelačný koeficient je vysoký 0,7857 a je signifikantný (p hodnota je 0,0000012). Umiestnenie indikátora PISACit je v súlade s konštatovaním v Správe o MLI.

Tabuľka 3 Poradia dôležitosti indikátorov MLI podľa dvoch metód

Metóda	FreeP	SITl	PISACit	PISAVed	PISAMat	Terc	Dovera	Epart
Náhodný les	6	3	1	5	2	7	4	8
Spearmanov korelačný koeficient	3	2	1	5	4	7	6	8

ZÁVERY

Dezinformácie sú nepravdivé alebo zavádzajúce informácie, ktoré sú zámerne šírené na to, aby ovplyvnili verejnú mienku. Dezinformácie sa často šíria prostredníctvom médií, sociálnych médií a iných online platforiem. Kritické hodnotenie informácií z médií je proces, pri ktorom posudzujeme pravdivosť, dôveryhodnosť a relevanciu informácií. Zahŕňa identifikáciu zdroja informácií, posúdenie jeho záujmov a motivácie a porovnanie informácií s inými zdrojmi. Preto sme ako mieru odolnosti voči dezinformáciám zvolili Index mediálnej gramotnosti. Cieľom príspevku bolo zistiť, ktoré ukazovatele MLI najviac ovplyvňujú jeho výslednú hodnotu. Inými slovami, ktoré indikátory MLI najviac napomáhajú kriticky hodnotiť informácie z médií. Pomocou algoritmu supervised machine learning - random forest sme identifikovali faktory, ktoré najviac ovplyvňujú schopnosť kriticky hodnotiť informácie z médií a tak znižovať účinnosť dezinformačných kampaní. Najdôležitejšie sa ukázali výsledky PISA v oblasti čitateľskej gramotnosti, v oblasti matematickej a Sloboda tlače.

Čitateľská gramotnosť je dôležitým faktorom, ktorý ovplyvňuje schopnosť kriticky hodnotiť informácie z médií a nepodliehať dezinformáciám. Ľudia s vyššou úrovňou čitateľskej gramotnosti sú lepšie schopní rozumieť komplexným textom, ktoré môžu obsahovať rôzne uhly pohľadu a argumenty, identifikovať zámyery a motivácie autora textu, porovnať informácie z rôznych zdrojov a identifikovať rozdiely a nezrovnalosti a v neposlednom rade kriticky hodnotiť informácie a identifikovať potenciálne dezinformácie.

Matematická gramotnosť je dôležitým faktorom, ktorý ovplyvňuje schopnosť kriticky hodnotiť informácie z médií a nepodliehať dezinformáciám. Ľudia s vyššou úrovňou matematickej gramotnosti sú lepšie schopní rozumieť štatistikám a grafickým údajom, ktoré sa často

používajú na prezentáciu informácií z médií, identifikovať potenciálne problémy s údajmi, ako sú chyby alebo skreslenia a kriticky hodnotiť tvrdenia, ktoré sú založené na údajoch. Ľudia s nižšou úrovňou matematickej gramotnosti sú náchylnejší na podliehanie dezinformáciám.

Vysoký Index slobody tlače je najčastejšie spojený s nízkou úspešnosťou dezinformačných kampaní. V krajinách s vysokou slobodou tlače sú novinári schopní nezávisle vyšetrovať a reportovať o aktuálnych udalostiach. To im umožňuje odhaľovať dezinformačné kampane a informovať verejnosť o nich. Ľudia v krajinách s vysokou slobodou tlače majú prístup k širokej škále informácií z rôznych zdrojov. To im umožňuje identifikovať potenciálne dezinformácie a vyvrátiť ich. V krajinách s vysokou slobodou tlače majú ľudia možnosť vyjadriť svoj nesúhlas s vládou alebo inými mocnými skupinami. To bráni týmto skupinám v rozširovaní dezinformačných kampaní bez toho, aby boli kritizované.

Zo získaných poznatkov vyplýva, že je potrebné snažiť sa o vysokú úroveň slobody tlače, aby boli ľudia lepšie informovaní. Treba tiež venovať zvýšenú pozornosť vzdelávaniu, lebo iba vzdelaní ľudia majú analytické schopnosti a dokážu kriticky myslieť. Dezinformačné kampane v krajinách s vysokou úrovňou slobody tlače a vzdelaným obyvateľstvom sú s menšou pravdepodobnosťou úspešné, lebo ľudia sú lepšie informovaní a kriticky zmýšľajúci.

Podakovanie

Príspevok vznikol v rámci národného projektu "Zvyšovanie odolnosti Slovenska voči hybridným hrozbám posilňovaním kapacít verejnej správy", kód projektu ITMS2014+: 314011CDW7. Tento projekt je podporený z Európskeho sociálneho fondu.

Zdroje

1. Bennett, W. L. & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122–139.
2. Duberry, J. (2022). AI and the weaponization of information: Hybrid threats against trust between citizens and democratic institutions. In *Artificial Intelligence and Democracy* (pp. 158-194). Edward Elgar Publishing.
3. EuPI (2023). The Media Literacy Index. Správa. Dostupné na <https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf>
4. Iasiello, E. J. 2017. "Russia's improved information operations: from Georgia to Crimea." *Parameters* 47 (2): 51-63.
5. Index mediálnej gramotnosti. <https://osis.bg/?p=3750&lang=en>
6. Liaw, A., Wiener, M. (2002). Classification and Regression by randomForest. *R News* 2(3), 18--22.
7. Guyon, I., Statnikov, A., & Batu, B. B. (Eds.). (2019). Cause effect pairs in machine learning. Springer (p. 353).
8. OECD: Assessing Scientific, Reading and Mathematical Literacy. A framework for PISA (2006). OECD, ISBN 92-64-02639-8
9. R Core Team (2021). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL <https://www.R-project.org/>
10. Revelle, W. (2022) psych: Procedures for Personality and Psychological Research, Northwestern University, Evanston, Illinois, USA, <https://CRAN.R-project.org/package=psych> Version = 2.2.5.
11. Wardle, C. (2017). Fake news. It's complicated. *First Draft*, 16, 1–11.

12. Weedon, J., Nuland, W., & Stamos, A. (2017). Information operations and Facebook. Facebook Newsroom. Facebook: <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>

ZPŮSOBY SPECIFICKÉHO ZKOUMÁNÍ PRAVICOVÉHO POLITICKÉHO EXTRÉMISMU JAKO MOŽNÉHO NÁSTROJE HYBRIDNÍHO PŮSOBNÍ

Doc. JUDr. PhDr. Ivo Svoboda, PhD., MBA

AMBIS Praha, a.s. Vysoká škola, Lindnerova 1, 180 00 Praha

Abstrakt: Příspěvek se zabývá zkoumáním projevů politického extremismu jako možného nástroje hybridního jednání. Politický extremismus a zejména pravicový politický extremismus je současný fenomén, který je z hlediska kriminologického výzkumu natolik specifický, že vyžaduje specifický přístup při jeho posuzování, zejména z pozice právních expertů. Proto je vhodné zvolit vhodnou konkrétní metodiku vědeckého zkoumání tohoto fenoménu a pro potřeby soudu poskytnout poznatky, které jsou relevantní pro rozhodování o konkrétní věci. V závěru jsou autorem navrženy obecné principy a přístupy k řešení tohoto aktuálního fenoménu naší doby.

Klíčová slova: extremismus, historický diskurz, hybridní hrozba, metodologie vědeckého výzkumu, extremismus, neonacismus, pravicový politický extremismus, hybridní hrozba.

ÚVOD

Extremismus (politický extrémismus) je v současné společnosti velmi frekventovaný pojem. Lidé takto obecně označují „abnormální“, „nepřípustné“ a „nebezpečné“ činnosti, které podle nich nelze nikdy tolerovat, zvláště když jsou spojeny s jejich ideologickými oponenty. Vzhledem k tomu, že mez tolerance je čistě subjektivní pojem, existují různé názory na problematiku politického extremismu. Většina je však hodnocena jako velmi agresivní, nebezpečné a zavrženíhodné činy. Málokdo však bere v úvahu podmínky, ve kterých jsou tyto a další sociálně negativní jevy založeny. Extremismus je přímo závislý na uspořádání a stavu společnosti, ve které se projevuje. Při konfrontaci s takovou společností ve fázi, ve které značně narůstají vnitřní rozpory, drtivá většina extrémních aktivit na ně bezprostředně reaguje.

Podle některých autorů je extremismus produktem – fenoménem demokratické společnosti. Demokracie obecně postrádá účinné obranné mechanismy k obraně všeho, co jí škodí. Kdyby takové mechanismy přestaly být demokratické, staly by se diktaturou. Proto každá demokracie, jakákoli demokratická společnost čelí extremismu. Po celém světě, včetně naší země, existuje mnoho různých extremistických skupin nebo hnutí (extremistických hnutí). *Politický extrémismus však může být součástí hybridního působení.* Často je však velmi obtížné určit, kdo je extremist a kdo ne, protože hranice mezi normalitou a extremismem jsou velmi široké a vágně formulované a jsou mnohdy věcí subjektivního postoje, zejména subjektivního politického názoru [1].

Utváření multidisciplinárního fenoménu současné společnosti, kterým politický extremismus bezesporu je, je tedy třeba řešit z širší interdisciplinární perspektivy. A to z hlediska filozofie, psychologie, sociologie, vzdělání, politiky a nakonec i z perspektivy práva. Pro účely jasného soudního líčení, resp. potřeby znaleckého posouzení věci je proto nejvhodnější použít vhodnou konkrétní formu vědeckého výzkumu. Jako specifická metoda vhodná pro sběr a zpracování informací se jeví metoda historického diskurzu a metoda analýzy²⁸², kterou lze použít pro posouzení společenské škodlivosti a nebezpečnosti pro společnost [2].

²⁸² Tato metoda byla poprvé použita M. Foucaultem v jeho „History of Madness“, později se rozvinula v práci „Archeologie vědění“.

1. MOŽNOST ZKOUMÁNÍ PROJEVŮ PRAVICOVÉHO POLITICKÉHO EXTREMISMU

Zvolená historická metoda, resp. historický přístup je užitečný především při posuzování textu a shromážděných jakýchkoliv obrazů hmoty a také pro analýzu a syntézu empirického materiálu, tedy všech dokumentů nastíněných výzkumnými odborníky nastíněných v jeho komplexu. Historická metoda, metoda může být použita přímo i nepřímo. Přímá metoda je v podstatě pouze prostou reprodukcí pramenů, ale neumožňuje další hloubkovou analýzu vedoucí k hodnocení složitých sociálních vztahů. Naproti tomu nepřímá metoda umožňuje deduktivnější extrapolaci a určení kauzální analogie určitých historických informací pro hodnocení konkrétní reality. Použití nepřímé historické metody však s sebou nese riziko částečného zkreslení historické reality [2]. Pro minimalizaci tohoto rizika, resp. jeho vyhnutí je vhodné hodnotit i vzorek, resp. Přibližuje se spíše materiálové dílčí metody, resp. jejich vzájemné kombinace.

Jako další nepřímé metody by bylo dle Hrocha [3]. možno použít i metody diachronní a synchronní. Tyto metody jako podpůrné určují pozici podle myšlené časové osy od staršího období k mladšímu a synchronní metoda je dále navíc i způsobilá vytvářet určité etapy dějin, v jejichž rámci jsou konfrontovány dějinné události a jsou zjišťovány jejich podobnosti a rozdíly. Tato podpůrná metoda se znalci jeví jako další vhodná, zejména z důvodu relativně delší doby vývoje projevů extremismu v České republice v návaznosti na fašistickou, neofašistickou, nacistickou a neonacistickou subkulturu [3].

Metoda diskursivní analýzy [4] se odvíjí od tzv. archeologie vědění, kterou formuloval její autor M. Foucault jako metodu pro výzkum dějin myšlení, dějin idejí, dějin poznání a filozofie, sociologie a ostatně i politologie. Jejím původním cílem bylo sledovat historický vývoj různých myšlenkových a ideových konceptů a jejich proměn v lidských dějinách. Centrální kategorií tohoto schématu se stal diskurs. Diskurs (Foucault také používal pojem „diskursivní formace“), je možno definovat jako strukturu, která ovlivňuje způsoby řeči, psaní a myšlení. „Diskurs“ v sociálních vědách je v obecném smyslu užíván pro označení jazyka jako prvku sociálního života, jenž je dialekticky propojen s dalšími elementy společenského života a obecně postojů společnosti ke konkrétním jevům. Ovšem i když analýza diskursu má co dělat se zkoumáním jazyka (v našem případě i jiných forem sociální komunikace – např. pomocí vlajek, odznaků, hudbě na datových nosičích a jiných fetišů vztahujících se ke konkrétní ideologii či období vedených jednotným ideovým diskursem apod.) není podle Foucaulta jednoduše totožná s prostou analýzou jazyka, nebo běžnou sémantikou (v našem případě i jiných forem sociální komunikace – např. pomocí vlajek, odznaků, hudbě na datových nosičích a jiných fetišů vztahujících se ke konkrétní ideologii či období vedených jednotným ideovým diskursem apod.). Zatímco prostá analýza jazyka či sémantika klade otázku, podle jakých pravidel je výpověď o realitě tvořena, a tudíž podle jakých pravidel mohou být vytvořeny další podobné výpovědi vypovídající o konkrétní realitě, popis diskursivní události klade zcela odlišnou otázku, a to: „jak se stalo, že se na tomto místě objevila tato, a ne nějaká jiná výpověď? [4]“.

Jednotlivé diskursy pak vystupují v podobě dominantních předmětů a metod zkoumání, typických pro danou historickou epochu. Vystupují jako určité pravidelnosti mezi typy výpovědí, pojmy, symboly či volbami. Tyto pravidelnosti pak lze metodologicky zpracovat vhodnou metodou sběru a zpracování shromážděných dat či dominantních předmětů zkoumání. Existence těchto dominantních předmětů či metod zkoumání podle Foucaulta ovlivňuje směr dalšího vědeckého zkoumání; v našem případě směr zkoumání celé předložené materie ve svém souhrnu jako předmětu znaleckého zkoumání a dílo samotné, tedy i posudek znalce, je z tohoto hlediska možno chápat jako výpověď, ve které se daný signifikantní diskurs odráží. Diskursy určují, jaké výpovědi jsou možné, proč jsou možné právě tyto výpovědi a proč jsou případně

opomenuty výpovědi jiné a z jakých důvodů. Autoři slovních výpovědí (v našem případě i jiných forem sociální komunikace – např. pomocí vlajek, odznaků, hudbě na datových nosičích a jiných fetišů vztahujících se ke konkrétní ideologii či období vedených jednotným ideovým diskursem apod.) vedených jednotným ideovým diskursem apod., již nejsou chápáni jen jako její tvůrci, popř. nositelé, ale především jako uživatelé, šířitelé a propagátoři určitého diskursu [5].

