DOI: https://doi.org/10.52651/nmb.c.2024.9788080406738.270-285

15. medzinárodná vedecká konferencia ♦15th International Scientific Conference
Národná a medzinárodná bezpečnosť 2024 ♦ National and International Security 2024
17. – 18. 10. 2024, Liptovský Mikuláš

SYSTÉM OCHRANY SR PRED HYBRIDNÝMI A KYBERNETICKÝMI HROZBAMI A NÁSTROJE POTLÁČANIA ICH VPLYVOV

PROTECTION SYSTEM OF THE SLOVAK REPUBLIC AGAINST HYBRID AND CYBER THREATS AND TOOLS FOR MITIGATING THEIR IMPACTS

Mário PAŽICKÝ

ABSTRACT

A conference proceedings paper titled "Cyber and Hybrid Threats as a Dynamizing Factor of the Security Environment of the Slovak Republic and Possibilities for Their Elimination" addresses the dynamics and complexity of cyber and hybrid threats in the current security environment of the Slovak Republic. It focuses on analyzing legislative frameworks and strategic documents that the Slovak Republic has adopted in the fight against these threats, especially the Action Plan for Coordination of the Fight Against Hybrid Threats. The paper also emphasizes the necessity of cooperation between the public and private sectors and the need for a whole-of-society approach to mitigating these threats. Additionally, the paper outlines potential solutions for eliminating these threats through strengthening cyber defense and building societal resilience against disinformation and other influences of hybrid activities.

Keywords: hybrid threats, cyber threats, action plan, disinformation

ÚVOD

V súčasnom dynamickom a nepredvídateľnom bezpečnostnom prostredí hybridné a kybernetické hrozby predstavujú významný a komplexný problém, ktorý si vyžaduje multidisciplinárny prístup a efektívne legislatívne riešenia. Tieto hrozby, kombinujúce o. i. aspekty klasických vojenských operácií, dezinformačných kampaní a kybernetických útokov, majú tendenciu zasahovať do viacerých oblastí našich životov, destabilizovať spoločenské a politické procesy a narúšať dôveru občanov v demokratické inštitúcie.

Hybridné hrozby, ako pojem, nadobudli na význame v posledných rokoch, najmä v kontexte konfliktov, v ktorých sa preukázalo ako a aké metódy využívajú štátni aj neštátni aktéri pre dosiahnutie svojich cieľov bez formálneho vyhlásenia vojny. Využívajú techniky ako propaganda, dezinformácie, ekonomické tlakové kampane a kybernetické útoky, ktoré nie sú ľahko identifikovateľné. Dôsledky týchto hrozieb sú však značné. Dezinformácie môžu manipulovať s verejnou mienkou, znižovať dôveru v inštitúcie a polarizovať spoločnosť. Kybernetické útoky môžu narušiť kritickú infraštruktúru, čo vedie k významným ekonomickým stratám a ohrozeniu národnej bezpečnosti. V posledných rokoch sme svedkami nielen nárastu frekvencie týchto hrozieb, ale aj ich sofistikovanosti. Vznik nových technológií a platforiem pre komunikáciu, ako sú sociálne médiá, poskytuje hybridným aktérom nové nástroje na šírenie dezinformácií a pre manipuláciu s verejnosťou. Tieto platformy umožňujú rýchle a široké rozšírenie informácií, ktoré môžu byť zavádzajúce alebo úplne nepravdivé.

Slovenská republika si uvedomila naliehavosť situácie a v posledných rokoch sa snaží vyvinúť adekvátne legislatívne a praktické odpovede na tento narastajúci problém. V rámci boja proti hybridným a kybernetickým hrozbám boli vypracované rôzne akčné plány a

strategické dokumenty. Medzi najvýznamnejšie patrí Akčný plán koordinácie boja proti hybridným hrozbám (ďalej iba APHH), ktorý sa snaží systematicky reagovať na aktivity domácich aj zahraničných aktérov.

Cieľom APHH je zvýšiť odolnosť štátu a spoločnosti voči hybridným hrozbám prostredníctvom posilnenia medzirezortnej spolupráce a koordinácie. To zahŕňa zavedenie mechanizmov pre rýchlu detekciu, analýzu a reakciu na hybridné aktivity, ako aj zvyšovanie povedomia verejnosti o rizikách spojených s týmito hrozbami. Kľúčovým aspektom tohto plánu je aj spolupráca medzi verejným a súkromným sektorom, no aj s občianskou spoločnosťou. Tá sa javí nevyhnutnou pre efektívnu obranu proti hybridným aktivitám.

Jedným z najdôležitejších faktorov pri ochrane pred hybridnými a kybernetickými hrozbami je zvyšovanie úrovne informovanosti a vzdelávania v tejto oblasti. Občania musia byť vybavení kritickým myslením a schopnosťou rozpoznať dezinformácie. To je možné dosiahnuť prostredníctvom moderných vzdelávacích programov. Školy, univerzity a iné vzdelávacie inštitúcie by mali zohrávať kľúčovú úlohu v rozvoji mediálnej gramotnosti a schopnosti analyzovať informácie.

Napriek prijatým opatreniam zostáva množstvo výziev, ktoré je potrebné riešiť. Tieto výzvy sa týkajú predovšetkým legislatívnych medzier, nedostatku informácií a vzdelania medzi občanmi, ako aj potreby rozvinúť robustnejšie mechanizmy pre ochranu kritickej infraštruktúry. Zároveň je nevyhnutné zlepšiť schopnosti štátnych inštitúcií v oblasti kybernetickej bezpečnosti a získať podporu zo strany medzinárodných organizácií, ako sú NATO a EÚ.

Rovnako je dôležité zohľadniť aspekty spolupráce s inými štátmi a organizáciami - hybridné hrozby nepoznajú hranice a vyžadujú si spoločný prístup na medzinárodnej úrovni. Slovensko by malo aktívne participovať na medzinárodných iniciatívach a projektoch, ktoré sa zameriavajú na zdieľanie informácií, technológií a osvedčených praktík v oblasti boja proti hybridným a kybernetickým hrozbám.

Faktom je, že hybridné a kybernetické hrozby sú pre Slovenskú republiku vážnym bezpečnostným problémom, ktorý si vyžaduje kontinuálnu a koordinovanú odpoveď. Tento príspevok sa snaží prispieť k dôležitej diskusii o nevyhnutnosti posilnenia odolnosti spoločnosti voči týmto hrozbám a môže poskytnúť podnety na ďalší rozvoj legislatívnych a praktických prístupov v tejto oblasti.

1 HYBRIDNÉ HROZBY

„V posledných rokoch mnoho vojenských teoretikov odhaduje, že bude naďalej dochádzať k poklesu počtu klasických ozbrojených konfliktov medzi štátmi na úkor asymetrických a nepravidelných konfliktov, kedy aspoň jedna bojujúca strana nebude štátom“ (Řehka, 2017, s. 47). Hybridná hrozba je kombináciou rôznych spôsobov a foriem útokov a nepriateľských aktivít, ktorých cieľom je oslabiť štát, či jeho organizáciu. Hybridné hrozby zahŕňajú široké spektrum techník, ktoré môžu zahŕňať tradičné vojenské operácie, kybernetické útoky, ekonomický tlak, dezinformácie, sabotáž, špionáž či podporu domácich konfliktov alebo terorizmu. Účelom hybridných hrozieb je často znížiť schopnosť štátu alebo organizácie efektívne reagovať na krízy, destabilizovať vnútornú situáciu, narušiť súdržnosť spoločnosti a oslabiť medzinárodnú pozíciu cieľa. Hybridné hrozby sú často menej zjavné a vyžadujú špecifické schopnosti na ich odhalenie a zvládnutie.

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.