„Diskurs lze tedy definovat v makrohistorickém foucaultovském smyslu jako strukturu, která reguluje konkrétní způsoby řeči, psaní a myšlení, která produkuje jak myšlení, tak konkrétní praktiky. Pro toto pojetí makrohistorického diskursu lze používat Foucaultův termín „diskursivní formace“ [6]. Šířitel tohoto diskursu je pak sám nositelem konkrétního společensky závadového diskursu tak, jako tvůrci samotní. Chceme-li proto identifikovat dominantní diskurs či diskursy konceptu společenské závadnosti či dokonce nebezpečnosti celého zkoumaného vzorku, resp. celé zkoumané materie a její vztah k diskursům současné filozofie, psychologie, politologie, sociologie, sociální pedagogiky, či sociologie práva, musíme nejdříve shromáždit dostatečné množství výpovědí, které se ke zkoumanému vzorku, resp. předestřené obrazové vztahují. Foucault doporučuje postupovat následujícím způsobem:

Nejprve je třeba vyznačit prvotní *povrchy vynoření*. Jde tedy o to ukázat, kde se tyto výpovědi vůbec mohou objevit, aby mohly být posléze označeny a analyzovány. V těchto polích povrchů vynoření dochází k prvotním diferenciacím, jsou zde ohraničovány oblasti vypovídání, je definováno to, o čem se hovoří a popisovaný jev získává statut objektu z oblasti aktivit přímo či zprostředkovaně směřujících k potlačení práv a svobod člověka, nebo hlásajících zášť nebo nenávisť vůči jiné výlučné skupině osob, anebo podpory či propagace hnutí směřujících k potlačení demokratických práv člověka, které je možno postihnout normami jak společenskými (jev obecně nekonformní, závadový, nevhodný až nebezpečný), tak případně i obecně závaznými právními předpisy z oblasti trestního práva. Prostřednictvím vynoření konkrétní výpovědi je pak tento jev učiněn pojmenovaným a popsatelem a stává se tak „skutečným“ [5].

Druhým krokem diskursivní analýzy je popis tzv. instancí vymezování. Instancemi vymezování jsou dobové instituce či organizace (vymezené například i místem, časem, způsoby projevu a dalšími relevantními okolnostmi), které mají klíčový podíl na vymezení společenské nekonformnosti, závadovosti, nevhodnosti až nebezpečnosti zkoumaného objektu a případně další trestní postížitelnosti tím, že uchopují určité jevy, vytvářejí z nich své předměty zájmu, zakotvují určité shody, markanty, či diferenciaci jako přirozené, sjednocující výpovědi a vytváří tím určitý model či skupinu modelů, které se stávají obecně užívanými [6]. V rámci zaměření znaleckého zkoumání a položených otázek za takové instance vymezování můžeme považovat především stát, jeho právní normy (zpočátku zvykové, později písemné legislativní nástroje) a také obecně kulturní, filozofické, politologické, sociologické, politologické, sociální a sociálně – pedagogické postoje společnosti v celé své šíři. Z užšího pohledu vnímání pak můžeme tyto instance vymezování specifikovat v souvislosti s odkazem na výše uvedený srovnávaný materiál na obsažené fašistické, neofašistické, nacistické a neonacistické projevy v nejširším slova smyslu.

Třetím krokem diskursivní analýzy je určení tzv. mřížek specifikace. Tímto pojmem označuje Foucault systémy, podle nichž se vzájemně třídí, oddělují, sdružují, přeskupují, klasifikují a navzájem odvozují jednotlivé signifikantní výpovědi o daném jevu. Podstatou identifikování těchto mřížek specifikace je využití komparativní metody [5].

Jsou srovnávány především jednotlivé shromážděné výpovědi o předmětu zkoumání jako primární objekty komparace, jejich elementární shody v označování daného problému a možnosti jejich diferenciací. Komparace výpovědí o předmětu zkoumání v zadání znaleckého posudku (tedy v celé předestřené materii) se bude zaměřovat především na následující kategorie [3] [7].:

- *způsoby nazírání společnosti na fašistickou, neofašistickou, nacistickou, neonacistickou a rasistickou subkulturu jako hnutí, které prokazatelně směřuje k potlačení demokratických práv člověka nebo hlásá národnostní, rasovou, náboženskou, třídní či jinou zášť nebo nenávist vůči jiné skupině osob, či podněcuje k projevům antisemitismu, xenofobie, rasismu apod.,*
- *postoj společnosti k slovní, hudebním či jiným aktivitám, které odpovídají podpoře, propagaci, veřejných projevů sympatií, nebo šíření idejí hnutí směřujících k potlačení demokratických práv člověka,*
- *možné a historicky běžně vzdělanému občanu srozumitelné formy protispolečenského až kriminálního jednání, které je charakteru projevu nenávisti k určité skupině obyvatel, popřípadě podpoře, propagaci nebo veřejných projevů sympatií k hnutím směřujícím k potlačení demokratických práv člověka,*
- *společností odmítané a postihovatelné způsoby propagace obecně extremismu a specificky nacismu a neonacismu jako hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka nebo hlásá národnostní, rasovou, náboženskou či třídní zášť, popřípadě hlásající zášť vůči jiné skupině osob, anebo podpoře, propagaci či veřejných projevů sympatií k hnutím směřujícím k potlačení demokratických práv člověka.*

2. ZÁVĚRY VYŠETŘOVÁNÍ PRAVICOVÉHO POLITICKÉHO EXTREMISMU JAKO MOŽNÉHO HYBRIDNÍHO PŮSOBNÍ

Určení těchto shod a pravidelností, jakož i zároveň identifikace možných diferencí se stává základem dalšího výše uvedeného metodologického zpracování do podoby určitých typů vypovídání, typů dobového a místního nazírání společnosti na předestřené obrazy vypovídající o realitě jazyka (v našem případě i jiných forem sociální komunikace – např. pomocí vlajek, odznaků, symbolů, hudbě na datových nosičích a jiných fetišů vztahujících se ke konkrétní ideologii či období vedených jednotným ideovým diskursem apod.).

S ohledem na charakter zadání znaleckého posudku však nemůže být vyústěním závěrů pouze formulace obecných zákonitostí možné neonacistické propagace směřující k potlačování práv a svobod občanů, popř. podpory a propagace hnutí směřujících k potlačení práv a svobod člověka ve smyslu trestního zákona, popřípadě vzbuzování nenávisti vůči jiné skupině obyvatel. Prostřednictvím této typologie budou ve znaleckém posudku individuálně provedeny závěry filozofických, politologických, sociologických a sociálně - pedagogických diskursů ve společnosti, které jsou formulovány v podobě typů, tedy ve smyslu určitých myšlenkových konstruktů a společenských postojů. Tyto typy tedy mají jen relativní platnost a nevznikají s cílem co nejpřesnější deskripce daného jevu a jeho hodnocení, ale naopak se záměrem jejich pochopení [8]. Výsledným produktem znaleckého zkoumání pak je charakteristika pozice a vnímání společenské nekonformnosti, závadovosti, nevhodnosti až nebezpečnosti konkrétních skutečností jazyka (v našem případě i jiných forem sociální komunikace – např. pomocí vlajek, odznaků, hudbě na datových nosičích a jiných fetišů vztahujících se ke konkrétní ideologii či období vedených jednotným ideovým diskursem apod.), které jsou předmětem znaleckého zkoumání zejména ve filozofických, politologických, psychologických, sociologických a sociálně – pedagogických diskurzech [8].

Z hlediska společenské nekorektnosti, nevhodnosti, nebo závadovosti je v námi posuzovaném případě třeba posuzovat především celkový kontext užití slovního spojení a jednání, které má za cíl působit jako potencionální hybridní hrozba. Důležitá je vazba slovního vyjádření popřípadě s tím spojeného jednání s určitými pravidly a společností komponovanými zakázanými či společensky neakceptovatelnými cíli, případně jeho hanobící či nenávisť podněcující vyznění, podpory a propagace hnutí směřujících k potlačení práv a svobod člověka, anebo souvislost s určitým přesvědčením pachatele, které jej vede k páchání protispoločenských aktivit odsuzovaných jak drtivou většinou veřejného mínění, tak odporující tradičním hodnotám demokratického státu (ve smyslu deklarace práv a svobod) [9].

ZÁVĚR

Projevy politického extremismu ve společnosti jsou aktuálním fenoménem současného globálního světa. Vzhledem k tomu, že se může jednat o součást hybridního jednání (např. proti vnitropolitické stabilitě státu nebo proti vnitřní bezpečnosti státu), je třeba tento jev posuzovat s náležitou péčí, jakož i odborným a vědeckým přístupem, který by neměl být adekvátní společenské realitě, ale byl by stejný jako vědecký pohled a zároveň přiměřeně dostupný každodenní praxi orgánů činných v trestním řízení, zejména policie a soudů.

Dopady projevů pravicového politického extremismu jako možné metody hybridního jednání mohou mít dopad nejen na vnitřní bezpečnost státu, ale mohou přinášet i významná ekonomická rizika. Může se jednat např. o znehodnocení budov či památek značného rozsahu, o znehodnocení budov či památek značné historické hodnoty nebo jejich poškození, které lze přímo vyjádřit v penězích, ale také např. o nárůst škody na veřejných zařízeních nebo se může jednat o přímé sabotáže či teroristické útoky namířené proti kritické infrastruktuře s cílem poškodit zájmy státu a v konečném důsledku i civilních obyvatel [10]. Může se jednat o širokou škálu možných škod, a to jak přímých (zničení konkrétních objektů nebo objektů kritické infrastruktury), tak i sekundárních škod vyplývajících z poškození či znehodnocení primárního cíle - tedy poškození při zajišťování nouzových dodávek elektřiny, vody, potravin a pod [11]. Je tedy zcela v zájmu státu předcházet jak bezpečnostním rizikům, tak případným značným materiálními škodám. Zde je vhodné zdůraznit preventivní a represivní roli státu, prostřednictvím orgánů činných v trestním řízení, zejména policie a soudů.

Na extremismus (včetně pravicového politického extremismu) je třeba pohlížet ve světle již zažitě a soudem respektované definice extremismu. Jedná se o explicitní či identifikovatelně implicitní ideologické stanovisko, provázené prvky nesnášenlivosti a agrese, odchyloující se od ústavních či právních norem, přičemž útoky směřují proti základním demokratickým ústavním principům, jak jsou definovány v ústavním pořádku ČR (a i SR), a útoky proti těm principům, které jsou obecně vyjmenovány v Deklaraci práv a svobod a které jsou společné zemím, které sdílejí stejné lidskoprávní hodnoty [12].

Pokud někdo apeluje na popření nabádání k popírání či jinak, k napadání těchto hodnot formou politického extrémismu, je na místě, aby státní moc zasáhla a bránila demokratické hodnoty. K prokázání těchto aktivit před soudem pak může posloužit znalecký posudek, který soud potřebuje k identifikaci příznaků, které jsou demokratickou cizí společností nebo ohrožují demokratickou společnost nebo působí jako hybridní hrozba pro demokratický stát.

Zdroje

1. CHMELÍK, J. *Symbolika extremistických hnutí*. Praha: Armex a Trivis, 2000, ISBN – sine.

2. HROCH, M. a kol. *Úvod do studia historie*. Praha: SPN, 1985, ISBN – sine
3. SVOBODA, I. Zločiny z nenávisti jako projevy politického extremismu současné neonacistické scény v Evropě, In. *Deliktologie, Akademie HUSPOL, Kunovice, 2021*, eds. Kopotun, I., Petkov, S., s. 155-173. ISBN 978-80-907587-1-1.
4. NOSÁL, I. Rekonstrukce diskurzu dětství. Rozbor čtyř textů In. *Obrazy dětství v české společnosti dnes. Studium sociologie dětství*. Brno: Barister & Principal, 2004,
5. FOUCAULT, M. *Archeologie vědění*. Praha: Heřman a synové, 2002,
6. SZALÓ, C. *Sociologie utváření sociálních identit*. V. SZALÓ, C., NOSÁL, I., Mozaika v rekonstrukci. Formování sociálních identit v současné střední Evropě. Brno: MU Brno, Mezinárodní politologický ústav, 2003,
7. MAREŠ, M. *Pravicový extremismus a radikalismus*. Brno: Centrum strategických studií, 2005
8. WEBER, M. *Metodologie společenských věd*. Bratislava: Nakladatelstvo Pravda, 1983 ISBN – sine.
9. SVOBODA, I. Klíčové kompetence manažera a leadra v ozbrojených silách. In.: *Zborník vědeckých příspěvků z vědecké konference „Bezpečnostné fórum 2021“*: Banská Bystrica, 2021, s. 146-156. ISBN 978-80-973394-4-9.
10. BRZYBOHATÝ, M. *Terorismus I*. Praha: Ministerstvo obrany ČR, 1999. ISBN 80-9026-70-1-7.
11. SVOBODA, I., VIČAR, R. Politický extremismus a terorismus jako destabilizující prvek vnitřní a vnější bezpečnosti EU. V. *Seminář Národního konventu o Evropské unii „Rozšíření, bezpečné a prosperující sousedské prostředí v EU“*, Liptovský Mikuláš 17. září 2009.
12. RATAJ, J. *Vize Česká nacionalistické politiky v současném pojetí krajní pravice v ČR*. Ve III. sjezd českých politologů, Olomouc 8.-10. 9. 2006; NĚMEC, J., ŠŮSTKOVÁ, M. (ed.). Praha, Olomouc: Česká společnost pro politické vědy, 2006.

KYBERNETICKÝ ROZMER HYBRIDNÝCH HROZIEB VO VZŤAHU K VEREJNEJ SPRÁVE

plk.v.v. doc. Ing. Stanislav Šišulák, PhD., MBA

Prorektor pre pedagogickú činnosť Akadémie Policajného zboru v Bratislave, stanislav.sisulak@akademiapz.sk / stanislav.sisulak@minv.sk

Abstrakt: Príspevok sa zaoberá verejnou správou ako oblasťou zodpovednou za riadenie verejných záležitostí, správu štátu a verejných služieb pre občanov, v rámci tohto kontextu sa verejná správa stretáva s výzvami, ktoré prichádzajú s hybridnými hrozbami. Tieto hrozby môžu zasiahnuť rôzne oblasti verejnej správy a spoločnosti ako celku. Hybridné hrozby sú zvlášť nebezpečné pre verejnú správu, pretože môžu oslabiť spoločnosť a jej inštitúcie, destabilizovať politický systém a spôsobiť nedôveru občanov voči vláde.

Kľúčové slová: informačná bezpečnosť, kybernetická bezpečnosť, kybernetický priestor, kybernetické útoky, bezpečnostné incidenty.