Základnou vlastnosťou hybridného pôsobenia je jeho nejednoznačnosť a neurčitosť pôvodu. Hybridní aktéri sa pri činnosti snažia zakryť svoju identitu alebo skutočný cieľ, ktorý chcú dosiahnuť. Konvenčnými a nekonvenčnými prostriedkami stierajú obvyklé hranice medzi legálnym a nelegálnym, či priamo medzi mierom a vojnou. Samostatným problémom je ovplyvňovanie vnútropolitickej situácie, netransparentná a skrytá podpora politických subjektov zo strany cudzích mocí a činiteľov, vrátane podpory pre polovojenské a extrémistické skupiny.

Používanie nástrojov hybridných hrozieb môže slúžiť na dosiahnutie konkrétnych cieľov aj bez formálneho vyhlásenia vojny. V súčasnosti existujú desiatky nástrojov hybridných hrozieb (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.

Vedenie hybridného útoku 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 je potrebné prijať celospoločenský prístup k problému.

1.1 AKČNÝ PLÁN BOJA PROTI HYBRIDNÝM HROZBÁM

Akčný plán koordinácie boja proti hybridným hrozbám predpokladá nízke riziko priameho ohrozenia konvenčným ozbrojeným útokom a v tomto zmysle zavádza systémové, všeobecné, ale aj čiastkové a konkrétne opatrenia reagujúce na koordinované pôsobenie cudzích a domácich aktérov, ktorí konajú proti bezpečnostným a iným záujmom Slovenskej republiky.

Pôsobenie hybridných hrozieb proti záujmom Slovenskej republiky sa za posledných niekoľko rokov presunulo z periférie do hlavného prúdu na takmer všetky úrovne spoločnosti. Akčný plán je vyústením niekoľkoročného spojeného úsilia expertov štátnej správy, občianskej spoločnosti a politických lídrov s odhodlaním efektívne zmierňovať rozvratné pôsobenie hybridných aktérov.

Títo pod prahom zvyčajnej reakcie priamo vplývajú na verejnú mienku, zhoršujú existujúce pnutia v spoločnosti, zasahujú do volebných procesov, znižujú dôveru verejnosti v inštitúcie, erodujú spoločenský konsenzus o správnosti demokratického usporiadania, či euroatlantického ukotvenia Slovenskej republiky a propagujú toxickú formu nacionalizmu, ktorá má tendenciu, často aj legislatívne, vyčleňovať a znevýhodňovať skupiny občanov, legitimizovať autokratické formy vládnutia, či marginalizovať kľúčovú dôležitosť ľudských práv a princípov právneho štátu.

„Pojmom hybridné hrozby sa v kontexte APHH označujú aktivity štátnych alebo neštátnych aktérov, ktoré majú otvoreným alebo skrytým pôsobením vojenských alebo nevojenských metód oslabiť, alebo inak poškodiť vybraný cieľ. Tieto aktivity sú často koordinované, zameriavajú sa na lokálne zraniteľnosti a sú navrhnuté tak, aby zostali pod hranicou detekcie, atribúcie a z toho vyplývajúcej zvyčajnej reakcie. Pojmom odolnosť sa

označuje schopnosť štátnych inštitúcií a spoločnosti vyrovnať sa s hybridným pôsobením rôznej intenzity a rôzneho trvania spôsobom, ktorý minimalizuje negatívne dopady tohto pôsobenia, odstráni prípadné škody a obnoví funkčnosť zasiahnutých alebo narušených politicko-spoločenských procesov. Pojmom budovanie odolnosti sa označujú paralelné procesy odstraňovania zraniteľností a budovania spôsobilostí, ktoré štátu a spoločnosti umožnia efektívne čeliť hybridnému pôsobeniu“ (Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024, Ministerstvo obrany SR, s. 3.).

Vypracovanie APHH vychádzalo ešte z programového vyhlásenia vlády pre roky 2021-2024 (ďalej iba PVV).

„Strategickým cieľom Akčného plánu koordinácie boja proti hybridným hrozbám je:

- posilnenie odolnosti štátu a spoločnosti voči hybridným hrozbám,
- posilnenie medzirezortnej spolupráce a koordinácie s cieľom včasnej detekcie, analýzy, atribúcie a reakcie na hybridné aktivity voči SR,
- zvyšovanie povedomia spoločnosti o rizikách hybridného pôsobenia a potrebe zvyšovania celospoločenskej odolnosti voči nim,
- vybudovanie systému strategickej komunikácie na vládnej a rezortnej úrovni,
- posilnenie aktívneho pôsobenia SR pri rozvoji spolupráce v rámci EÚ a NATO v oblasti boja s hybridnými hrozbami a posilňovania medzinárodnej spolupráce“ (Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024, Ministerstvo obrany SR, s. 4.)“.

Dokument podporuje aliančné záväzky Slovenskej republiky smerujúce k posilňovaniu spoločenskej odolnosti voči hybridným hrozbám, zvyšovaniu pripravenosti v oblasti civilnej ochrany (prostredníctvom litery NATO 7 baseline requirements) a tiež ambície Európskej únie popísané v Stratégii EÚ pre bezpečnostnú úniu a tie, ktoré sa formujú v procese prípravy Strategického kompasu EÚ.

Kvôli chýbajúcej stratégii pre boj Slovenskej republiky s hybridnými hrozbami nadväzuje APHH priamo na Koncepciu pre boj Slovenskej republiky proti hybridným hrozbám (2018). Okrem PVV sa materiál opiera o aktuálnu Bezpečnostnú stratégiu Slovenskej republiky (2021) a Obrannú stratégiu Slovenskej republiky (2021), ktoré jednoznačne rámcujú potrebu zabezpečiť pripravenosť štátu a spoločnosti efektívne a koordinovane zmierňovať hybridné hrozby a použiť na to všetky dostupné obranné kapacity, zdroje a opatrenia, ktoré má k dispozícii.

Model inštitucionálnej koordinácie, ktorý bol zavedený Koncepciou pre boj Slovenskej republiky proti hybridným hrozbám (2018) zapája Situačné centrum Slovenskej republiky (ďalej iba SITCEN), ktoré plní úlohu národného kontaktného miesta pre hybridné hrozby a Národné bezpečnostné analytické centrum (ďalej iba NBAC), ktoré plní úlohy národného kooperačného centra pre hybridné hrozby. APHH dopĺňa systém o nový prvok - Výbor pre hybridné hrozby Bezpečnostnej rady Slovenskej republiky, ktorý má byť koordinačným uzlom pre tvorbu relevantných politík.

Kľúčovým predpokladom efektívnej reakcie štátu na hybridné hrozby je celospoločenský prístup k bezpečnosti a precízne nastavenie procesov zapojenia a vzájomnej koordinácie inštitúcií štátnej správy, ekonomického a akademického sektora (vysoké školy a výskumné inštitúcie spolufinancované z verejných zdrojov) a občianskej spoločnosti (whole-of-society approach). Celospoločenský prístup predpokladá sofistikované narábanie s otvorenými zdrojmi a transparentnú, vysoko koordinovanú a efektívnu strategickú komunikáciu štátu a z toho vyplývajúcu vysokú mieru verejnej diskusie a zapojenia verejnosti do obrany všeobecne.

Akčný plán, vypracovaný v gescii Ministerstva obrany SR, dopĺňa a posilňuje koordinovaný mechanizmus boja proti hybridným hrozbám v zmysle vyššie uvedenej koncepcie. Ten má tiež ministerstvo obrany spolu s relevantnými Ústrednými orgánmi štátnej správy (ďalej ‚ÚOŠS') pomáhať implementovať a adekvátne optimalizovať. Na jeho konci má byť agenda boja proti hybridných hrozbám naďalej sústredená v NBAC, no zároveň významne rozšírená o nové prvky. Najvýznamnejším z nich je vznik nových, resp. posilnenie už existujúcich útvarov na Úrade vlády SR, Ministerstve obrany SR, Ministerstve zahraničných vecí a európskych záležitostí SR a Ministerstve vnútra SR, ktorých úlohou je efektívne budovanie odolnosti Slovenskej republiky voči hybridným hrozbám.

Opatreniami akčného plánu vláda Slovenskej republiky reaguje na bezpečnostné riziká spojené so zahraničnými investíciami do kritickej infraštruktúry, médií, či akademického sektora, ovplyvňovanie volebných procesov, strategickú korupciu, či pôsobenie nelojálnych polovojenských skupín, so zvýšeným dôrazom na podvratné vplyvové aktivity aktérov, ktorí využívajú propagandu, dezinformácie, šírenie nenávistných alebo extrémistických obsahov a to aj verejne činnými osobami, či predstaviteľmi verejnej moci. Ich cieľom je obvykle erózia spoločenského konsenzu o správnosti euroatlantického ukotvenia Slovenskej republiky, dôvery vo verejné inštitúcie a demokratické zriadenie, spochybňovanie štátnej identity, zdieľanej interpretácie histórie, viery v správnosť a dodržiavanie zákonov, či pocit občianskej spolupatričnosti.

1.2 VÝCHODISKÁ AKČNÉHO PLÁNU BOJA PROTI HYBRIDNÝM HROZBÁM

APHH vychádza z predpokladu, že úspešná reakcia štátu na hybridné hrozby musí stáť na:

a) koordinovanom zapojení relevantných ÚOŠS, subjektov ŠS, ekonomického a akademického sektora a občianskej spoločnosti,

b) vzniku a pôsobení pracovísk pre boj s hybridnými hrozbami na relevantných ÚOŠS spolupracujúcich s NBAC ako národným kooperačným centrom pre hybridné hrozby,

c) systémovej a koordinovanej implementácii konceptu strategickej komunikácie štátu zriadením a pôsobením útvaru strategickej komunikácie Úradu vlády SR a relevantných ÚOŠS, d) kontinuálnom navyšovaní spôsobilostí ÚOŠS a inklúzii širokej verejnosti.

Úspešný prístup k zmierňovaniu hybridných hrozieb musí odrážať potreby súčasného rýchlo sa meniaceho bezpečnostného prostredia, ktoré si vyžaduje celospoločenský prístup k obrane štátu. APHH preto navrhuje aj súbor opatrení zameraných na budovanie odolnosti obyvateľstva, ktoré stojí na zavádzaní moderných vzdelávacích programov do vzdelávacieho systému, ako aj na riešeniach, ktoré zodpovedajú súčasným decentralizovaným možnostiam vzdelávania a technickým spôsobilostiam verejnosti. Ústrednou témou budovania odolnosti je tiež ochrana občianskej spoločnosti a stransparentňovanie - pre hybridné hrozby relevantných - častí verejného priestoru.

APHH bol vytvorený so zreteľom na meniace sa bezpečnostné prostredie a prepojenie na aktuálne etablovaný bezpečnostný systém štátu. Jeho plnenie si vyžaduje úzku súčinnosť a spoluprácu existujúcich štátnych inštitúcií a posilnenie bezpečnostného systému o nové centralizované inštitucionálne prvky. Realizácia úloh stanovených v APHH má za cieľ vylepšiť adresnosť a reakcieschopnosť štátu, nenahrádza však potrebu komplexnej aktualizácie Koncepcie bezpečného systému SR. APPH je zároveň otvoreným dokumentom, ktorý môže byť v závislosti od identifikovaných potrieb aktualizovaný o ďalšie úlohy.

Úspešnou implementáciou opatrení APHH Slovenská republika zvýši povedomie o hybridných hrozbách v radoch zamestnancov ÚOŠS, ŠS, ozbrojených zložiek a širokej verejnosti. Akčný plán má zaviesť formou a obsahom moderné vzdelávacie programy, zvýšiť odolnosť obyvateľstva a občianskej spoločnosti, stransparentniť verejný priestor a zlepšiť koordináciu a efektivitu spolupráce relevantných zložiek ÚOŠS zodpovedných za zmierňovanie dôsledkov aktivít, ktoré pod prahom zvyčajnej reakcie dlhodobo, sústavne a koordinovane pôsobia proti záujmom Slovenskej republiky.

2 KYBERNETICKÉ HROZBY

Kybernetické hrozby sú hrozby aktivít ohrozujúcich dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov, súvisiacich služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov. „Kybernetická bezpečnosť je stav, v ktorom sú informačné systémy a služby odolné voči aktuálnym hrozbám a zraniteľnostiam, ale aj pripravené na detekciu a riešenie kybernetických bezpečnostných incidentov, obnovu dát a procesov a minimalizáciu následkov. Kybernetická bezpečnosť však nie je len záležitosťou konkrétnych organizácií a subjektov, ktoré prostredníctvom vhodných opatrení chránia svoje aktíva“ (Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, Národný bezpečnostný úrad, s. 4). Modernizácia spoločnosti prostredníctvom informačných a komunikačných technológií, jej digitalizácia a rozvoj inovatívnych služieb sú nepopierateľným faktom, ktorý sa stal prirodzenou súčasťou našich životov. Rozvoj, ktorý prináša rozširovanie možností, však musí byť vyvažovaný zodpovednosťou za riziká, ktoré vznikajú paralelne ako negatívna daň za výhody digitálnej spoločnosti.

Informatizácia verejného sektora, automatizácia výrobných a iných procesov, ktoré boli v minulosti vykonávané manuálne, neustály rozvoj a ľahká dostupnosť technológií, jednoduchosť ich používania v širokom spektre bežných činností vytvárajú priestor, v ktorom popri nesporných výhodách vznikajú hrozby namierené proti kritickým a citlivým systémom a službám štátu. Môžu narušiť dôveru občana v štát, spôsobiť rozsiahle ekonomické a hospodárske škody až po škody na zdraví a živote občanov.

Systém riadenia informačnej a kybernetickej bezpečnosti, ktorým sa má zabezpečiť vysoká miera odolnosti systémov a služieb a tiež efektívne detekčné a reakčné schopnosti, je strategickým bezpečnostným záujmom Slovenskej republiky. Ucelený koncept riadenia informačnej a kybernetickej bezpečnosti, strategické smerovanie na základe jasných princípov a presne definované strategické ciele sú základom pre dobre vyvinutý systém, ktorý dokáže pružne reagovať na aktuálne hrozby a zabezpečiť tak vysokú mieru kybernetickej bezpečnosti na národnej úrovni.

Historicky, Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len „Národná stratégia") nie je prvým strategickým dokumentom, ktorý bol na národnej úrovni vytvorený. V roku 2007 bola vytvorená stratégia informačnej bezpečnosti spolu s akčným plánom a následne v období rokov 2015 až 2020 bola platná Koncepcia kybernetickej bezpečnosti Slovenskej republiky, ktorá bola prvým uceleným plánom, ktorý popísal princípy, zásady a ciele kybernetickej bezpečnosti. Opatrenia, ktoré zarámcovali túto koncepciu, sa zameriavali na vytvorenie inštitucionálneho rámca riadenia, prijatie vhodnej legislatívy, rozpracovanie základných mechanizmov správy kybernetického priestoru, vypracovanie systému vzdelávania, vytvorenie kultúry riadenia rizík, aktívnu medzinárodnú spoluprácu a podporu vedy a výskumu. Ku koncepcii bol vytvorený Akčný plán jej realizácie, ktorý určil konkrétne úlohy viažuce sa na jednotlivé opatrenia, gestorstvo subjektov, zodpovednosti participujúcich orgánov, ako aj časové rozmedzie plnenia úloh. V časovom horizonte, na ktorý

boli Koncepcia s Akčným plánom prijaté, sa podarilo vytvoriť stabilný inštitucionálny rámec riadenia kybernetickej bezpečnosti, prijať historicky prvú komplexnú legislatívu v oblasti kybernetickej bezpečnosti a boli vytvorené špecializované entity na riešenie kybernetických bezpečnostných incidentov.