ÚVOD

Kybernetický rozmer hybridných hrozieb vo verejnej správe je významný a predstavuje jednu z najväčších výziev. Kybernetické útoky sa stávajú čoraz sofistikovanejšími a šíria sa rýchlejšie ako kedykoľvek predtým. Ich cieľom je narušiť, poškodiť alebo získať neoprávnený prístup k dátam a informačným systémom verejnej správy. Pre verejnú správu je dôležité venovať pozornosť hybridným hrozbám a vyvíjať opatrenia na ich predchádzanie a zvládanie. To zahŕňa posilnenie kybernetickej bezpečnosti, zlepšenie informačnej gramotnosti a kritického myslenia občanov, budovanie odolnosti voči dezinformáciám a manipulácii s verejnou mienkou, a zlepšenie spolupráce medzi rôznymi inštitúciami na boj proti hybridným hrozbám. Verejná správa využíva informačné technológie na spracovanie a uchovávanie citlivých údajov, ako sú osobné údaje občanov, dôverné informácie a utajované skutočnosti. Kybernetické útoky na tieto systémy môžu spôsobiť značné škody a ohroziť dôveru verejnosti v inštitúcie verejnej správy.

Pre boj proti kybernetickým hrozbám vo verejnej správe je dôležité implementovať silné bezpečnostné opatrenia, vrátane viacúrovňovej autentifikácie, šifrovania, monitorovania sietí a systémov, aktualizácie softvéru a vytvorenie kultúry kybernetickej bezpečnosti medzi zamestnancami. Spolupráca s odborníkmi na kybernetickú bezpečnosť a kontinuálne zlepšovanie bezpečnostných opatrení je nevyhnutná pre ochranu informačných systémov verejnej správy pred kybernetickými hrozbami.

Informačnú bezpečnosť je možné definovať ako „zachovanie dôvernosti, integrity a dostupnosti informácií“²⁸³.

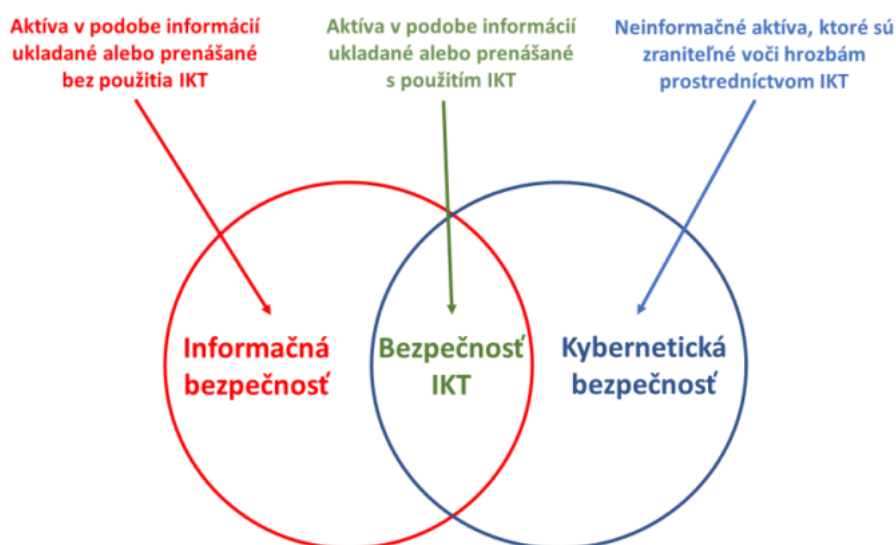
Kybernetická bezpečnosť je definovaná ako „zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore“²⁸⁴.

²⁸³ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.

²⁸⁴ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27032: 2012 – Information technology—Security techniques—Guidelines for cybersecurity.

Kybernetický priestor je „komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete prostredníctvom technologických zariadení a sietí, ktoré sú k nemu pripojené, a ktoré neexistujú v žiadnej fyzickej podobe“²⁸⁵.

Rozdielom a spoločným črtám týchto dvoch bezpečností sa venujú viaceré výskumné skupiny. Dôležitou prácou v tomto smere je výskum vedený Rossouw Von Solms. V rámci svojej práce uvádza, že informačná bezpečnosť je ochrana informácií, ktoré sú aktívom pred možným poškodením v dôsledku rôznych hrozieb a slabých miest. Na druhej strane kybernetická bezpečnosť nie je nevyhnutne len ochranou samotného kyberpriestoru, ale aj ochranou tých, ktorí v kyberpriestore fungujú, a všetkých ich aktív, ktoré sú prostredníctvom kyberpriestoru dostupné²⁸⁶.



Obrázok 1 Rozdiel medzi informačnou a kybernetickou bezpečnosťou
Zdroj: spracované podľa Von Solms R. - Van Niekerk . (2013)²⁸⁷

Informačná ako aj kybernetická bezpečnosť sledujú rovnaké ciele (princípy), a to zabezpečenie dôvernosti (confidentiality), celistvosti (integrity) a dostupnosti (availability) informácií, prostredia (napr. informačných systémov), v ktorých sú tieto informácie uložené a spracúvané ako aj iných entít, ktoré majú určitú hodnotu²⁸⁸, ²⁸⁹ (Obrázok 2).

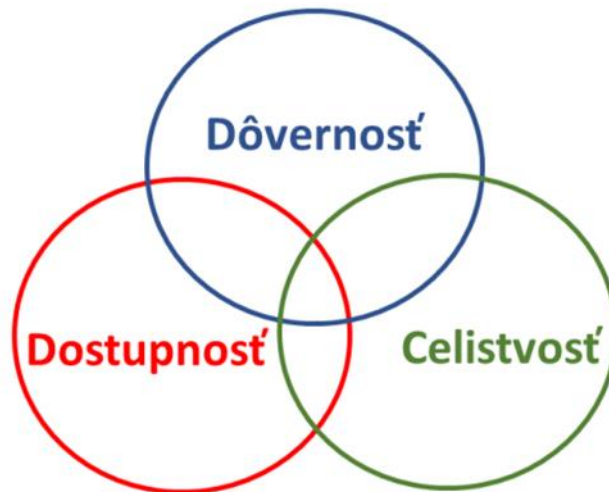
²⁸⁵ Ibid.

²⁸⁶ VON SOLMS R. - VAN NIEKERK J.: From information security to cyber security. Computers & security. 2013, 38, s. 97-102. Dostupné na internete.

²⁸⁷ VON SOLMS R. - VAN NIEKERK J.: From information security to cyber security. Computers & security. 2013, 38, s. 97-102. Dostupné na internete.

²⁸⁸ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.

²⁸⁹ FLORES M. The Language of Cybersecurity. XML Press, 2018.



Obrázok 2 Triáda CIA

Zdroj: vlastné spracovanie podľa Andraško, J. – Mesarčík, M. – Sokol, P. 2022. Právo kybernetickej bezpečnosti.

Prvý cieľ predstavuje zabezpečenie **dôvernosti (confidentiality)**. Zabezpečenie dôvernosti znamená, že dôverné informácie nie sú sprístupnené alebo zverejnené neoprávneným osobám, subjektom alebo procesom²⁹⁰. Ak by sa neoprávnený používateľ dostal k dôverným informáciám, nesmie mať možnosť zistiť ich obsah. Príkladom zabezpečenia dôvernosti je ochrana obsahu emailovej komunikácie, rôznych typov dokumentov, ktoré sú určené len konkrétnym osobám, ale aj rôzne informácie o samotnom informačnom systéme (konfiguračné nastavenia) alebo jeho používateľoch (napr. pridelené oprávnenia, role, záznamy o prihláseniach). V tomto kontexte je nutné zabezpečiť, aby sa s údajmi používateľa mohli oboznámiť len vopred určené osoby. Iný príklad môže predstavovať zdravotná dokumentácia pacienta (bez ohľadu na formu), s ktorej obsahom by sa nemala možnosť oboznámiť iná osoba ako pacient, jeho ošetrojúci lekári a v určitých prípadoch aj rodinní príslušníci.

Druhým cieľom je zabezpečenie **celistvosti (integrity)**. Tento cieľ sa dosiahne v tom prípade, keď sa zabezpečia kompletne, konzistentné a nemodifikované informácie²⁹¹. Oprávnený používateľ musí mať možnosť zistiť, ak dôjde k narušeniu celistvosti informácií, napríklad jej modifikáciou. V tomto kontexte je nutné rozlišovať fyzické a logické pozmenenie informácií.

Príkladom fyzického pozmenenia informácií môže byť poškodenie ich nosiča (napr. databázy, diskov), pri ktorom nie je možné prísť k časti alebo všetkým informáciám. Príkladom logického poškodenia je pozmenenie informácie o používateľovi (napr. zmena jeho pracovného zaradenia, zmena role), alebo zásah do konfiguračného nastavenia servera alebo sieťového zariadenia.

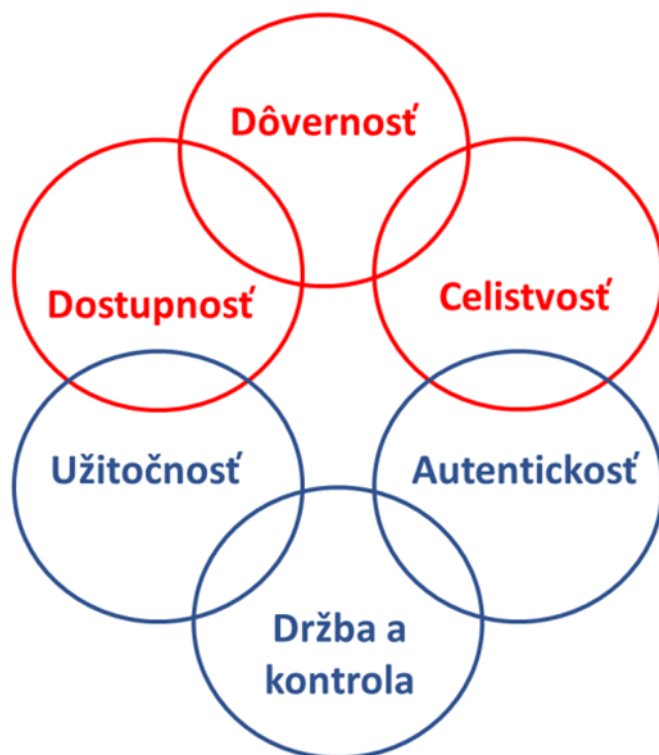
Zabezpečenie **dostupnosti (availability)** predstavuje tretí cieľ. Podstatou tohto cieľa je, aby informácie boli prístupné a použiteľné v správny čas, na správnom mieste, oprávnenej osobe, subjektu alebo procesu, a existujú prekážky, ktoré znemožňujú prístup neoprávneným osobám,

²⁹⁰ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.

²⁹¹ DEATH, D. Information security handbook: develop a threat model and incident response strategy to build a strong information security framework. 2017.

subjektom alebo procesom.²⁹² 10 Medzi príklady nedostupnosti môžeme zaradiť nedostupnosť informácií (napr. v dôsledku chyby systému sa časť obsahu webového sídla nezobrazí), nedostupnosť komunikačnej siete (napr. výpadok pripojenia k sieti internet), nedostupnosť systému (napr. v dôsledku chýbajúceho elektrického napájania nebude dostupný celý informačný systém) a nedostupnosť ľudských zdrojov (napr. chýbajúci zamestnanci, ktorí majú know-how pre riešenie konkrétnych problémov).

Vyššie uvedené ciele sa v literatúre označujú ako **triáda C(onfidentiality) I(ntegrity) A(vailability)**.²⁹³ Okrem spomínanej triády je možné pri cieľoch informačnej a kybernetickej bezpečnosti uvažovať aj o tzv. **Parkerianovej šestici** (Parkerian Hexad)²⁹⁴. Tá okrem už vyššie rozobraných cieľov informačnej a kybernetickej bezpečnosti obsahuje aj držbu alebo kontrolu (possession or control), autenticitosť (autenticity) a užitočnosť (utility) (Obrázok 3).



Obrázok 3 Parkerianova šestica.

Zdroj: vlastné spracovanie podľa Andraško, J. – Mesarčík, M. – Sokol, P. 2022. Právo kybernetickej bezpečnosti.

Prvý cieľ Parkerianovej šestice predstavuje **držba alebo kontrola (possession or control)** týkajúca sa fyzického nakladania s médiom, na ktorom sú informácie uložené²⁹⁵. Inými slovami, cieľom je zabrániť fyzickému kontaktu s údajmi, resp. informáciami (napr. zamedziť skopírovaníu údajov z kariet používaných v hromadnej doprave) alebo zabrániť

²⁹² INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.

²⁹³ GRAHAM, J. - HOWARD, R. - OLSON, R. (eds.) Cyber Security Essentials. 2011.

²⁹⁴ REID, R. C. - GILBERT, A. H. Using the Parkerian Hexad to introduce security in an information literacy class. In: 2010 Information Security Curriculum Development Conference. 2010. s. 45-47. Dostupné na internete.

²⁹⁵ ANDRESS J. Foundations of Information Security: A Straightforward Introduction. 2019.

neoprávnenému používaniu duševného vlastníctva (napr. vytvorenie kópie obsahu dokumentu, ktorého obsah podlieha autorským právam).

Druhým princípom je **autenticita (authenticity)**. Tento princíp nám umožňuje povedať, či sú príslušné informácie pripísané správne vlastníkovi alebo tvorcovi. Inými slovami, tento princíp predstavuje zhodu so zamýšľaným významom. To sa môže zabezpečiť tak, že sa vyhýbame nezmyselnosti (napr. vo formulári, kde sa má uviesť dátum narodenia osoby neuvedieme priezvisko osoby) alebo bránime podvodu (napr. v prípade ak niekto zašle podvodnú správu, ktorá je upravená tak, že sa javí, ako keby pochádzala od z inej emailovej adresy ako bola skutočne odoslaná).

Napokon, **užitočnosť (utility)** odkazuje na to, ako užitočné sú informácie. To sa prejavuje vo vyhnutí sa konverzie údajov na menej užitočnú formu (napr. zmena dátumu narodenia do inej formy, 19.9.2017 -> 2017-09-19-00) alebo zabráneniu nepoužitej formy údajov (napr. ak dôjde k zašifrovaniu dokumentu obsahujúceho konkrétne informácie a súčasne sa stratí dešifrovací kľúč).