Kybernetické hrozby, ako aj kybernetická bezpečnosť, sa neustále vyvíjajú. Neustále vznikajú nové ciele a vektory kybernetických útokov, ktoré sú čoraz rozsiahlejšie, častejšie a sofistikovanejšie. Niektoré štáty a neštátni aktéri sa stále viac uchyľujú k presadzovaniu svojich cieľov prostredníctvom nekalých kybernetických aktivít. Tieto môžu mať viaceré formy, vrátane útokov na kritickú infraštruktúru, kybernetickú špionáž, krádeže duševného vlastníctva, kybernetickú kriminalitu a kybernetické útoky ako súčasti hybridných hrozieb. Kybernetický priestor sa stále viac stáva oblasťou strategickej konfrontácie medzi štátmi, ktorá odráža dynamické geopolitické prostredie a úsilie o zmenu súčasného medzinárodného poriadku. Technologické inovácie, vrátane inovácií v oblasti kybernetickej bezpečnosti sa stávajú nástrojom konfrontácie a rastúceho napätia v politickej, hospodárskej a bezpečnostnej oblasti.

Dobrou správou je, že strategické smerovanie systému kybernetickej bezpečnosti môže stavať na dobrých základoch, ktoré položila Koncepcia a rozvinul jej akčný plán aj napriek tomu, že niektoré z úloh neboli úspešne ukončené.

Nová stratégia nadväzuje na vykonané aktivity a má ambíciu moderným spôsobom reagovať na aktuálne a perspektívne bezpečnostné hrozby, zadefinovať princípy systému kybernetickej bezpečnosti a určiť strategické ciele, ktorých dosiahnutím sa zabezpečí vyššia miera bezpečnosti v kybernetickom priestore Slovenskej republiky. Národná stratégia je určená pre všetky subjekty, ktoré sa podieľajú na budovaní systému kybernetickej bezpečnosti Slovenskej republiky a je strešným dokumentom, z ktorého vychádza základné smerovanie Slovenskej republiky v tejto oblasti.

Víziou Národnej stratégie je posilňovanie a vytvorenie otvoreného, slobodného a bezpečného kybernetického priestoru pre všetkých.

2.1 AKČNÝ PLÁN BOJA PROTI KYBERNETICKÝM HROZBÁM

Kybernetická bezpečnosť je s neustále rastúcou digitalizáciou spoločnosti jednou z najdôležitejších oblastí, ktorá priamo ovplyvňuje fungovanie modernej spoločnosti. Aby bolo možné ju efektívne riadiť, potrebuje strategické ukotvenie v systéme správy štátu. Komplexný prístup ku kybernetickej bezpečnosti s jasnými princípmi a cieľmi nie len zaručuje jasnú víziu, ale aj potvrdzuje jej dôležitosť v celom bezpečnostnom systéme.

Previazanie kybernetickej bezpečnosti s problematikou počítačovej kriminality, kybernetického spravodajstva, kybernetickej obrany a kybernetickej diplomacie podčiarkuje multidimenzionálny presah kybernetickej bezpečnosti do viacerých významných oblastí, ktoré formujú kybernetický priestor. Systém riadenia kybernetickej bezpečnosti si na národnej úrovni vyžaduje nie len implementáciu tuzemských právnych noriem a procesov, ale musí zohľadňovať aj vývoj na úrovni EÚ, Rady Európy a OSN, nakoľko problematika kybernetickej bezpečnosti stiera hranice medzi štátmi a má globálny dopad na fungovanie spoločnosti.

Dňa 7. januára 2021 bola vládou schválená Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len "Národná stratégia"), ktorá zakotvila smerovanie Slovenskej republiky v oblasti kybernetickej bezpečnosti. V Národnej stratégii sú popísané princípy, na ktorých stojí systém riadenia kybernetickej bezpečnosti, ako aj hrozby, ktoré vplývajú na procesy a činnosti v oblasti kybernetickej bezpečnosti a majú významný dopad na bezpečnosť štátu, ako aj jeho obyvateľov. Ako reakciu na tieto hrozby Národná stratégia určila strategické ciele, na ktoré je potrebné sa v najbližších rokoch zamerať:

- dôveryhodný štát pripravený na hrozby,
- efektívne odhaľovanie a objasňovanie počítačovej kriminality,
- odolný súkromný sektor,
- kybernetická bezpečnosť ako základná súčasť verejnej správy,
- silné partnerstvá,
- vzdelaní odborníci a vzdelaná verejnosť,
- výskum a vývoj v oblasti kybernetickej bezpečnosti.

Aby mohla byť Národná stratégia a jej ciele vykonateľné, musia byť určené konkrétne úlohy a aktivity spolu s jasnými zodpovednosťami. Na tento účel slúži Akčný plán Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len 'APKB'), ktorý tieto úlohy definuje, určuje zodpovedné subjekty a takisto aj časové horizonty pre jednotlivé úlohy.

Cieľom akčného plánu je vytvoriť ucelený koncept úloh a aktivít v oblasti kybernetickej bezpečnosti na najbližších 5 rokov. Navrhované úlohy sú adekvátne k potrebám naplnenia vízie a strategických cieľov stratégie a rešpektujú základné princípy, ktoré boli v stratégii zakotvené.

Budovanie spôsobilostí v oblasti kybernetickej bezpečnosti je nevyhnutným predpokladom pre účinnú ochranu kybernetického priestoru. Ide o komplexný proces, zahŕňajúci budovanie personálnych kapacít, vybudovanie organizačného rámca, rozvíjanie partnerskej spolupráce na národnej a medzinárodnej úrovni ako aj akvizície technických a technologických nástrojov. Vhodné nastavenie systému budovania spôsobilostí, zahŕňajúceho konkrétne úlohy a aktivity, prináša jasné priority, ako aj smerovanie SR v oblasti kybernetickej bezpečnosti.

Za monitorovanie implementácie je zodpovedný stály monitorovací výbor pre implementáciu APKB. Za implementáciu úloh a aktivít sú zodpovedné konkrétne subjekty. Tie sú uvedené pri jeho jednotlivých úlohách a aktivitách.

2.2 VÝCHODISKÁ AKČNÉHO PLÁNU BOJA PROTI KYBERNETICKÝM HROZBÁM

Od 1. januára 2016 sa novelou zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy stal Národný bezpečnostný úrad (ďalej len „úrad") ústredným orgánom štátnej správy pre kybernetickú bezpečnosť. Úrad tak prevzal zodpovednosť za túto oblasť a tým sa zjednotila kompetencia, súvisiaca s riadením kybernetickej bezpečnosti v Slovenskej republike. Dňom 1. apríla 2018 vstúpil do platnosti zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorým sa transponovala 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 (ďalej len "smernica NIS"), no najmä sa precizovalo postavenie, úlohy a právomoci úradu v oblasti kybernetickej bezpečnosti a legislatívne sa zadefinoval a zjednotil systém riadenia kybernetickej bezpečnosti.