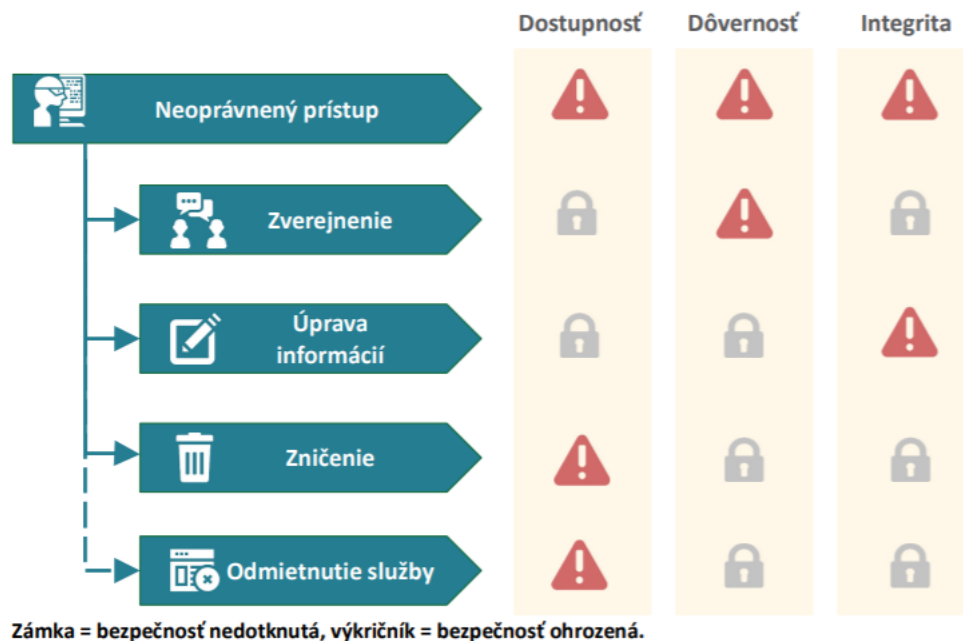
Kybernetická bezpečnosť ovplyvňuje každodenný život všetkých občanov EÚ

Všeobecné štandardné vymedzenie pojmu kybernetická bezpečnosť neexistuje. V tomto dokumente kybernetická bezpečnosť znamená činnosti potrebné na ochranu sietí a informačných systémov, ich používateľov a iných osôb dotknutých kybernetickými hrozbami. Kybernetická bezpečnosť zahŕňa prevenciu a odhaľovanie kybernetických útokov, reakciu na ne a obnovu po nich. Tieto incidenty môžu byť úmyselné alebo neúmyselné a môžu siahať od náhodného zverejnenia informácií po útoky na podniky a kritickú infraštruktúru, krádež osobných údajov, či dokonca až po zasahovanie do demokratických procesov vrátane zasahovania do volieb či všeobecné dezinformačné kampane na ovplyvnenie verejnej diskusie.

Kybernetická bezpečnosť má vplyv na každodenný život všetkých občanov EÚ vždy, keď používame osobné zariadenia informačných technológií, akými sú smartfóny, bezdrôtové miestne počítačové siete (Wi-Fi), sociálne médiá či elektronické bankovníctvo. V roku 2020 viac než kedykoľvek predtým už otázkou nie je, či ku kybernetickým útokom dôjde, ale ako a kedy k nim dôjde. Týka sa to nás všetkých: jednotlivcov, podnikov a subjektov verejného sektora.

Na obrázku 4 sa uvádza, ako EÚ potvrdzuje kybernetickú bezpečnosť a vytvorila rámec na ochranu každodenných elektronických činností občanov pred kybernetickými útokmi. Ochrana kritických informačných systémov a digitálnej infraštruktúry pred kybernetickými útokmi sa stala strategickou výzvou.

Mnohé druhy kybernetických hrozieb, ktorým naše spoločnosti čelia, možno rozdeliť podľa toho, čo sa pri nich deje s údajmi (zverejnenie, úprava, zničenie alebo zamietnutie prístupu), alebo podľa toho, ktoré základné zásady informačnej bezpečnosti porušujú (pozri obrázok 4).



Obrázok 4 EÚ potvrdzuje kybernetickú bezpečnosť v každodennom živote občanov EÚ
Zdroj: EDA, Ikony vytvorené Pixel perfect z <https://flaticon.com>²⁹⁶.

Zakaždým, keď sa zariadenie pripojí na internet alebo sa prepojí s inými zariadeniami, zvyšuje sa možnosť útokov proti kybernetickej bezpečnosti. Exponenciálny rast internetu vecí, cloudu, veľkých dát (big data) a digitalizácie priemyslu sprevádza zvyšovanie expozície voči slabým miestam systému, ktoré útočníkom umožňujú cieľiť na čoraz viac obetí. Rozmanitosť druhov útokov a ich čoraz väčšia dômyselnosť znemožňujú držať krok s ich vývojom²⁹⁷.

Druhy kybernetických útokov

Malvér (škodlivý softvér) je navrhnutý tak, aby poškodzoval zariadenia alebo siete. Táto kategória zahŕňa vírusy, trójske kone, ransomvér, počítačové červy, advér a spyvér (napr. NotPetya).

Ransomvér je softvér, ktorý šifruje údaje, čím bráni používateľom v prístupe k ich súborom, kým nezaplatia výkupné, zvyčajne v kryptomene, alebo kým nevykonajú istú činnosť. Podľa Europolu prevládajú útoky typu ransomvéru a v niekoľkých posledných rokoch došlo k prudkému nárastu počtu druhov ransomvéru (napr. Wannacry²⁹⁸).

Pribúdajú útoky **distribúovaného odmietnutia služby** (ďalej len „útoky DDoS“), pri ktorých sa znemožní prístup k službám alebo zdrojom prostredníctvom zaplavenia týchto služieb alebo zdrojov vyšším počtom požiadaviek, než sú schopné zvládnuť, pričom v roku 2017 tento druh útokov postihol jednu tretinu organizácií²⁹⁹.

²⁹⁶ EURÓPSKY PARLAMENT, Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, štúdia pre Výbor pre občianske slobody, spravodlivosť a vnútorné veci (LIBE), september 2015. Dostupné na internete.

²⁹⁷ ENISA. Threat Landscape Report 2017, 18. januára 2018.

²⁹⁸ Ransomvér WannaCry využíval chyby v protokole operačného systému Microsoft Windows, ktoré umožňovali prevziať na diaľku kontrolu nad akýmkoľvek počítačom. Spoločnosť Microsoft po odhalení chyby vydala opravu. Státisíce počítačov však neboli aktualizované a mnoho z nich bolo neskôr infikovaných.

²⁹⁹ EUROPOL. Internet Organised Crime Threat Assessment 2020. Dostupné na internete.

Atraktívnou metódou sú **útoky prostredníctvom webu**, pomocou ktorých dokážu aktéri hrozby podviesť obeť tak, že ako vektor hrozby použijú webové systémy alebo služby. Zahŕňa možnosť rozsiahlych útokov, napríklad uľahčenie škodlivých URL alebo škodlivých skriptov s cieľom nasmerovať používateľa alebo obeť na požadovanú webovú stránku alebo sťahovanie škodlivého (útoky typu watering hole, útoky typu drive-by), a **vloženie** škodlivého kódu do legitímneho, ale ohrozeného webového sídla na krádež informácií (t. j. formjacking) na účely finančného zisku alebo krádeže informácií³⁰⁰.

Používateľov je možné zmanipulovať tak, aby nevedomky vykonali istú akciu alebo zverejnili dôverné informácie. Tento úskok sa môže použiť pri krádeži údajov alebo kybernetickej špionáži a je známy ako **sociálne inžinierstvo**. Existujú rozličné spôsoby, ako to dosiahnuť, bežnou metódou je však tzv. **phishing**, pri ktorom sa prostredníctvom e-mailových správ, ktoré vyzerajú, akoby pochádzali z dôveryhodných zdrojov, oklamú používateľa, aby prezradili informácie alebo klikli na odkazy, ktoré nakazia ich zariadenie stiahnutým malvérom. Vyše polovice členských štátov nahlásilo vyšetrovania týkajúce sa takýchto útokov na siete³⁰¹.

Asi najpohodlnejším druhom hrozieb sú **pokročilé pretrvávajúce hrozby**. Tieto hrozby sú dielom rafinovaných útočníkov, ktorí dlhodobo sledujú a kradnú údaje, niekedy s deštruktívnymi cieľmi. Ich cieľom je zostať čo najdlhšie neodhalení. Pokročilé pretrvávajúce hrozby sa často týkajú štátov a bývajú zamerané najmä na citlivé sektory, akými sú technológie, obrana a kritická infraštruktúra. Tento typ kybernetickej špionáže údajne predstavuje najmenej jednu štvrtinu všetkých kybernetických incidentov³⁰².

Model informačnej a kybernetickej bezpečnosti

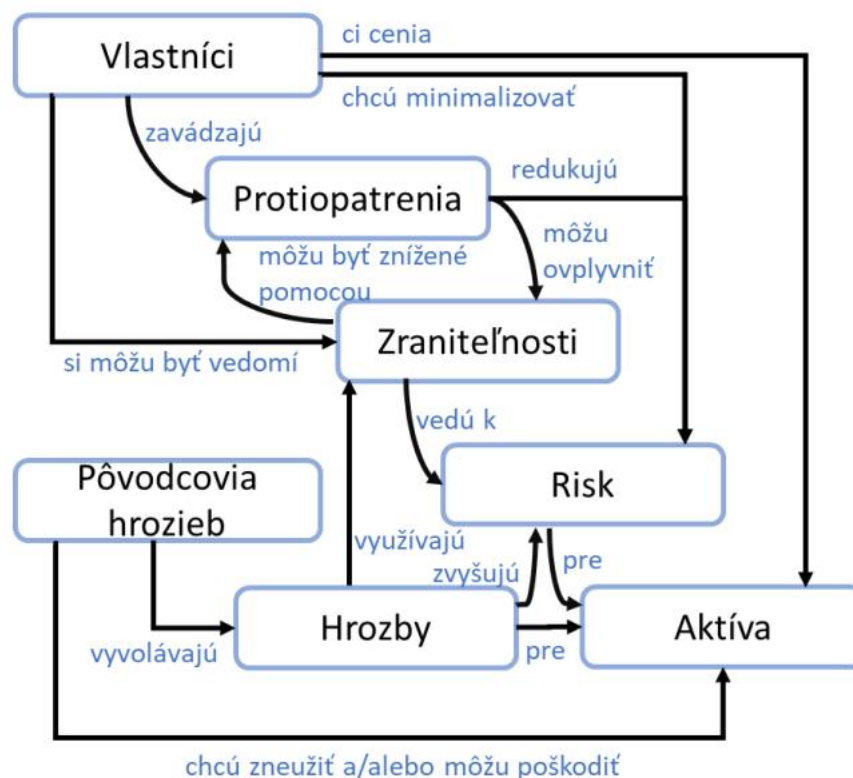
V oblasti informačnej aj kybernetickej bezpečnosti existuje viacero rôznych pojmov (napr. aktívum, hrozba, útok) a vzťahov medzi nimi. Pochopenie týchto vzťahov je dôležité pre pochopenie toho, čo kybernetická bezpečnosť je a akým spôsobom sa pristupuje k jej realizácii. Vzťahy medzi základnými pojmami kybernetickej bezpečnosti sú vyjadrené v modeli informačnej a kybernetickej bezpečnosti (Obrázok č. 4), ktorý upravuje norma ISO/IEC 15408 - 1:2005³⁰³. V ďalšej časti sa bližšie zameriame na jednotlivé pojmy z tejto oblasti a uvedieme viacero príkladov pre ich bližšie pochopenie.

³⁰⁰ ENISA. Threat Landscape 2021 – Web-based attacks, 20. októbra 2021. Dostupné na internete.

³⁰¹ EUROPOL, pozri vyššie, 2020.

³⁰² EUROPEAN CENTRE FOR POLITICAL ECONOMY, Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?, február 2018. Dostupné na internete.

³⁰³ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 15408-1: 2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.



Obrázok 5 Model informačnej bezpečnosti podľa normy ISO/IEC 15408-1:2005³⁰⁴

Zdroj: vlastné spracovanie podľa International Organization for Standardization, International Electrotechnical Commission. 2005.

Strategické aktíva organizácie

Cieľom informačnej a kybernetickej bezpečnosti je zabezpečiť to, čo má pre organizáciu hodnotu. „*Položku, vec alebo entitu, ktorá má pre organizáciu potenciálnu alebo skutočnú hodnotu označujeme*“ ako aktívum (asset)³⁰⁵. Aktíva je možné rozdeliť do viacerých skupín³⁰⁶, ktoré si nižšie popíšeme.

- Prvú skupinu predstavujú **informácie**. Tu môžeme zaradiť životne dôležité informácie pre plnenie poslania alebo činností organizácie, osobné údaje, strategické informácie alebo veľmi nákladné informácie, ktorých zhromažďovanie, skladovanie, spracovávanie vyžaduje veľa času alebo vysoké náklady.
- Druhú skupinu predstavujú **obchodné procesy a činnosti**. Do tejto skupiny môžeme zaradiť procesy, ktorých strata alebo obmedzenie neumožňuje plniť poslanie organizácie. Iným príkladom sú procesy, ktoré obsahujú obchodné tajomstvá alebo zahŕňajú duševné vlastníctvo, alebo ktorých zmena môže významne ovplyvniť plnenie poslania organizácie. Posledným príkladom sú procesy, ktoré sú pre organizáciu nevyhnutné, aby spĺňala zmluvné, právne alebo regulačné požiadavky.
- Tretiu skupinu aktív predstavuje **hardvér**. Pôjde najmä o zariadenia na spracovanie dát (napr. počítač), prenosné zariadenia (napr. notebook), pevné zariadenia (napr. server),

³⁰⁴ Ibid.

³⁰⁵ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 55000:2014 Asset management — Overview, principles and terminology.

³⁰⁶ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 7005:2018 Information technology — Security techniques — Information security risk management.

periférne zariadenia (napr. tlačiareň), dátové nosiče (napr. pevný disk, USB kľúč) alebo ostatné nosiče (napr. papier).

- d) Štvrtá skupiny aktív je tvorená rôznym **softvérovým vybavením**. Okrem operačných systémov (napr. operačný systém Windows 11) a podnikových aplikácií (napr. SAP) pôjde aj o iné aplikácie. Príkladom môže byť aj systém na správu webového obsahu alebo samotný kód webovej stránky organizácie (napr. ústredný portál verejnej správy). V súčasnosti sa množstvo služieb poskytuje prostredníctvom cloudových služieb a medzi aktíva môžeme zaradiť aj softvér pre správu cloudu, počítačovej siete.
- e) Do piatej skupiny aktív môžeme radiť **komunikačné siete**. Ide skôr o podporné aktívum, bez dostupnosti ktorého by bolo ohrozená funkčnosť systémov a prístup k informáciám. Ako príklad môžeme uviesť prenosové médium a jeho podpora (napr. optický kábel), pasívne alebo aktívne prenosové zariadenia (napr. WiFi smerovač - router) alebo samotné komunikačné rozhranie (napr. adaptér sieťovej karty na notebooku).
- f) Napokon šiestu skupinu aktív predstavujú **pracovníci** a ich know-how. Tu zaraďujeme napríklad osoby, ktoré rozhodujú o činnosti organizácie (napr. vedúci projektu), osoby v pozícii používateľov informačných systémov (napr. pracovník na personálnom oddelení), osoby v rámci prevádzky alebo údržby (napr. správca počítačovej siete) a vývojárov informačných systémov (napr. vývojár informačného systému na správu daní).