2.3 SYSTÉM RIADENIA KYBERNETICKEJ BEZPEČNOSTI v SR

Systém riadenia kybernetickej bezpečnosti v Slovenskej republike má niekoľko vrstiev, ktoré môžeme rozdeliť na národnú úroveň a sektorovú úroveň. Na národnej úrovni úrad riadi strategické, koncepčné a normotvorné činnosti, je kontaktným bodom pre zahraničie, vrátane medzinárodných organizácií, vedie register základných služieb, register prevádzkovateľov základných služieb, register poskytovateľov digitálnych služieb a vykonáva ďalšie dôležité činnosti a aktivity v oblasti kybernetickej bezpečnosti na národnej úrovni, vymedzené v §5

zákona o kybernetickej bezpečnosti. Taktiež plní úlohu Národnej jednotky CSIRT, ktorá na národnej úrovni rieši a koordinuje riešenie kybernetických bezpečnostných incidentov, vydáva včasné varovania a výstrahy pred kybernetickými bezpečnostnými incidentami a zraniteľnosťami a rieši ostatné úlohy, súvisiace s riešením kybernetických bezpečnostných incidentov a obnovou systémov.

Na sektorovej úrovni je podľa zákona definovaných 11 sektorov a 25 podsektorov. Za každý zo sektorov je zodpovedný ústredný orgán, ktorý plní úlohy na úrovni poskytovania požadovanej súčinnosti s úradom, spolupráce s inými sektorovými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti, budovaní bezpečnostného povedomia, koordinovanej spolupráce na všetkých stupňoch riadenia kybernetickej bezpečnosti, aplikácie bezpečnostných opatrení, identifikácie základnej služby a prevádzkovateľa základnej služby a spolupráce so zahraničnou inštitúciou obdobného zamerania.

V každom sektore, na základe identifikácie podľa zákona, vystupujú prevádzkovatelia základných služieb. Títo majú povinnosti vyplývajúce zo zákona a to najmä prijať a dodržiavať zákonne vymedzené bezpečnostné opatrenia, bezodkladne úradu hlásiť závažný kybernetický bezpečnostný incident, riešiť kybernetické bezpečnostné incidenty, zabezpečovať dôkazy o kybernetických bezpečnostných incidentoch, spolupracovať s úradom a ústredným orgánom, ako aj oznámiť orgánom činným v trestnom konaní, ak bol spáchaný trestný čin v súvislosti s kybernetickým bezpečnostným incidentom.

Zákon definuje aj Poskytovateľov digitálnej služby, ktorí prevádzkujú jednu z troch služieb - online trhovisko, internetový vyhľadávač alebo službu vcloud computingu. Ich povinnosti sú veľmi podobné ako povinnosti Prevádzkovateľov základnej služby - teda prijať a dodržiavať bezpečnostné opatrenia v rozsahu špecifickom pre poskytovateľa digitálnej služby, hlásiť - podľa špecifických pravidiel - kybernetický bezpečnostný incident a tento aj riešiť a spolupracovať s úradom pri jeho riešení.

3 HYBRIDNÉ BOJISKO BEZ HRANÍC

Bombastickými sa javili správy pre Slovensko: 8. decembra 2020 bol slovenský poslanec Európskeho parlamentu Vladimír Bilčík zvolený za koordinátora európskeho výboru pre boj s dezinformáciami. Výbor sa zameriava na identifikáciu oblastí, ktoré potrebujú európsku legislatívnu úpravu, vrátane budúceho fungovania sociálnych sietí a digitálnych platforiem. Analyzuje takisto porušovanie a obchádzanie volebných pravidiel a pracuje na spoločnom postupe proti hybridným hrozbám a škodlivým dezinformačným kampaniam tretích krajín, ktorých cieľom je podkopávať Európsku úniu.

Krátko na to vtedajší minister obrany Naď vystúpil na medzinárodnom kongrese, kde v diskusii zdôraznil najmä nevyhnutnosť efektívne a koordinovane reagovať na hybridné hrozby vrátane dezinformačných vplyvov, ktorým čelí aj Slovenská republika. Odpoveďou na ich zvládnutie bola nová Bezpečnostná stratégia SR a Obranná stratégia SR.

Okrem iného povedal: ‘Bezpečnostná stratégia v hodnotení bezpečnostného prostredia jasne pomenúva, že Slovensko čelí aj hybridným hrozbám. Chceme preto posilniť kapacity a expertízu vo verejnej správe, ako aj celoštátnu koordináciu v tejto oblasti. Oblasť hybridných hrozieb a dezinformácií je súčasťou aj novej Obrannej stratégie. Tá určuje za predpoklad zvládania výziev v kybernetickom priestore včasnú identifikáciu prípadných hrozieb a reakciu proti nim. Najefektívnejšia je samozrejme prevencia. Obranná stratégia preto počíta aj so zvyšovaním informovanosti obyvateľstva o zabezpečovaní obrany štátu, čím sa zvýši odolnosť obyvateľstva voči dezinformáciám a škodlivej propagande. Už zmienenou významnou

medzirezortnou iniciatívou – aj na tomto poli - je ‚Akčný plán na koordináciu boja proti hybridným hrozbám a dezinformáciám'. Jeho ambíciou je identifikácia problémov aj v tejto oblasti spolu s konkrétnymi návrhmi ich riešení. K hybridným hrozbám Slovensko pristupuje aktívne aj na pôde NATO, ktoré v roku 2016 uznalo kybernetický priestor ako operačnú doménu a zaviazalo sa k zlepšeniu kybernetickej obrany na národnej úrovni."

„Informačné operácie sú vojenskou činnosťou, ktorá podporuje ciele širšej strategickej komunikácie a zabezpečuje jej realizáciu vo vojenských operáciách. Zameriavajú sa predovšetkým na ovplyvnenie vôle, porozumenia a schopností protivníka alebo iných cieľových skupín a zároveň chránia vlastné sily pred týmto ovplyvňovaním. Riadia sa usmerneniami vychádzajúcimi zo strategickej úrovne, sú naplánované predovšetkým na operačnej úrovni a vedené na operačnej a taktickej úrovni velenia. Vždy musia podporovať ciele strategickej komunikácie. Informačné aktivity na všetkých úrovniach vedenia vojny musia sledovať hlavný a jednotný strategický naratív, čiže príbeh" (Řehka, 2017, s. 137).

Informačné operácie sú vo svojom modernom ponímaní aj v NATO stále relatívne mladou disciplínou, predovšetkým v porovnaní s verejnými záležitosťami a psychologickými operáciami. Oproti strategickej komunikácii sú metodicky prepracovanejšie a majú svoju vlastnú doktrínu, v jej implementácii je však stále čo doháňať a v jednotlivých členských krajinách nie je táto schopnosť na rovnakej úrovni. „Okrem iného je dôležité vycvičiť vyšší počet odborníkov na túto oblasť a zabezpečiť jej širšie chápanie medzi vojenskými veliteľmi a ich štábmi" (Řehka, 2017, s. 137).

3.1 DEZINFORMÁCIE NA SOCIÁLNYCH SIEŤACH

'sociálne siete sú novou zbraňou moderného konfliktu...'

Dnešný svet je charakterizovaný rýchlym a ľahkým prístupom k informáciám. Túto rýchlosť niekoľkonásobne zvýšil nástup sociálnych sieti. Tie zmenili spôsob ako sú ľudia informovaní, no najmä ako spracúvajú realitu – a spôsob akým sa zapájajú do verejnej diskusie. Ľudia na sociálnych sieťach majú tendenciu vnímať informácie, ktoré súvisia s ich preferovanými naratívmi a zároveň ignorovať iné protichodné názory či informácie. Táto zaujatosť má vplyv na ďalšie šírenie obsahu.

Dezinformácie sú neoddeliteľnou súčasťou moderných informačných operácií. Ide o koordinované, dobre organizované a plánované aktivity zamerané na ovplyvňovanie cieľového publika. Na šírenie dezinformácií sa využívajú rôzne kanály. Sociálne siete ako také sú zvyčajne koncovým bodom a výstupom, no šírenie dezinformácií sa realizuje hlavne prostredníctvom rôznych outletov a 'alternatívnych' spravodajských portálov, z ktorých je obsah ďalej preberaný a šírený.

Dezinformácie majú rôzne účely. Napríklad polarizácia spoločnosti, destabilizácia vlády, pokrivenie spoločenských hodnôt, ale aj odvádzanie pozornosti od iných vážnych tém. Dezinformácie sa objavujú naprieč celým spektrom oblastí spoločenského života od rôznych zdravotných tém, technologických tém, geopolitiky, až po krajné konšpiračné teórie. Markantným príkladom dezinformačných trendov posledných rokov sú tie spojené s COVID, jeho vznikom, alebo vakcínami. Cieľom je – okrem polarizácie spoločnosti – aj zahmlievanie závažnosti situácie (napr. čínske dezinformácie o vzniku, pôvode a zvládaní pandémie v jej začiatkoch, cielené kampane na kompromitáciu západných vakcín v prospech Sputnik V atď.).

Takéto nastavenie prostredia zvýhodňuje aktérov, ktorých stratégia cieli na extrémnu mobilizáciu vlastných podporovateľov a demobilizáciu podporovateľov oponentov. Prostredníctvom kognitívnych dezinformačných operácií zahraniční aktéri cielia na skupiny náchylnejšie k radikalizácii a rozvracajú spoločnosť, alebo publikum protivníka. Problematické

algoritmy sociálnych sietí tak vytvárajú priestor plný slabín, zvýhodňujúci dezinformačný obsah, ktorý je naplno zneužívaný škodlivými aktérmi vo vlastný prospech.

Zneužívanie dezinformácii exponenciálne narastá. Lídri, politici a novinári zodpovední za iniciovanie a formovanie verejnej diskusie tiež prispievajú – často nevedome – k podnecovaniu ideologických bublín. To je mimoriadne alarmujúce, najmä v čase, keď sa dezinformácie môžu stať otázkou života a smrti.

3.2 SPÔSOBY ŠÍRENIA DEZINFORMÁCIÍ

Komercializácia správania na sociálnych sieťach

Nákup lajkov, zhliadnutí a followerov a tým ovplyvňovanie diskusií na sociálnych sieťach. Algoritmy sociálnych sietí preferujú obľúbený a komentovaný obsah. Takému následne dávajú viac priestoru.

Príklad experimentu NATO STRATCOM COE poukazuje na fakt, ako si za 300 € výskumníci kúpili 3.530 komentárov, 25.750 lajkov, 20.000 zhliadnutí a 5.100 followerov. V tomto aspekte zlyhávajú najmä sociálne siete. Aj napriek tomu, že účty vykazovali podozrivé správanie boli po štyroch týždňoch od zakúpenia 4 z 5 služieb stále aktívne. 95% nahlásených účtov bolo aktívnych aj po troch týždňoch od nahlásenia neautentického správania.

Digitálny astroturfing

Astroturfing označuje metódu, ktorá ovplyvňuje spotrebiteľské správanie či politické preferencie tým, že daný subjekt sa snaží vyvolať dojem autentickosti a spontánneho pôvodu ‘zdola‘. V skutočnosti je však takáto kampaň profesionálne organizovaná. Mnohé skupiny na sociálnych sieťach sa tvária ako hnutia zdola s vôľou zmeniť lokálnu politiku, no v realite môžu cielene manipulovať verejnú mienku a polarizovať masy. Spolu s netransparentnými skupinami sa objavuje aj personalizovaná propaganda prostredníctvom micro–targetingu reklám. Príkladom sú skupiny na Facebooku vytvorené ruskou trolliou farmou IRA. Jednou z nich bola skupina Heart of Texas, ktorá mala zlučovať secesionistické hnutie Texasu, no v skutočnosti propagovala konšpiračné teórie, krajne pravicovú ideológiu, xenofóbiu, anti–LGBT a anti–moslimskú rétoriku.

Zaplavenie zóny a využívanie botov

Škodliví aktéri pomocou infikovaných počítačov dokážu kontinuálne zaplavovať sociálne siete dezinformačným obsahom. Tento fenomén v kombinácii so všeobecne chýbajúcimi znalosťami o fungovaní algoritmov, či ich netransparentnosťou a umelou inteligenciou, ktorá reguluje obsah, predstavuje ďalší významný problém. K ‘zaplaveniu zóny‘ sa využívajú napríklad boti – účty, ktoré generujú závadový dezinformačný obsah automatizovane. Botneti, čiže skupiny či siete botov, prostredníctvom dosahu na sociálnych sieťach vedia rozšíriť dezinformácie veľkou rýchlosťou. Sú najčastejšie viditeľní na Twitteri, pred časom sa objavili už na Instagrame. Ďalším podobným úkazom sú trollovia – reálne osoby, ktoré iniciujú konflikt a znemožňujú diskusie v online priestore, často prostredníctvom zdieľania dezinformácií. Trollovia takto ďalej polarizujú ostatných užívateľov. Populárni sú najmä na Facebooku a diskusných fórach.

Mediálne trojské kone

Existujú falošné webové stránky, ktoré sa tvária ako relevantné médiá, no šíria dezinformácie a propagandu. Zvyčajne ide o lokálne noviny, ktoré sa prezentujú ako nezávislé, no témy a smerovanie článkov sú diktované priamo zo zahraničia.

Source hacking

Spôsob manipulácie obsahu, aby akceleroval s čo najväčším dosahom na sociálnych sieťach bez vzbudzovania podozrení. Primárnym cieľom sú novinári a iné vplyvné osobnosti, ktoré následne prevezmú konkrétny obsah a ponúknu ho širšiemu publiku. V známom prípade Macron Leaks dva dni pred francúzskymi prezidentskými voľbami unikla kombinácia pravých aj falošných dokumentov, ktoré mali dokázať daňové podvody Emmanuela Macrona. Cieľom bolo zdiskreditovať jeho kampaň počas volebného moratória, kedy sa francúzske médiá k obsahu nemôžu vyjadriť. Na sociálnych sieťach však dokumenty cirkulovali s obrovským dosahom.

Získavanie influencerov

Získavanie známych osobností na vlastnú stranu má zásadný dopad v offline aj online svete. Štúdia Oxford's Reuters Institute odhalila, že k šíreniu dezinformácií o koronavíruse najviac napomáhajú influenceri a celebrity. Aj napriek tomu, že zo všetkých šíriteľov dezinformačného obsahu predstavujú celebrity len 20 % percent, ich posty generujú až 69 % interakcie na sociálnych sieťach. Príklad: V Českej republike sa v kontexte koronavírusových dezinformácií zviditeľnila speváčka Ilona Csáková, ktorá predstavuje skupinu ľahko ovplyvniteľných celebrít. Vhodným cieľom pre nepriateľských aktérov sú práve ašpirujúci či začínajúci influenceri. Výmenou za technologickú či finančnú pomoc tak aktéri získajú ďalšie publikum dezinformačných naratívov.

3.3 ZÁKLADNÉ POJMY V DEZINFORMAČNOM SVETE

Falošné správy – informácie, ktoré zámerne napodobňujú formát spravodajstva alebo iného produktu žurnalistiky, pričom ich tvorcovia úmyselne alebo neúmyselne zavádzajú svoje publikum. Ich šírením navyše skresľujú realitu.

Dezinformácie – (slovenský ekvivalent: úmyselne falošná informácia, anglický ekvivalent: disinformation) – nepravdivá alebo zmanipulovaná informácia, ktorá je vytvorená a zámerne šírená s jednoznačným úmyslom spôsobiť ujmu. Producenti dezinformácií sú zvyčajne motivovaní politickými, ekonomickými, sociálnymi či psychologickými faktormi. Môže ísť o informáciu v podobe textu, obrazu, videa, grafiky alebo zvuku.