Príklady aktív je možné nájsť v rámci niekoľkých štúdií. Európska agentúra pre kybernetickú bezpečnosť (ENISA) publikovala viacero štúdií, v ktorých sa bližšie venuje popisu aktív. Ako príklad môžeme uviesť štúdiu organizácie ENISA z roku 2016, v ktorej sa zamerala na inteligentné nemocnice vrátane analýzy základných aktív pri poskytovaní zdravotnej starostlivosti. Následne v roku boli takto identifikované aktíva použité aj v štúdiu v roku 2018:

- aktíva systému vzdialenej starostlivosti - zdravotnícke vybavenie na diaľkové monitorovanie a diagnostiku (napr. monitory srdcového rytmu, glukomery),
- zdravotnícke pomôcky zapojené do počítačovej siete - implantovateľné alebo nositeľné zariadenia (napr. inzulínové pumpy, kardiostimulátory, stacionárne zariadenia ako MRI),
- identifikačné systémy - systémy na autentifikáciu a sledovanie pacientov, personálu a vybavenia (napr. náramky, inteligentné odznaky, biometrické štítky)
- sieťové vybavenie – IT vybavenie používané v zdravotníckych zariadeniach (napr. sieťové zariadenia, bezdrôtové vybavenie, počítače),
- mobilné klientske zariadenia - notebooky, smartfóny, tablety a aplikácie, na ktorých pracujú, prepojené klinické informačné systémy - špecifické systémy nasadené v zdravotníckych zariadeniach (napr. rádiologické informačné systémy),
- údaje - administratívne údaje o pacientovi, klinické údaje (napr. zdravotné záznamy, výsledky testov, anamnéza), fyzické vybavenie - budovy zdravotníckych zariadení, dodávka elektriny, klimatizácia atď.

Kybernetické útoky majú značný hospodársky dosah

Hrozba kybernetických útokov a počítačovej kriminality sa v posledných rokoch stala jednou z hlavných otázok. Už v roku 2016 80 % podnikov EÚ zažilo aspoň jeden kybernetický incident³⁰⁷. V roku 2018 40 % respondentov prieskumu z organizácií, ktoré využívajú robotiku alebo automatizáciu, uviedlo, že najkritickejším dôsledkom kybernetického útoku na ich

³⁰⁷ EUROPOL. Internet Organised Crime Threat Assessment 2020. Dostupné na internete.

systémy by bolo prerušenie prevádzky. Napriek informovanosti o rušivých kybernetických rizikách však spoločnosti často nemajú zavedený systém na ich riešenie³⁰⁸.

Odvtedy sa počet kybernetických útokov, ich závažnosť a finančné náklady ďalej zvyšovali. Pokiaľ možno odhadnúť jej finančný vplyv, počítačová kriminalita bude do roku 2021 stáť svetové hospodárstvo 6 biliónov USD ročne, čo je nárast z odhadovaných 3 biliónov USD v roku 2015³⁰⁹, v porovnaní s odhadovaným celosvetovým HDP vo výške 138 biliónov USD v roku 2020. Náklady počítačovej kriminality zahŕňajú poškodenie a zničenie údajov, ukradnuté peniaze, stratu produktivity, krádež duševného vlastníctva, krádež osobných a finančných údajov, narušenie riadneho priebehu podnikania po útoku či poškodenie dobrej povesti. Európsky výbor pre systémové riziká (ESRB) odhaduje, že priemerné náklady na kybernetické incidenty sa v rokoch 2015 až 2020 zvýšili o 72 %³¹⁰.

Z nedávnej štúdie z roku 2020³¹¹ vyplýva, že počítačová kriminalita ovplyvňuje rôzne hospodárske odvetvia rôznym spôsobom: bola najrušivejším podvodným javom vo vládnej sfére a verejnej správe, v sektoroch technológií, médií a telekomunikácií a v odvetví zdravotníctva a zároveň bola druhým najrušivejším podvodným javom vo finančnom sektore a v sektore priemyslu a výroby.

Fínski pacienti psychoterapie boli vydieraní pomocou osobných lekárskych údajov, ktoré boli ukradnuté v rokoch 2018 – 2019

Jednotlivých pacientov veľkej fínskej psychoterapeutickej kliniky s pobočkami po celej krajine, ktorých osobné údaje boli ukradnuté v novembri 2018, s ďalším možným narušením v marci 2019, oslovil v roku 2020 vydierač. Údaje zrejme obsahovali osobné identifikačné záznamy a poznámky o tom, čo sa hovorilo na terapeutických sedeniach.

Klinika aj pacienti mali vydieračovi zaplatiť výkupné v bitcoinoch, aby údaje neboli zverejnené. Incident viedol fínsku vládu k zorganizovaniu mimoriadneho stretnutia³¹².

V roku 2019 EUROPOL³¹³ opäť zdôraznil pretrvávajúce a pevnosť viacerých kľúčových hrozieb v oblasti počítačovej kriminality:

- najvyššou hrozbou zostávajú útoky ransomvérom, sú čoraz presnejšie zacielené, ziskovejšie a spôsobujú väčšie hospodárske škody. Pokiaľ bude ransomvér zabezpečovať páchatelom počítačovej trestnej činnosti pomerne jednoduchý príjem, zrejme zostane najvyššou hrozbou počítačovej kriminality,
- kľúčovými hlavnými vektormi infekcie malvérom sú phishing a zraniteľné protokoly vzdialeného počítača (RDP) a o hlavným cieľom, komoditou a umožňujúcim faktorom počítačovej kriminality zostávajú údaje.

Podobne Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) vo svojej správe z roku 2020 s názvom Main incidents in the EU and worldwide³¹⁴ uvádza niekoľko príkladov kybernetických incidentov.

³⁰⁸ PWC, Global State of Information Security (GSISS) Survey – Strengthening digital society against cyber shocks, 2017. Dostupné na internete.

³⁰⁹ CYBERSECURITY VENTURES, 2019 Official Annual Cybercrime Report, 2019. Dostupné na internete.

³¹⁰ EURÓPSKY VÝBOR PRE SYSTÉMOVÉ RIZIKÁ, Systemic cyber risk, February 2020. Dostupné na internete.

³¹¹ PWC, Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey, 2020.

³¹² BBC NEWS, Therapy patients blackmailed for cash after clinic data breach, 26. októbra 2020. Dostupné na internete.

³¹³ EUROPOL. Internetet organised crime threat assessment (IOCTA), 2019. Dostupné na internete.

³¹⁴ ENISA, Main incidents in the EU and worldwide – January 2019 to April 2020, október 2020. Dostupné na internete.

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA): kybernetické bezpečnostné incidenty v rokoch 2019 – 2020

E-mailovú platformu verifications.io postihlo veľké porušenie ochrany údajov, ktorého príčinou bola nechránená databáza MongoDB. Zverejnené boli údaje z viac ako 800 miliónov e-mailov, ktoré obsahovali citlivé informácie vrátane informácií o totožnosti.

Na obľúbenom hackerskom fóre, ktorého hostiteľom je cloudová služba MEGA1, bolo zverejnených viac ako 770 miliónov e-mailových adries a 21 miliónov jedinečných hesiel. Stali sa najvýznamnejším súborom narušených osobných prvkov v histórii, ktorý dostal pomenovanie Collection #1 (Zbierka č. 1).

Obetou cieleného kybernetického útoku sa stala spoločnosť Citrix, ktorá je poskytovateľom cloudu a virtualizácie. Na získanie prístupu do systémov spoločnosti Citrix útočníci využili viacero kritických zraniteľných miest softvéru, napríklad CVE-2019 – 19781, a použili techniku tzv. password spraying.

Poskytovateľ hostiteľských služieb pre cloud iNSYNQ19 sa stal obeťou útoku ransomvérom, po ktorom zákazníci viac ako týždeň nemali prístup k svojim údajom a boli nútení využívať miestne zálohy.

ZÁVER

Rozvoj technológií so sebou neprináša len pozitívne stránky a výhody. Zber údajov a následné spracovanie na jednom mieste je efektívnejšie a môže pozitívne ovplyvniť spoločnosť a ľudské životy. Na druhej strane ale zvyšuje pravdepodobnosť, že dôjde k zneužitiu týchto údajov a tiež samotný dopad takého zneužitia (vzhľadom na akumulované množstvo dát). Systém, na ktorom bude závislý ľudský život, síce výrazne pomáha pri zdraví a živote ľudí, ale súčasne sa stáva niečím, čo predtým nebolo v takejto miere dôležité.

Zdroje

1. ANDRAŠKO, J. – MESARČIK, M. – SOKOL, P. Právo kybernetickej bezpečnosti. 1. vyd. Bratislava: UK BA, PF, 2022, 186 s. ISBN 978-80-7160-632-1
2. ANDRESS J. Foundations of Information Security: A Straightforward Introduction. No Starch Press, 2019. 248 s. ISBN 9781718500044
3. BBC NEWS. Therapy patients blackmailed for cash after clinic data breach, 26. októbra 2020. [online] [11.7.2023]. Dostupné na: <https://www.bbc.com/news/technology-54692120>
4. CYBERSECURITY VENTURES. 2019 Official Annual Cybercrime Report, sponzorovaná spoločnosťou Herjavec Group, 2019. [online] [2.6.2023]. Dostupné na: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>
6. DEATH D. Information security handbook: develop a threat model and incident response strategy to build a strong information security framework. Packt Publishing Ltd; 2017. 330 s. ISBN 978-1788478830
7. ENISA, Main incidents in the EU and worldwide – January 2019 to April 2020, október 2020. [online] [21.3.2023]. Dostupné na: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents>
8. ENISA. Threat landscape report 2018. Január 2019, [online] [21.3.2023]. Dostupné na: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>.
9. ENISA: Threat Landscape 2021. Október 2021, [online] [21.3.2023]. Dostupné na: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>.
10. EURÓPSKY VÝBOR PRE SYSTÉMOVÉ RIZIKÁ, Systemic cyber risk, February 2020. [online] [1.6.2023]. Dostupné na:

- https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
11. EUROPEAN CENTRE FOR POLITICAL ECONOMY, Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?, občasník č. 2/18, február 2018. [online] [21.3.2023]. Dostupné na: <https://ecipe.org/publications/stealing-thunder/>
 12. EUROPOL. Internetet organised crime threat assessment (IOCTA), 2019. [online] [21.3.2023]. Dostupné na: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019>
 13. EUROPOL. Internet organised crime threat assessment (IOCTA) 2020, [online] [21.3.2023]. Dostupné na: https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.
 14. EURÓPSKY PARLAMENT, Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, štúdia pre Výbor pre občianske slobody, spravodlivosť a vnútorné veci (LIBE), september 2015. [online] [21.3.2023]. Dostupné na: [https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU\(2015\)536470_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf)
 15. FLORES M. The Language of Cybersecurity. London: XML Press, 2018. 188 s. ISBN 978-1937434625
 16. GRAHAM, J. - HOWARD, R. - OLSON, R. (eds.) Cyber Security Essentials. Boca Raton: CRC Press, 2011. ISBN 978-1-4398-5123-4.
 17. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27000: 2018 - Information technology—Security techniques—Information security management systems—Overview and vocabulary.
 18. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27032: 2012 – Information technology—Security techniques—Guidelines for cybersecurity.
 19. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management.
 20. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 55000:2014 Asset management — Overview, principles and terminology.
 21. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, International Electrotechnical Commission. ISO/IEC 15408-: 2005 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
 22. PWC, Global State of Information Security (GSISS) Survey – Strengthening digital society against cyber shocks, 2017. [online] [21.5.2023]. Dostupné na: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory.html>
 23. REID, R. C., GILBERT, A. H.: Using the Parkerian Hexad to introduce security in an information literacy class. In: 2010 Information Security Curriculum Development Conference. ACM, 2010. [online] [21.3.2023]. Dostupné na: <https://doi.org/10.3390/app12105037>
 24. VON SOLMS R., VAN NIEKERK J.: From information security to cyber security. Computers & security. 2013. [online] [21.3.2023]. Dostupné na: <https://doi.org/10.1016/j.cose.2013.04.004>

PROCESNÁ ANALÝZA V BOJI PROTI HYBRIDNÝM HROZBÁM

doc. RNDr. Vladimír Špitalský, PhD., Ing. Ľubomír Török, PhD.

Beset, spol. s r.o.; Jelenia 18, 811 05 Bratislava; {vladimir.spitalsky, lubomir.torok}@beset.sk

Abstrakt: Procesná analýza sa zaoberá analýzou procesov v podniku a primárne sa zameriava na optimalizáciu nákladov, kvality a rýchlosti výstupu. Jej základy siahajú do deväťdesiatych rokov minulého storočia a behom niekoľkých rokov bola prijatá za štandard v oblasti riadenia podnikov. S postupným vývojom informatizácie v podnikoch sa prirodzene vyskytli otázky ako identifikovať a ďalej optimalizovať procesy, ktoré popisujú fungovanie podniku. Tieto otázky položili základy pre vznik process miningu – vednej disciplíny, ktorá sa zaoberá objavovaním procesov v bežiacom systéme popísanom sériou udalostí. Predkladaný príspevok je skrátenou verziou článku, ktorý je venovaný koncepcii aplikácie poznatkov procesnej analýzy a process miningu vo všeobecnom systéme s cieľom identifikácie neštandardného chovania sa systému, detekcie odchýlok a odhaľovaniu potenciálnych hrozieb pokusov o útok na samotný systém. Napriek tomu, že spomínané disciplíny sa zaoberajú hlavne podnikmi a optimalizáciou procesov v nich, je možné tieto koncepcie využiť aj na analýzu všeobecných systémov, ktorých fungovanie je popísané žurnálom s udalosťami. Preto je možné postupy z oboch oblastí aplikovať aj na systémy v kybernetickom priestore – od informačných systémov, cez sociálne siete až po jednotlivé pracovné stanice prípadne sieťové zariadenia. V článku priblížime základné pojmy a postupy s návrhom ich jednoduchých modifikácií s cieľom identifikovať neštandardné správanie sa v systéme, ktoré môže pre samotný systém predstavovať hrozbu v podobe bezpečnostného incidentu prípadne zvýšenie intenzity neželaných aktivít. Tým priamo poukazuje na využitie predstavených konceptov v boji proti hybridným hrozbám.

KLúčové slová: proces, analýza, process mining, hybridná hrozba, conformance, incident, bezpečnosť, systém, podnik.

ÚVOD

Bezpečnostné systémy v organizáciách prešli za posledné roky zaujímavým vývojom. Jednotlivé typy bezpečnostných systémov, ako sú napríklad kamerový, dochádzkový, zabezpečovací a iné, je možné spolu integrovať do systému, ktorý dokáže komunikovať s každým z nich. Na trhu je niekoľko riešení tohto typu. Ich hlavnou úlohou je zbierať údaje z jednotlivých systémov, ktoré často pochádzajú od rôznych dodávateľov, agregovať tieto údaje na jedno miesto a jednotlivé systémy ovládať z centrálnej konzoly. Výhodou agregácie údajov z niekoľkých systémov do jedného je širší pohľad na zozbierané údaje a možnosť ich jednoduchšej analýzy. Vývojom prešli aj samotné systémy – kamerové systémy už bežne obsahujú prvky umelej inteligencie, ktoré umožňujú rozpoznávať osoby a predmety na zaznamenanom obraze. Systémy na monitoring komunikačných sietí sa priebežne „učia“ z bežnej prevádzky, vďaka čomu vedia presnejšie identifikovať neštandardné správanie na sieti a odhaľovať potenciálne hrozby. Stále však platí, že súhrnnú analýzu nad všetkými systémami realizuje operátor, ktorý vyhodnocuje podnety z jednotlivých systémov v celkovom kontexte prevádzky organizácie.

Typickým príkladom hrozby, ktorú vie vyhodnotiť len operátor v kontexte hlásení zo všetkých bezpečnostných systémov, je prihlásenie sa používateľa správnymi, ale ukradnutými prihlasovacími údajmi. Takáto udalosť prejde monitoringom siete bez povšimnutia, lebo nie je nijak podozrivá. Ak by však operátor vedel identifikovať, že daný používateľ neprešiel dochádzkovým systémom, že kamerový systém z parkoviska nehlásil príchod auta s jeho evidenčným číslom, úspešné prihlásenie sa do systému údajmi používateľa, ktorý pravdepodobne neprišiel na pracovisko, naberaá úplne iný rozmer.

V tomto článku sa pozrieme na dostupné riešenia, ktoré by vedeli pomôcť pri identifikácii bezpečnostných incidentov na základe analýzy správania sa systému popísaného pomocou udalostí z rôznych zdrojov. Udalosti môžu mať svoj pôvod napríklad v operačnom systéme počítača, v informačnom systéme, v monitoringu komunikačnej siete. Väčšina podnikov používa nástroje tohto typu, takže monitoring udalostí v bezpečnostných systémoch, komunikačnej sieti, informačných systémoch, ale aj jednotlivých pracovných staniciach a hardvérových zariadeniach nám poskytuje množstvo informácií o tom, čo sa v podniku deje a analýzou takýchto udalostí nepriamo analyzujeme aj fungovanie podniku samotného. Cieľom článku je poukázať na možnosti využitia koncepcií z analýzy procesov a process mining v oblasti bezpečnosti a identifikácie neštandardného chovania sa sledovaného systému.

Dôvodom pre výber a analýzu postupov z oblasti process mining je možnosť ich aplikácie na široké spektrum systémov. Riadenie podnikov postavené na procesoch má svoje počiatky v deväťdesiatych rokoch minulého storočia ¹. Postupne sa stávalo čoraz populárnejším a ako si podniky prešli informatizáciou, vynorili sa otázky ohľadom automatizovaného identifikovania procesov v podniku, za účelom optimalizácie nákladov, zvýšenia kvality výstupu, prípadne zrýchlenia výroby. Keď boli procesy organizácie popísané, vznikla potreba kontroly reálneho behu podniku voči formálne popísaným procesom, pričom procesy podniku boli formálne popísané napríklad pomocou BPMN diagramov ². Tieto základné otázky – identifikácia procesov v bežiacom systéme a overenie reálnych procesov v systéme voči navrhnutým procesom položili základ výskumu v oblasti process mining ³. Process mining spadá do oblasti dátových vied a prepája oblasť procesného modelovania a biznis inteligencie. Základným pojmom, s ktorým sa pri process mining pracuje, je udalosť. Metódy process miningu predpokladajú, že je k dispozícii záznam správania sa systému vo forme udalostí, pričom udalosť je charakterizovaná len niekoľkými základnými atribútmi: časom, typom udalosti, prípadom. Síce sa stále jedná o procesy v podniku, ale abstrakcia pohľadu cez udalosti nám umožňuje analyzovať akýkoľvek systém, ktorého beh dokážeme sledovať ako sekvenciu udalostí, ktoré v ňom vznikli. Preto sa v tomto článku pozrieme na metódy process miningu aj v kontexte všeobecných systémov. Sústreďme sa hlavne na kybernetický priestor – počítače, siete, informačné systémy a aplikácie.

V poslednom období sa stupňuje intenzita útokov v kybernetickom prostredí, v neregulovanom prostredí sociálnych médií sa šíria informácie s pochybným pôvodom, ktoré spôsobujú polarizáciu v spoločnosti a to nielen v súvislosti s vojnovým konfliktom na Ukrajine. Kybernetické útoky a šírenie dezinformácií spadajú pod súhrnný pojem hybridné hrozby. Pojem hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť cieľ ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni ⁴. Naším cieľom teda bude poukázať na možnosti využitia procesnej analýzy správania sa systému a poznatkov z oblasti process mining v boji proti hybridným hrozbám. Predpokladáme pri tom, že skúmaný systém generuje štruktúrované informácie o udalostiach, ku ktorým v ňom dochádza počas jeho aktivity.

1. ZÁKLADNÉ POJMY

1.1 Procesy

Vo všeobecnosti je proces prirodzene sa vyskytujúca alebo umelo vytvorená postupnosť zmien vlastností objektu alebo systému. V prípade, že sa sústreďme na procesy v rámci organizácie, môžeme podnikový proces definovať ako *objektívne prirodzenú postupnosť činností konaných s úmyslom dosiahnutia daného cieľa v objektívne daných podmienkach* ⁵. V tomto článku sa budeme zaoberať procesmi, ktoré je možné identifikovať v systémoch, ale nie sú nutné

explicitne popísané. Zaujímajú nás totiž aj procesy, ktoré sú súčasťou bežného fungovania systému, ale nemusia priamo súvisieť s napĺňaním jeho cieľov akými sú napríklad výroba, alebo poskytovanie služieb.

1.2 Udalosti

Ako sme spomínali v úvode, predpokladáme, že skúmaný systém počas svojej aktivity vytvára záznamy o zmenách, ktoré sa v ňom dejú. V oblasti IT riešení sa záznamy o behu systému zapisujú do žurnálu (v anglickom jazyku sa používa výraz „log“). Je to bežná prax, ktorá nám dáva k dispozícii informácie o tom, čo sa kedy v systéme udialo a kto danú udalosť spôsobil. Nedá sa však očakávať, že záznamy o behu systému budú v rôznych systémoch vyzerieť rovnako a že budú k dispozícii v rovnakej forme alebo štruktúre. Pre potreby rigorózneho analýzy údajov z behu systému je však potrebné vytvoriť základnú definíciu, ktorá bude určovať, aké minimálne informácie musí záznam o behu systému obsahovať, aby ich bolo možné ďalej analyzovať. Základným pojmom, s ktorým budeme ďalej pracovať, je pojem udalosť. *Udalosť definujeme ako zmenu vlastností alebo atribútov v systéme, ktorá je popísaná časom svojho vzniku, prípadom a typom.*

Pod prípadom pritom rozumieme napríklad inštanciu procesu, v rámci ktorého došlo ku danej udalosti, inštanciu procesu vykonávanú konkrétnym používateľom, prípadne pre konkrétneho zákazníka. Okrem uvedených nutných vlastností, môže udalosť obsahovať dodatočné informácie, ktoré môžu byť použité pre účely presnejšieho spracovania pri konkrétnom prípade použitia. Vo všeobecnosti ale od udalosti očakávame, že budeme vedieť o nej povedať, o akú udalosť sa jedná, kedy vznikla, a prípad jej vzniku.

Žurnál systému môže obsahovať aj množstvo iných informácií, ktoré sa môžu týkať stavu systému v danom momente. Preto je veľmi často potrebné žurnál nejakým spôsobom spracovať tak, aby výsledkom spracovania bola len množina udalostí, ktorá je relevantná pre účely vybranej analýzy.

1.3 Spracovanie žurnálu

Problematika zberu udalostí z rôznych zdrojov a v rôznych formátoch, ich unifikácia a agregácia na jedno miesto nie je v oblasti IT riešení nijak nová. V bežnej praxi prevádzky systémov je veľmi často potrebné mať žurnálové záznamy k dispozícii v jednotnom formáte na jednom mieste kvôli rýchlym a jednoduchším analýzám udalostí v jednotlivých systémoch. Na tento účel slúžia nástroje, ktorých cieľom je konverzia žurnálov z rôznych zdrojov na jednotný formát. Každá technológia, ktorá sa v súčasnosti využíva pre vývoj IT systémov, obsahuje nejakú podporu pre vytváranie žurnálov. Zaužívané konvencie v praxi znamenajú, že aj prípadné konverzie na iné formáty nie sú náročnou úlohou. Väčšinu týchto konverzií zabezpečia nástroje pre spracovanie žurnálov, a v prípade, že daný formát nepodporujú, poskytujú možnosť implementácie vlastného konvertora. Účelom tohto článku nie je analyzovať tieto nástroje. Čitateľovi ale môžeme odporučiť napríklad prehľad voľne dostupných nástrojov pre spracovanie žurnálu na odkaze ⁶.

1.4 Process mining

V praxi sa process mining využíva hlavne v situáciách, kedy je popis procesov v systéme nedostatočný, prípadne ho nie je možné získať inými spôsobmi. V našej koncepcii využitia metód process miningu máme niekoľko cieľov:

1. Získať popis správania sa sledovaného systému.
2. Identifikovať odchýlky od bežného správania sa systému.
3. Overiť, či explicitne popísané procesy prebiehajú v systéme podľa svojho popisu.

V analýze správania sa systému prostredníctvom metód process miningu sa nebudeme zameriavať na optimalizáciu existujúcich procesov, čo je hlavný cieľ process miningu, ale skôr na identifikáciu vzťahov medzi udalosťami v systéme, získanie prehľadu o fungovaní systému ako celku a detekciu neštandardného správania sa v systéme. Metódy process miningu pokrývajú dve hlavné oblasti:

1. Vyhľadanie procesov v systéme (Process Discovery)
2. Overenie procesov v systéme voči ich formálnym návrhom (Conformity test)

Triedy algoritmov, ktoré sa zaoberajú objavovaním procesov v systéme nám poslúžia na splnenie prvého cieľa – získania popisu sledovaného systému ako celku. Podrobnejšie si ich popíšeme v nasledujúcej podkapitole.

1.5 Vyhľadávanie procesov

Vyhľadávanie, alebo objavovanie procesov, je prvým krokom v process miningu. Jeho hlavným cieľom je transformácia žurnálu s udalosťami do procesného modelu. Prvým algoritmom pre získanie náhľadu do kauzality jednotlivých udalostí v žurnále je Alfa algoritmus, ktorý z udalostí v žurnále vytvorí Petriho sieť⁷ reprezentujúcu následnosti jednotlivých udalostí.

Takýmto prístupom vieme zmapovať chovanie sa systému, nájsť opakujúce sa sekvencie, ktoré v systéme identifikujú nejaké zaužívané procesy a následne tento systém monitorovať a v určitých časových intervaloch vyhodnocovať, či sa stále správa štandardne.

1.6 Kontrola konformity

V tejto časti predpokladáme, že máme k dispozícii explicitne popísané procesy v systéme a chceme overiť, či sa procesy v reálnej prevádzke systému dodržia podľa popisu. Hlavnou motiváciou pre tento typ kontroly je overenie, či reálne vykonávané procesy v systéme dodržia pravidlá nastavené manažmentom, vládou, prípadne inými zainteresovanými entitami. Jedná sa o audit fungovania systému a jeho výsledkom môže byť odhalenie sprenevery, bezpečnostných incidentov, alebo zneužitia systému.

Analýza bude opäť postavená na tom, že máme k dispozícii žurnál s udalosťami z reálnej prevádzky systému a BPMN modely procesov, ktoré chceme v reálnej prevádzke systému kontrolovať. Výstupom takejto kontroly je vyjadrenie zhody reálne bežiaceho procesu voči jeho návrhu v BPMN diagrame, čo je základný koncept kontroly konformity (Conformance Checking).

BPMN diagram sa využíva ako vstup z toho dôvodu, že v praxi sa jedná o najpoužívanější spôsob zápisu procesov v biznis aj technickom prostredí. Jeho základný problém je, že sa nedá formalizovať, preto sa v analýzach využívajú skôr Petriho siete, ktoré majú formálnu sémantiku a modely nimi popísané sa dajú formálne overiť. Konverzia BPMN diagramu na Petriho sieť sa dá realizovať rôznymi postupmi⁸.

Medzi základné metódy pre kontrolu konformity patria:

1. Porovnanie matice odtlačkov (footprint matrix⁹) žurnálu a modelu
2. Token-replay¹⁰ algoritmus na Petriho sieti zodpovedajúcej modelu
3. Alignments¹¹ algoritmus

Náš cieľ sa trochu líši od účelu využitia testu konformity. Síce je pre nás zaujímavé vedieť, ako presne sa dohodnuté procesy dodržia v praxi, ale zaujímajú nás hlavne situácie, kedy reálny proces v systéme nezbehná podľa návrhu. Všetky tri algoritmy ale analyzujú žurnál udalostí po jednotlivých identifikovaných sekvenciách, takže nie je problém algoritmy modifikovať tak, aby sekvencie udalostí zo žurnálu, ktoré nekorešpondujú s navrhnutým procesom, nejakým vhodným spôsobom označili a umožnili tak ich podrobnejšiu analýzu za účelom identifikácie potenciálnej hrozby pre systém, prípadne bezpečnostného incidentu. Naopak, v prípade, že sa jedná o jav, ktorý súvisí s očakávaným vývojom systému v čase a nepredstavuje hrozbu, je možné ho zaradiť medzi štandardné vzorce chovania sa sledovaného systému.

ZÁVER

V tomto článku sme si priblížili process mining a možné využitie jeho metód v oblasti monitoringu systému s cieľom odhaľovať neštandardné chovanie v systéme. Prevádzka systému bola v našich analýzach popísaná len žurnálom s udalosťami, ktoré v systéme vznikali. Udalosti boli popísané len niekoľkými základnými atribútmi, akými sú čas vzniku udalosti, jej pôvodca a typ udalosti. S trochou práce je možné takýto žurnál vytvoriť aj z bežných logových záznamov informačných systémov a metódy process miningu využiť na ich analýzu.