Konšpiračná teória – (slovenský ekvivalent: konšpirácia, anglický ekvivalent: conspiracy theory) teória, ktorá vysvetľuje udalosť alebo súbor okolností ako výsledok tajného sprisahania (konšpirácie) zvyčajne malou mocnou skupinou osôb. Takouto skupinou má byť zväčša vláda, predstavitelia tajných spolkov, organizácií alebo služieb, jedna alebo viacero spoločne pôsobiacich firiem alebo predstavitelia štátov, národov alebo náboženstiev, či dokonca mimozemské civilizácie. Konšpiračné teórie odmietajú všeobecne akceptované vysvetlenie takýchto udalostí.

Hoax – (slovenský ekvivalent: podvod, klamlivá správa) – falošná správa alebo úmyselné klamstvo, ktoré sa spolieha na ochotu ľudí niečomu uveriť. Virálne rozšírená poplašná správa, ktorá je podmnožinou dezinformácie. Je trestnoprávne postihnuteľná a nemusí sa zakladať na realite.

Propaganda – informácia, idea, názor alebo vizuálny materiál, ktorý je vytvorený s účelom ďalšej distribúcie, zväčša uvádza iba jednu časť argumentu a jeho cieľom je ovplyvniť názory ľudí.

Malinformácia – (slovenský ekvivalent: škodlivá informácia, anglický ekvivalent: malinformation) – informácia, ktorá je založená na realite, šírená zámerne s cieľom spôsobiť ujmu osobe, organizácii alebo štátu, napr. uniknuté informácie, nenávistné prejavy, obťažovanie. Skutočná informácia, ktorá je verejne zdieľaná s úmyslom spôsobiť ujmu. Patria sem súkromné informácie, ktoré sa šíria tak, aby poškodili druhú stranu alebo jej povesť.

Misinformácia – (slovenský ekvivalent: neúmyselne nepravdivá informácia, anglický ekvivalent: misinformation) – informácia, ktorá je nesprávna/nepravdivá, avšak jej zámerom nie je úmyselne spôsobiť ujmu. Napríklad ide o prípady, kedy jednotlivci na sociálnych sieťach v snahe pomôcť šíria informácie bez toho, aby vedeli o tom, že sú nepravdivé.

Trol – (anglický ekvivalent: troll) – užívateľ internetu, ktorý svojimi komentármi a správaním na internete zámerne provokuje ostatných, alebo odvádza diskusiu od pôvodnej témy pod skutočnou, ale aj falošnou identitou.

Trolovanie (anglický ekvivalent: trolling) – akt zámerného urážlivého alebo poburujúceho správania sa v online komunite s cieľom vyprovokovať čitateľov alebo narušiť konverzáciu.

Weaponizácia – útočenie nepriateľskými informáciami na cieľovú skupinu, mobilizácia, šírenie naratívov, vedenie informačných operácií s cieľom ovplyvňovania správania, postojov, nálad a názorov svojej cieľovej skupiny.

4 PODPORNÉ RIEŠENIA BOJA PROTI HYBRIDNÝM HROZBÁM

Strategická komunikácia

Strategická komunikácia v krajine musí byť jednotná, koordinovaná s komunikáciou rezortov a vykonávaná nepretržite a proaktívne. Je nevyhnutné vybudovať dostatočne veľké kapacity a oddelenia strategickej komunikácie – výkonné prvky, ktoré budú aktívne a moderne komunikovať témy, ktoré im prináležia. Dnes je možné ešte stále konštatovať, že strategická komunikácia na úrovni štátu neexistuje a 30 rokov, teda od vzniku SR ani neexistovala, i keď za posledné roky sa pre jej budúce štruktúry urobili prvotné kroky.

Hlavným predpokladom pre personál STRATCOM musí byť vzdelanie – teda získanie odborníkov na komunikáciu, sociálne siete, dátovú analýzu, grafikov a pod. Jednou z pravdepodobných ciest k úspechu je ich získavanie podobným spôsobom ako odborníkov na cyber defence. Objem finančných prostriedkov na vykonávanie takýchto aktivít musí byť dostatočne veľký, aby obsiahol vzdelanie, kurzy, technické zabezpečenie (internet, PC, telefóny), tvorbu platených informačných kampaní (tzv. boostovanie príspevkov), analytické softvéry...

Vzdelávanie v oblasti dezinformácií a rozvoj kritického myslenia

Je mimoriadne dôležité rozvíjať zručnosti spoločnosti v oblasti kritického myslenia a mediálnej či informačnej gramotnosti.

Paleta je pestrá: využívanie moderných technológii a aplikácii, vrátane počítačových hier, vytvorených za účelom podporenia kritického myslenia, či rozlišovania pravdivých a nepravdivých informácii, ako aj možnosti uplatňovania umelej inteligencie na odhaľovanie falošných správ.

Nezaobídeme sa však bez operatívnej činnosti bezpečnostných zložiek proti dezinformačným médiám a zavedenia funkčných právnych noriem a zákonov s adekvátnou vymožiteľnosťou.

Monitorovacia činnosť a analytika

Ďalšou skupinou nástrojov sú softvérové riešenia – dnes absolútne nevyhnutná podmienka. Takéto softvérové nástroje musia byť spôsobilé monitorovať informačný priestor 24/7 s využitím AI (umelá inteligencia, z angl. artificial intelligence).

Monitorovacie a analytické činnosti si vyžadujú:

- identifikovanie dezinformačných médií a vytváranie databáz falošných správ,
- používanie výstražných systémov na informovanie vládnych úradníkov a novinárov o nových dezinformáciách,
- zvolávanie pravidelných workshopov pre štátnych zamestnancov,
- odhaľovanie ‘kto stojí za webmi šíriacimi dezinformácie‘.

ZÁVER

Jedným z najdôležitejších aspektov boja proti hybridným hrozbám je posilnenie medzirezortnej spolupráce a koordinácie. To zahŕňa vytvorenie systémov a mechanizmov, ktoré umožnia rýchlu a efektívnu reakciu na zistené hrozby. Spolupráca medzi verejným a súkromným sektorom je nevyhnutná, pretože súkromné subjekty často disponujú technológiami a expertízou, ktoré môžu byť neoceniteľné pri ochrane pred kybernetickými útokmi. Bez efektívneho zdieľania informácií a zdrojov nebude možné dosiahnuť požadovanú úroveň bezpečnosti.

Rovnako dôležitá je aj angažovanosť občianskej spoločnosti, ktorá hrá kľúčovú úlohu pri zvyšovaní povedomia o rizikách spojených s hybridnými a kybernetickými hrozbami. Vzdelávanie a rozvoj mediálnej gramotnosti sú kritické pre budovanie odolnosti spoločnosti voči dezinformáciám a manipuláciám. Iniciatívy, ktoré sa zameriavajú na posilnenie kritického myslenia, sú nevyhnutné pre zabezpečenie, aby občania mohli identifikovať a reagovať na dezinformácie, ktoré môžu ohroziť demokratické hodnoty a stabilitu spoločnosti. Na zabezpečenie efektívneho boja proti hybridným hrozbám je potrebné neustále monitorovať a aktualizovať existujúce legislatívne rámce. To si vyžaduje systémový prístup, ktorý umožní adaptáciu na meniace sa podmienky a výzvy. V tejto súvislosti stojí za úvahu posilnenie kapacít štátnych inštitúcií, ktoré sú zodpovedné za ochranu kybernetickej bezpečnosti a zabezpečiť, aby mali dostatočné zdroje na plnenie svojich úloh.