Druhým hlavným smerom výskumu v oblasti process mining je testovanie konformity reálnej prevádzky systému voči procesnému modelu. V plnej verzii článku prezentujeme dve metódy: porovnanie matíc odtlačkov a token-replay algoritmus na Petriho sieti skonštruovanej z procesného modelu. V oboch prípadoch navrhujeme jednoduché modifikácie algoritmov, ktorých účelom je poukázať na odlišnosti v chovaní sa systému v porovnaní s modelom s cieľom identifikovať potenciálne incidenty v prevádzke systému.

Aplikácia spomenutých postupov v oblasti boja proti hybridným hrozbám primárne pokrýva hlavne kybernetický priestor. Tým, že predpokladáme analýzu udalostí, systém ich musí nejakým spôsobom generovať – čím sa automaticky dostávame do oblasti informačných technológií. Môžeme tak identifikovať odchýlky v správaní sa informačných systémov záujmových podnikov a identifikovať tak pokusy o hacking, útoky v kybernetickom priestore, prípadne priemyselnú špionáž. Používanie metód z oblasti process mining má tú výhodu, že množstvo podnikov (a tým aj informačných systémov, ktoré využívajú), majú v menšej či väčšej miere popísané interné procesy. Pre zvýšenie bezpečnosti a ochrany je možné ďalšie procesy dodefinovať tak, aby ich následný monitoring bol prínosom pre celkovú bezpečnosť systému, prípadne tieto procesy identifikovať priamo zo vzorky bezpečných udalostí z bežiaceho systému pomocou metód process miningu pre objavenie procesov.

Zdroje

1. Hammer M, Champy J. *Reengineering Corporation*. Harper Business; 1993.
2. Business Process Model and Notation. <https://www.omg.org/spec/BPMN>
3. van der Aalst WMP. *Process Mining*. Springer; 2016.
4. NBÚ. Hybridné hrozby. <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html>

5. Řepa V. *Procesně Řízená Organizace*. Grada Publishing; 2012.
6. Ankush. 10 Open Source Log Collectors for Centralized Logging. Published 2023.
<https://geekflare.com/open-source-centralized-logging>
7. Petri C, Reisig W. Petri net. *Scholarpedia*. 2008;3(4):6477. doi:10.4249/scholarpedia.6477
8. Lohman N, Verbeek E, Dijkman R. Petri Net Transformations for Business Processes - A Survey. Jensen WMP K, van der Aalst, ed. *Transactions on Petri Net and Other Models of Concurrency II, Lecture Notes in Computer Science*. Published online 2009:46-63.
9. Van Der Aalst W, Weijters T, Maruster L. Workflow mining: discovering process models from event logs. *IEEE Trans Knowl Data Eng*. 2004;16(9):1128-1142.
doi:10.1109/TKDE.2004.47
10. Van Der Aalst W. Data Science in Action. In: *Process Mining*. Springer Berlin Heidelberg; 2016:3-23. doi:10.1007/978-3-662-49851-4_1
11. Van Der Aalst W, Adriansyah A, Van Dongen B. Replaying history on process models for conformance checking and performance analysis. *WIREs Data Min & Knowl*. 2012;2(2):182-192. doi:10.1002/widm.1045

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

ÚLOHA BEZPEČNOSTNÍHO MANAGEMENTU PŘI IDENTIFIKACI A PREVENCI PROJEVŮ EXTRÉMISMU JAKO SPECIFICKÉ HYBRIDNÍ HROZBY

doc. PhDr. Barbora Vegrachtová, Ph.D., Ing. Bc. Eduard Slad

ČVUT Praha, Jugoslávských partyzánů 3, 160 00 Praha, AMBIS Praha, a.s. Vysoká škola, Lindnerova 1, 180 00 Praha

Abstrakt: Tento příspěvek přispívá k úloze bezpečnostního managementu při prevenci projevů politického extremismu jako specifické hybridní hrozby. Příspěvek rozebírá potenciál osobních a společenských důvodů a příčin politického extremismu a poukazuje na to, že projevy politického extremismu pronikají přes konkrétní osoby do struktur ozbrojených sil a jsou významným destabilizačním faktorem jejich činnosti. V závěru příspěvku jsou navrženy obecné principy a přístupy k řešení tohoto aktuálního fenoménu naší doby.

Klíčová slova: ozbrojené síly, frontierství, hybridní hrozba, politický extremismus, prevence, bezpečnostní management, terorismus, vigilantismus.

ÚVOD

Projevy politického extremismu jsou aktuálním fenoménem současného globálního světa, přičemž stoupající tendence politické (či jiné) nesnášenlivosti až extremismu nabývají lokálně takových rozměrů, že způsobují velmi napjaté vztahy mezi státy či národy a vytvářejí napjatou mezinárodně politickou a obecně společenskou situaci. Důvody politického napětí a politického extremismu mezi státy jsou různé, ale dá se říci, že převažují důvody národnostní, geopolitické, rasové a náboženské. Tento stav však vede jak k nedůvěře až nepřátelství jak mezi jednotlivými státy EU, tak i k projevům nesnášenlivosti mezi konkrétními osobami či skupinami osob bez ohledu na státní příslušnost a je způsobilý dokonce navodit destabilizaci vnitřní bezpečnosti ve státě. V poslední době je obzvlášť markantní nárůst politického extremismu a jeho projevů, obzvlášť v zemích střední Evropy, Českou republiku a Slovensko nevyjímaje. Tyto projevy jsou charakteru od vypjatého vigilantismu až po otevřený rasismus a xenofobii v pojetí soudobého extremismu převážně vnitrostátního jednotlivých zemí EU, až po drobné provokace a narušování tradičně dobrých sousedských vztahů mezi sousedními zeměmi. Všechny tyto i další aktivity politických extremistů jsou možným zdrojem destabilizace zejména vnitřní bezpečnosti státu. Specifickým problémem pak jsou projevy extremismu v rámci soubory hybridních hrozeb. Specifickým projevem je frontierství a vigilantismus. Hovoří o tom veřejně známé i ty před veřejností utajené incidenty, resp. projevy extremismu. Zde je míněn zejména pravicový politický extremismus. Z pohledu tohoto článku lze hybridní hrozby chápat jako kombinaci různých prostředků, technik, aktivit a nástrojů, které mají za cíl destabilizovat nebo ochromit cílovou strukturu; v našem případě tedy stát a zejména jeho kritickou infrastrukturu, nebo způsobit politickou či jinou destabilizaci zásadních funkcí státu. Může se jednat jak kybernetické útoky, šíření propagandy, sabotáže apod.

1. POJEM „EXTRÉMISMUS“

Velmi často se lze setkat s veřejným prohlášením novináře či politika, že nějaká akce, nějaký symbol, popřípadě nějaký postoj je extrémní, nebo extremistický. Co to však extremismus je, jak se projevuje, kde jsou jeho kořeny a kdo je tedy extremistou a z jakého pohledu? Tento fenomén současné doby je hoden vědeckého zkoumání a hodnocení. Současně je také nezbytně nutno tento fenomén jasně a zřetelně pojmenovat, resp. pojmenovat jeho příčiny a mít řešení, nebo se alespoň o to snažit. Na extremismus lze nahlížet z různých pohledů zkoumání,

z pohledu vzniku projevů extremismu, z pohledu možného rozdělení extremismu, či z pohledu řešení projevů extremismu a reakcí společnosti. Dílčích pohledů na uvedený fenomén je však možných mnohem více, a to zcela ve smyslu multidisciplinarity uvedeného fenoménu. Extremismus lze vnímat jako sociologický, politologický či psychologický, ale zejména jako právní fenomén. Je však třeba na fenomén extremismu nahlížet z multidisciplinárního, resp. interdisciplinárního komplexního hodnocení a možného řešení.

2. DĚLENÍ A DEFINICE EXTRÉMISMU

Extremismus bývá dělen na extremismus *politický*, *náboženský*, *národnostní (rasový)*, *ekologický* a někdy se setkáme i s jiným dělením, resp. identifikací. Tato dělení jsou však namnoze pouze snahou o bližší specifikaci konkrétního projevu, nicméně extremismus, resp. extrémní postoj má jen jednu definici, resp. jeden společný jmenovatel. Zde lze vycházet z definice, která se sice může zdánlivě jevit jako poněkud starší, nicméně se jedná o stále platnou a užívanou definici. Tato definice byla poprvé ve své podobě použita (již) ve „Zprávě o problematice extremismu na území České republiky v roce 2002“, avšak je v odborných kruzích užívaná do současnosti.

Pojmem „extremismus“ jsou označovány vyhraněné ideologické postoje, které vybočují z ústavních, zákonných, norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku (nebo obecněji jako principy jako obsažené v Deklaraci práv a svobod). [1]

Mezi tyto principy patří zejména úcta k právům a svobodám člověka a občana (čl. 1 Ústavy ČR), svrchovaný, jednotný a demokratický právní stát (čl. 1 Ústavy ČR), nezměnitelnost podstatných náležitostí demokratického právního státu (čl. 9 odst. 2 Ústavy ČR), svrchovanost lidu (čl. 2 Ústavy ČR), soutěž politických stran respektujících základní demokratické principy a odmítajících násilí jako prostředek k prosazování svých zájmů (čl. 5 Ústavy ČR), ochrana menšin při rozhodování většiny (čl. 6 Ústavy ČR), svoboda a rovnost lidí v důstojnosti a právech, nezadatelnost, nezcizitelnost, nepromlčitelnost a nezrušitelnost základních práv a svobod bez rozdílu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického nebo jiného smýšlení, národního a sociálního původu, příslušnosti k národnosti nebo etnické menšině, majetku, rodu nebo jiného postavení (čl. 1, čl. 3 Listiny základních práv a svobod). Vzhledem k principiálně obdobným základům Ústavního práva, vč. začlenění Deklarace práv a svobod (Listiny práv a svobod) do Ústavních systémů v drtivé většině zemí Evropy, je možno výše uvedené zobecnit na všechny země v rámci střední a západní kontinentální Evropy. Jedná se o zájem chráněný státem, a to ve formě zejména trestních předpisů, resp. konkrétních skutkových podstat. Porušení těchto práv občanů (ve formě trestních deliktů) bývají též někdy nazývány jako tzv. „**trestné činy z nenávisti**“. Klíčovou úlohu v prevenci těchto jevů má pak bezesporu management a leadři Armády České republiky.

3. POLITICKÝ EXTRÉMISMUS

Politický extremismus je pak v souladu s platnými oficiálními dokumenty v tomto článku chápán jako pojem, který označuje „vyhraněné ideologické postoje, které vybočují z ústavních, zákonných, norem, vyznačují se prvky netolerance, a útočí proti základním demokratickým ústavním principům, jak jsou definovány v českém ústavním pořádku“. Základní členění je extremismus pravicový (neonacismus, český nacionalismus) a levicový (dogmatický komunismus, anarchismus), přičemž jednotlivé varianty pravicového extremismu budou zmíněny dále.

Politický extremismus je často vymezen jako určitý abstraktní prostor politického spektra a je třeba vnímat, že do skutečné politiky jej vnášejí až konkrétní aktéři. Jsou jimi především politické strany, zájmové skupiny (působící registrovaně i neregistrovaně, případně otevřeně i skrytě, přičemž skrytá působnost je charakteristická i pro různá extremistická spiklenecká centra), média, subkultury (zvláště subkultury mládeže, resp. jejich vnitřní proudy). Celkově pak extremisté mohou tvořit hnutí, resp. sociální hnutí, jakým byl např. ve dvacátých a třicátých letech dvacátého století fašismus. V případě, že se extremisté chopí moci, lze za extremistického aktéra označit i politický režim. Extremisté užívají při svém působení různé metody získávání vlivu. V legálním rámci se jedná o běžný politickou propagandu, o veřejné legální demonstrace, o vzdělávání a osvětu vůči stoupencům apod. Extremismus je však charakteristický tím, že demokratické mechanismy zneužívá k získání politické moci, která demokracii odstraní nebo omezí. Tyto svoje cíle mnohdy také nepokrytě deklarují s různými záminkami a důvody.

Vedle legálních metod se politický extremismus v demokracii často uchyluje i k metodám na hraně legality či zcela nelegálním. Jedná se především o různé formy násilí, od nepřipravených výpadů proti politickým oponentům až po propracovaný *terorismus*. Násilí může sloužit i jako nástroj k šíření propagandy a jeho cílem je spolu s dalšími nástroji vytvoření vhodné situace pro politickou změnu režimu formou puče či revoluce [2].

V obecném pohledu je extremismus spíše politologický pojem, ale svým multidisciplinárním vnitřním obsahem je však nesporně také pojmem sociálně – pedagogickým a právním. Extremismus se stává bezpečnostním rizikem v okamžiku, kdy jsou jeho motorem ostře antagonistické postoje vůči stávajícímu společenskému řádu a nesmiřitelnost vyúsťuje v konkrétní záměry a aktivity, směřující k destabilizaci a odstranění daného politického a sociálního systému. Ve svobodné společnosti by vítězství krajně vyhocených, demokracii nepřátelských postojů, názorů a ideologií znamenalo ústup od lidských práv a nastolení autoritářství, totality nebo anarchie [3].

4. IDENTIFIKACE EXTRÉMISMU

Při identifikaci co je a co není extrémní projev je nutno v první řadě identifikovat, co je legitimní projev ve smyslu uplatňování práva na svobodu slova a kdy se už jedná o nelegální projev omezování ústavních principů nebo zaručených práv jiných osob. To se pro potřeby orgánů činných v trestním řízení provádí často formou znaleckého posudku

S terorismem, jako velmi častým projevem extremistických projevů se setkáváme mnohdy díky zpravodajství médií. Díky nim má téměř každý občan představu o tom, co znamená a jaké jsou prostředky boje extremistů. Velká většina velkých teroristických útoků je provedena islámskými fundamentalisty a je zaměřena proti Izraeli. V Evropě se setkáme s útoky skupin, jako je IRA nebo ETA. Ideologií teroristických skupin je převážně snaha získat jisté území (Hizballáh, PKK, IRA ETA...), nebo nastolit jiný řád (fundamentalistické skupiny - svatá válka) [4].

5. FORMY POLITICKÉHO EXTRÉMISMU

V současné době je nejnebezpečnější formou politického extremismu v České republice neonacismus a nacionalismus. *Neonacismus* je hnutím, které ideově alespoň zčásti navazuje na původní nacismus. Nacismus bylo původně hnutí vniklé ve dvacátých letech dvacátého století

především v Německu (případně na území jiných států s německou populací), které po uchopení moci v roce 1933 v Německu vytvořilo totalitní a agresivní režim, který masivně potlačoval lidská práva (a hodlal vyhladit celé národy, především Židy a Romy) a od roku 1939 vedl agresivní válku. Na obsazených územích (často za pomoci místních kolaborantů) realizoval okupační teror. Po porážce nacistického Německa (kapitulovalo v květnu 1945) se alespoň na některé jeho ideje snaží navázat neonacismus, který v současnosti většinou opustil výhradní vazbu na Německo a Germány a snaží se o využití nacistických rasistických, antisemitských a mocenských cílů, názorů a strategií v rámci celé „bílé rasy“. Neonacismus zpravidla obecně hlásá v celosvětovém rámci koncepci rasistického boje a nadřazenost bílých árijských národů, vycházející z tradic původního nacionálního socialismu [5].

V současné době se objevují i menší proudy více inspirované dělnickým étosem části nacismu z přelomu dvacátých a třicátých let. Existují i různé národní variace vzhledem k historickým tradicím, ať se již týkají inklinace k pohanským tradicím různých národů, zohlednění tradičních národních nepřátel anebo tradic kolaborace za druhé světové války. V ČR lze vysledovat jak neonacismus více propojený s původním německým pojetím nacismu, jehož specifickým vyjádřením je návaznost na sudetoněmecké nacistické tradice, tak i neonacismus respektující rovnoprávnou českou identitu v rámci panářijského neonacistického hnutí (dílčí návaznost na vlajkařské koncepce z Protektorátu Čechy a Morava) [5].

Základními formami působení neonacistů jsou zejména:

- stranickopolitická agitace (v ČR se doposud neprosadila silná neonacistická strana, v poslední době někteří neonacisté spolupracují s Dělnickou stranou),
- veřejné získávání sympatií a upevňování identity hnutí šířením propagandy (demonstrace, internet, tiskoviny, oblečení, hudba, tzv. white power music, přičemž obchodování s uvedenými artefakty slouží i jako zdroj financování hnutí,
- násilí (využití projevů agresivity) k ovlivnění protivníků i stoupenců.

Za druhý základní proud českého pravicového extremismu lze označit český nacionalismus. Pravicově extremistický nacionalismus se liší od demokratického nacionalismu vysokou mírou nacionální netolerance k jiným národům a etnikům (či alespoň některým z nich) a antidemokratickým zaměřením.

Český extremistický nacionalismus lze dále členit na:

- český nacionalismus vycházející z husitské tradice českých dějin, šovinisticky pojatého pokrokářského „národně-obrozeného étosu“ a čechoslovakismu a českého expanzionismu (národovecko-pokrokářský nacionalismus),
- český nacionalismus, který navazuje na tradice českých dějin zbavených „pokrokářského mýtu“ (konzervativní integrální nacionalisté) [6], v jehož rámci se některé skupiny silněji přiklání k tradicím českého fašismu (neofašisté) a může se v něm objevovat různě silná vazba na křesťanství, autoritářský křesťanský konzervatismus, v případě propojení s fašismem klerofašismus (v poslední době prolínání části tohoto proudu s neonacismem).

Jako další možné směry politického extremismu jsou známy zejména dogmatický komunismus, Levicově extremistický anarchismus a autonomové, ale lze k nim počítat i specifické formy fašismu, neofašismu, nacionalismu, neonacionalismu, panslavismus apod.

Vzhledem k zejména právnímu, politologickému a sociologickému diskursu činnosti skupin politického extremismu, kdy se tyto snaží o zviditelnění a získání občanské podpory (byť pasivní), je třeba pomoci nástrojů z oblasti právní vědy, politologie, filozofie, psychologie a

sociální práce, resp. sociální pedagogiky působit na veřejnost se snahou eliminovat silící vliv agresivity a netolerance ve společnosti.

6. MOŽNÉ FORMY PREVENCE VLIVU POLITICKÉHO EXTRÉMISMU Z POZICE BEZPEČNOSTNÍHO MANAGEMENTU

Z hlediska strategie boje státu proti politickému extremismu je tedy v každém případě nutno zaměřit pozornost především na *stěžejní cíle boje proti extremismu, jimiž jsou*:

- a) zamezit vlivu propagandy extremistů, zejména vůči příslušníkům ozbrojených sil, což je v současné době obzvlášť aktuální,
- b) zamezit přijetí extremistů ozbrojených sil a státní správy obecně,
- c) celkově působit tak, aby extremistům nebyla zavádána žádná příčina k věrohodným propagandistickým výpadům, což by jim napomohlo v dosahování vlivu na veřejnost a plnění jejich antidemokratických cílů tak, jak je vnímá současná legislativa.

Z kriminologického pohledu je obecně možno provádět *prevenci na úrovni primární, sekundární a terciární a v různých formách, přičemž v podmínkách ozbrojených sil a možnostech bezpečnostního managementu (leadra) je možno nejreálněji uvažovat o situační prevenci*. Z povahy činnosti a možností bezpečnostního managementu v rámci ozbrojených sil je za nejvhodnější nástroje považovat aktivní činnost v oblasti legislativní (vnitřní předpisy), ale zejména organizační a personální, tedy individuální, systematické a kontinuální vzdělávání v oblasti práva, psychologie, sociologie [7]. Tyto aktivity, tedy zejména v úrovni primární a sekundární prevence a využití vhodných situačních preventivních aktivit je způsobilé nenásilným a důvěryhodným způsobem ovlivnit vnitřní klima u jednotlivých jednotek a skupin a zamezení vzniku extrémistických nálad a projevů extremismu. Jako vhodné se jeví jednak *přednášky z řad pedagogů, znalců, rozbor typických projevů extremismu* (včetně konkrétních případů v ozbrojených sborech států NATO), popřípadě *rozboru ustálené judikatury s komentářem znalce v oboru (politického) extremismu* [8]. Nutno poznamenat, že bezpečnostní management na řídicí úrovni v ozbrojených silách by měl mít schopnost znát a využít i *specifických metod identifikace rizikových příslušníků ozbrojených sil* pro jejich vnější projevy, např. jejich deklarované příslušnosti či sympatii k rizikové skupině osob (např. fotbaloví chuligáni) [9].

Nutno poznamenat, že politický extremismus se může projevovat různými způsoby; od slovních výpadů, přes vzbuzování sympatií k organizacím pošlapávajícím základní lidská práva a svobody až po administrativní obstrukce a schválnosti ve státní správě, resp. její činnosti. Nejzávažnějším projevem politického extremismu však je individuální fyzická agrese proti výlučným skupinám osob, anebo proti celým rasám či národnostem ve formě teroru, a to ať již individuálního, tak skupinového (hromadného). A právě extremismus projevený teroristickým útokem (či jeho hrozbou) je nejzávažnější hrozbou a destabilizujícím prvkem vnitřní i vnější bezpečnosti státu [10].

Projevy politického extremismu u příslušníků Armády České republiky, ale i Slovenska či jiných států NATO mohou mít několik rovin ohrožení signifikantních veřejných zájmů. V první řadě mohou ještě více destabilizovat již tak napjatou atmosféru mezi příslušníky (nejen) Armády České republiky a částí místního obyvatelstva, pokud by se tyto projevy urážely nebo se negativně dotýkaly místního náboženství nebo národního uvědomění. To by mohlo mít za následek zhoršení bezpečnostní situace v místě. Další rovinou ohrožení je negativní konotace z řad politických či jiných oponentů vojenských misí NATO, kterých je možno následně využít k snížení prestiže vojáků NATO a zejména země původu vojáků, kteří se projevů extremismu

dopustili. [11] Další rovinou je (v případě medializace) i ohrožení prestiže např. příslušníků armády, což by mohlo mít za následek ovlivnění veřejného mínění. Není vyloučeno, že by takové incidenty mohly mít za následek negativní legislativní či finanční dopady na financování armády jako celku.

ZÁVĚR

S přihlédnutím ke všem těmto rovinám ohrožení, resp. negativních dopadů případných projevů extremismu v ozbrojených sborech je možno konstatovat, že nezastupitelnou roli v prevenci před těmito projevy má bezpečnostní management a zejména leadr. Tak jako mají projevy politického extremismu různé příčiny a jednotliví aktéři různé motivy, je třeba k řešení tohoto fenoménu přistupovat z interdisciplinárních pozic. V tomto smyslu je pak třeba vzdělávat bezpečnostní management a formovat osobnost leadra, který je pak způsobilý vést a ovlivňovat svoje podřízené a kolegy tak, aby k těmto sociálně patologickým projevům nedocházelo. To je však již otázka vhodného výběru bezpečnostního managementu a zejména také vhodného ovlivňování prostředí a rozvoje osobnosti leadra. Multidisciplinárnost jeho kompetencí je třeba vidět zejména v oblasti pedagogiky, psychologie, práva, historie, ale i z dalších oblastí společenského života tak, aby leadr byl způsobilý tuto preventivní úlohu schopen plnit.

Zdroje

1. SVOBODA, I. *Projevy politického extremismu v ozbrojených sborech*. Bratislava: In. Policajná teória a prax, 2010, s. 117. ISSN – 1335-1370, EV 568/08.
2. MAREŠ, M. *Pravicový extremismus a radikalismus*. Brno: Centrum strategických studií, 2005, s. 46-58. ISBN-sine
3. Bezpečnostní informační služba [online]. [cit. 2008-11-21]. Dostupné z WWW:
4. <<http://www.bis.cz/extremismus.html>>
5. Cestovatel v ohrožení [online]. 2000 [cit. 2008-11-21]. Dostupné z WWW:
6. <<http://www.mujiweb.cz/www/jpdepot/danger/teror.htm>>
7. MAREŠ, M. *Symboly používané extremisty na území ČR v současnosti*. Praha: MVČR, 2006, s. 12-14. ISBN-sine
8. RATAJ, J. Vize české nacionální politiky v soudobých konceptech krajní pravice v České republice. In. *III. kongres českých politologů*, Olomouc 8.-10. 9. 2006; NĚMEC, J., ŠUSTKOVÁ, M. (ed.). Praha, Olomouc: Česká společnost pro politické vědy, 2006.
9. SVOBODA, I. Efektivita vzdělávání bezpečnostního managementu v konceptu celoživotního vzdělávání. In.: *Komenského odkaz a vybrané problémy současného vzdělávání*. Praha: Manažer, poradce, auditor 2022, 15. roč., s. 193-204. ISSN 1803-5213, ISSN – e: 1803-9324.
10. SVOBODA, I. Úloha bezpečnostního managementu ozbrojených sborů při prevenci projevů extrémismu v zahraničních operacích. In. *Policajná teória a prax, Police Theory and Practice*, 4/2019. Bratislava: Akadémia Policajného zboru, 2019, s. 169-176. ISSN 1335-1370, ev. č. EV 568/08.
11. SVOBODA, I., VEGRICHTOVÁ, B. Identifikace rizikových osob v kontextu služebních zákroků policie. In. *Sborník z medzinárodnej vedeckej konferencie „Teoretické a praktické aspekty služobných zákrokov“*. Bratislava: Akadémia Policajného zboru v Bratislave, 2018, s. 145-149. ISBN 978-80-8054-789-9.
12. SVOBODA, I., VIČAR, R. Politický extremismus a terorismus jako destabilizující prvek vnitřní a vnější bezpečnosti EU, In. *Sborník ze semináře Národního konventu o Evropské unii „Rozšiřovanie, bezpečné a prosperujúce susedské prostredie EÚ“*. Liptovský Mikuláš, 2009, ISBN – 978-80-8106-022-9.

13. SVOBODA, I. Hate Crimes as Manifestations of Political Extremism of Contemporary Neo-nazi Scene in Europe, In. *Deliktology. Akademie HUSPOL, Kunovice, 2021, eds. Kopotun, I., Petkov, S.*, s. 155-173. ISBN 978-80-907587-1-1.



AKADÉMIA
POLICAČNÉHO ZBORU
V BRATISLAVE



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond

Program konferencie „Zvýšenie odolnosti Slovenska voči hybridným hrozbám“

5. – 6. 10. 2023

Časť - Papierníčka

Dobrý deň,

program konferencie v rámci národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu ITMS2014+: 314011CDW7, ktorá sa koná v dňoch 5. – 6. 10. 2023 v Účelovom zariadení Kancelárie Národnej rady SR Časť – Papierníčka bude prebiehať podľa časového harmonogramu nasledovne:

Časový harmonogram:

1. deň konferencie - 5.9.2023

- 12:00 – 13:00 registrácia účastníkov,
- 13:00 – 13:15 uvítanie účastníkov na konferencii,
- 13:15 – 14:45 1. blok vystúpení jednotlivých účastníkov konferencie s príspevkami,
- 14:45 – 15:30 coffe break,
- 15:30 – 17:00 2. blok vystúpení jednotlivých účastníkov konferencie s príspevkami,
- 18:00 – 19:00 slávnostná večera,
- 20:30 – 21:00 neformálne posedenie, diskusie.

2. deň konferencie - 6.9.2023

- 7:30 – 9:00 raňajky,
- 9:15 – 10:00 odborná diskusia účastníkov konferencie,
- 10:00 – 10:15 coffe break,



AKADÉMIA
POLICAČNÉHO ZBORU
V BRATISLAVE



Operačný program
**Efektívna
verejná správa**



Európska únia
Európsky sociálny fond

10:15 – 10:30 odovzdávanie certifikátov o účasti na konferencii,

12:00 – 12:55 obed,

12:55 – 13:00 ukončenie konferencie.

V priebehu voľného času bude účastníkom konferencie dostupný bazén a wellness centrum vo vopred vymedzenom čase, o ktorom budú účastníci informovaní pri registrácii. Zároveň účastníkov informujeme, že poskytované ubytovanie a strava je pre účastníkov konferencie bezplatná.

V prípade doplňujúcich otázok sa na nás môžete obrátiť prostredníctvom e-mailu apzkonferenciahh@gmail.com. Radi zodpovieme Vaše otázky.

Prajeme Vám pekný deň!

Organizačný výbor konferencie

Názov: Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy

Zborník príspevkov z konferencie konanej v dňoch 5. – 6. 10. 2023 v Účelovom zariadení Kancelárie Národnej rady SR Časť – Papiernička

Kód projektu: ITMS2014+: 314011CDW7

Vydala: Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava

Zostavil: Mgr. Ivana Rubisová, PhD.

Recenzenti: prof. Ing Miroslav Lisoň, PhD.
plk.v.v. doc. JUDr. Robert Odler, PhD.

Vytlačilo: Centrum polygrafických služieb MV SR

Formát: B5

Rozsah: 327 strán

Počet znakov: 976 646

Náklad: výtlačkov

Rok vydania: 2023

Vydanie: prvé

ISBN

EAN