Medzinárodná spolupráca je tiež kľúčovým aspektom efektívneho boja proti hybridným a kybernetickým hrozbám. Slovenská republika by mala aktívne participovať na medzinárodných iniciatívach, ktoré sa zaoberajú zdieľaním informácií, technológií a osvedčených praktík. Týmto spôsobom môže získať prístup k novým zdrojom a odborným znalostiam, ktoré sú potrebné na posilnenie jej obranných kapacít.

Celkovo sa dá konštatovať, že hybridné a kybernetické hrozby predstavujú vážnu výzvu pre bezpečnostné prostredie Slovenskej republiky. Prijaté opatrenia a stratégie sú krokom správnym smerom, ale ich úspech závisí od schopnosti štátu, súkromného sektora a občianskej spoločnosti spolupracovať a koordinovane reagovať na tieto hrozby. Iba tak môžeme zabezpečiť, aby Slovenská republika zostala odolná voči hybridným útokom a dokázala ochrániť svoje demokratické inštitúcie a hodnoty.

Pri problematike ovplyvňovania vnútropolitickej situácie, netransparentnej a skrytej podpore politických subjektov zo strany cudzích mocí a činiteľov, vrátane podpory pre polovojenské a extrémistické skupiny, je potrebné pripomenúť, že takáto podpora v súčasnosti nie je v Slovenskej republike v dostatočnej miere sankcionovaná. Cieľom opatrení môže byť

rozšírenie možností na vyhostenie, udelenie zákazu vstupu na územie Slovenskej republiky, či zaradenie osôb, ale aj členov takýchto organizácií, na zoznam subjektov, ktorým je odopretý vstup aj do celého Schengenského priestoru.

Séria opatrení, ktoré majú zmierniť hybridné pôsobenie cudzích aktérov v Slovenskej republike, spočíva aj v plošnom stransparentnení finančných tokov a investícií v relevantných doménach, napríklad v médiách, energetike a iných entitách kritickej infraštruktúry, v rozšírení trestnosti prvku cudzej moci do trestného zákona.

Kybernetické hrozby už dávno nie sú len záležitosťou špeciálnych systémov a profesionálov v oblasti informačných technológií. Týkajú sa každého z nás. Kybernetická bezpečnosť musí byť spoločnou zodpovednosťou štátu a jeho občanov. Útoky cudzích mocností, ale aj aktivity kybernetických zločincov majú signifikantný dopad na naše bežné fungovanie. K základným strategickým záujmom Slovenskej republiky musí patriť udržiavanie a zdokonaľovanie systému kybernetickej bezpečnosti tak, aby hrozby, zraniteľnosti a incidenty mali čo najmenší dopad na štát a jeho občanov, ako aj na fungovanie spoločenského zriadenia.

Iba vytvorením a udržiavaním reálneho a funkčného, dostatočne plochého a zároveň hlbokého systému aktérov na poli boja proti hybridným hrozbám je možné s úspechom zamedzovať, resp. predchádzať, hybridným útokom.

Predpokladaný vývoj systému ochrany Slovenskej republiky pred hybridnými a kybernetickými hrozbami bude ovplyvnený viacerými kľúčovými faktormi, medzi ktoré patrí technologický pokrok, geopolitické zmeny a vývoj hrozieb v rámci hybridnej vojny. V nasledujúcich rokoch sa očakáva posilnenie kybernetickej bezpečnosti a ochrany kritickej infraštruktúry, pričom pokročilé systémy na detekciu a reakciu na kybernetické útoky budú hrať hlavnú rolu. Zároveň sa zvýši dôležitosť využívania umelej inteligencie a strojového učenia, ktoré pomôžu neutralizovať hrozby ešte pred tým, ako spôsobia závažné škody.

Veľký dôraz sa bude klásť na verejno-súkromné partnerstvá, keďže značná časť digitálnej infraštruktúry je v rukách súkromného sektora. Aj preto bude nevyhnutné rozvíjať spoluprácu medzi štátnymi a súkromnými subjektmi s cieľom chrániť strategicky dôležité systémy pred kybernetickými útokmi.

Jednou z najväčších výziev v oblasti hybridných hrozieb sú dezinformácie a psychologické operácie. Očakáva sa, že Slovenská republika bude používať pokročilé nástroje na monitorovanie a neutralizáciu dezinformácií šírených v online priestore. Tieto nástroje budú schopné v reálnom čase identifikovať a blokovať falošné informácie, čím sa zvýši informačná bezpečnosť verejnosti. Zároveň sa bude zvyšovať význam vzdelávacích kampaní zameraných na posilnenie kritického myslenia občanov, aby boli schopní rozpoznať manipulácie a odolať im.

Ďalší vývoj v oblasti obrany bude zahŕňať inovatívne stratégie, pričom Slovensko zintenzívni výcvik špecializovaných jednotiek v oblasti kybernetickej bezpečnosti a hybridných hrozieb. Spolupráca s medzinárodnými partnermi, ako sú NATO a EÚ, bude kľúčová pre posilnenie strategických schopností krajiny. V súvislosti s hybridnými hrozbami sa očakáva aj úprava legislatívneho rámca, ktorá bude zahŕňať nové zákony a sankčné mechanizmy zamerané na potlačenie kybernetických útokov a dezinformačných kampaní.

V rámci posilňovania obrany bude nevyhnutné rozvíjať medzinárodné aliancie a zintenzívniť zdieľanie informácií o hrozbách. Slovensko sa pravdepodobne viac zapojí do medzinárodných iniciatív, ktoré umožnia lepšiu koordináciu reakcií na hybridné útoky. Dôležitou súčasťou tejto stratégie budú spoločné cvičenia na simuláciu hybridných útokov, čím sa posilnia schopnosti krajiny reagovať na podobné scenáre v budúcnosti.

Celkovo sa očakáva, že systém ochrany Slovenskej republiky pred hybridnými a kybernetickými hrozbami sa bude vyvíjať smerom k flexibilnejšiemu, technologicky pokročilejšiemu a legislatívne podloženému prístupu. Tento vývoj bude nevyhnutný pre zabezpečenie odolnosti Slovenskej republiky voči novým formám hybridných hrozieb.

Na záver je dôležité zdôrazniť, že kybernetická bezpečnosť a obrana proti hybridným hrozbám nie sú iba úlohou štátu, ale aj zodpovednosťou každého jednotlivca. Posilnením nášho povedomia a vzdelanosti v tejto oblasti môžeme spoločne prispieť k vytvoreniu bezpečnejšej a odolnejšej spoločnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

MINISTERSTVO OBRANY SR: *Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024*. [online]. Dostupné na internete: https://www.hybridnehrozby.sk/wp-content/uploads/2023/09/APHH-2022.pdf [cit. 2024-07-10]

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Akčný plán realizácie: Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, Národný bezpečnostný úrad*. [online]. Dostupné na internete: https://www.nbu.gov.sk/data/att/2760.pdf [cit. 2024-07-10]

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD: *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025*. [online]. Dostupné na internete: https://www.nbu.gov.sk/data/att/2759.pdf [cit. 2024-07-10]

PAŽICKÝ, M. 2021. *Hybridné hrozby ako determinanty strategickej komunikácie v podmienkach bezpečnostného prostredia Slovenskej republiky*. Záverečná práca. Akadémia ozbrojených síl generála Milana Rastislava Štefánika.

ŘEHKA, K. 2017. *Informační válka.* Praha: Academia, 2017. 218 s. ISBN 978-80-200-2770-2.

Mgr. Mário Pažický, EMBA
externý doktorand, Katedra bezpečnosti a obrany
Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 01 Liptovský Mikuláš, SR
mario.pazicky@me.com