Miroslav Lisoň, Ľudovít Fidler

Potreba a možnosti identifikácie rizík z realizácie hybridných hrozieb

Anotácia: Autori v predkladanej štúdii zdôrazňujú, že vzhľadom k spoločenskej závažnosti rizík vyplývajúcich z realizácie hybridných hrozieb, od policajno-bezpečnostných orgánov občan oprávnene očakáva, že akceptáciou delegovaných kompetencií ich dokážu identifikovať, a tým participovať pri realizácii adekvátnych opatrení v systéme kontroly týchto foriem protispoločenských konaní (v oblasti prevencia, represia). Akceptujúc uvedené, spracovaním názorov oslovených príslušníkov kompetentných policajno-bezpečnostných orgánov a odbornej verejnosti, predkladajú možnú alternatívu postupov realizovaných za účelom identifikovania hybridných hrozieb.

Kľúčové slová: identifikovanie, hrozba, riziko, hybridná hrozba, aktéri hybridných hrozieb, kybernetická bezpečnosť, energetická bezpečnosť, paramilitárne a extrémistické skupiny, strategická korupcia, ovplyvňovanie volebných procesov, Národný bezpečnostný úrad.

Úvod

Vo všeobecnosti je možné uviesť, že ak chce niekto nájsť liek na určitú chorobu, odstrániť niečo nežiaduce, je povinný to objektívne diagnostikovať (*identifikovať*), a to z pohľadu ich možností a schopností. Určite v odbornej verejnosti nik nepochybuje, že hybridné hrozby predstavujú významný prostriedok, ktorý rôzne subjekty (*fyzické, právnické osoby, dokonca štáty*) používajú pri presadzovaní a dosahovaní spoločensky neakceptovateľných záujmov. Vo vzťahu k ochrane spoločnosti, ktorá korešponduje s uplatňovaním princípov *slobody, demokracie, humanizmu a práva,* je vhodné tieto činnosti charakterizovať, ako intencionálne aktivity. Ich štruktúrovaný realizačný obsah tvoria špecifické znaky, osobitne *motívy, účel, ciele, postupy charakterizujúce prípravu, dokonanie a sledovanie účinkov a efektov*. To znamená, že tieto činnosti je možné poznávať prostredníctvom identity ich ontologických a gnozeologických vlastností (*realizátori a participujúce subjekty svojim konaním spôsobujú odrazy*) a toto poznanie následne použiť pri eliminovaní sledovaných protispoločenských účinkov.

V syntéze túto realitu rešpektujeme v predkladanej štúdii. Pri jej spracovaní sme využili výstupy štúdií publikovaných informácií v našej a zahraničnej odbornej literatúre, ktoré sme konfrontovali (*aplikáciou logických operácií*) so získaným poznaním názorov príslušníkov Národného bezpečnostného úradu (*5 respondentov*), Vojenského spravodajstva (*5 respondentov*), Slovenskej informačnej služby (*5 respondentov*) a Policajného zboru (*10 respondentov*), ako aj neformálnou diskusiou s občanmi.

Našou ambíciou je touto prezentáciou zapojiť sa do diskusie, ktorej objektom je spoločenská závažnosť hybridných hrozieb a možnosti ich účelového poznávania. Osobitne v tomto smere zvýrazňujeme význam našich aktivít, ktorý je spájaný s konštruktívnou komunikáciou s občanmi. Celkom sme oslovili formou riadeného rozhovoru 20 občanov, obyvateľov Bratislavy (*1. skupina - 10 respondentov vo veku od 30-50 rokov, 2. skupina – 10 respondentov starších ako 50 rokov*). Nami oslovení respondenti na našu otázku: *„Poznáte význam zloženého termínu „hybridná hrozba“?“* pri hľadaní odpovedí používali jeho sémantický výklad (*krížené hrozby – 75 % respondentov, z 1. sk. 7, 2. sk. 8*).[1] Pri zdôvodňovaní tohto prístupu uviedli, že termín v médiách registrujú v diskusiách, ktorých účastníkmi sú politici a novinári. K uvedenému dodali, že vzhľadom k používaným rôznym argumentom, ktoré nekorešpondovali s vymedzenou témou, paradoxne z týchto diskusií

[1] 5 respondentov (občanov) termín *hybridné hrozby* charakterizovalo ako činnosť (*prostriedok*), ktorú štátne služby alebo iné subjekty používajú k ovplyvňovaniu konania a správania sa verejnosti.

nedokázali pochopiť jeho presný význam. Dokonca sú presvedčení, že ani sami diskutéri význam používaného termínu nepoznajú komplexne, nedokázali ho systémovo, najmä vo vzťahu k možným následkom, hrozbám, a pod. vysvetliť.

.

1 Hybridné hrozby a ich aktéri

Ohrozenie a riziko sú javmi, s ktorými sa človek stretáva vo svojom životnom kolobehu takmer v každej situácii. Činnosti, ktoré bežne alebo účelovo vykonáva, nie sú priamočiare, ale môžu byť veľmi rozmanité a často protikladné. A práve v tejto protikladnosti spočívajú i javy, ktoré sú označované termínmi ohrozenie a riziká. Hrozby a riziká sa vyskytujú v prostredí, či už ide o verejno-spoločenské, hospodárske, životné prostredie a iné. V spoločenskom prostredí ide o riziká politické, ideové, kultúrne, etnické, nadnárodné a pod. V hospodárstve sú to riziká spojené s trhovým hospodárstvom, riziká menové, inflačné, úverové či podnikateľské riziká. V prírodnom a životnom prostredí ide o riziká spojené s bytím človeka v prírode a s jeho ohrozením prírodou. Osobnosti, ako spoločenské indivídua, sú taktiež sústavne ohrozované spoločenským prostredím, ale aj vlastným osobným fyzickým i psychickým stavom a pod.

V systémovom vyjadrení, riziká a ohrozenia sú kategórie (*existujú, sú poznateľné*), pomocou ktorých je možné vymedziť narušenie bezpečnosti v štáte (*spoločnosť, občan, právo, sloboda, demokracia, humanizmus*). Riziko vyjadruje možnosť ohrozenia dôsledkami rôznych aktivít (*udalostí a krízových javov*). V konkrétnom ponímaní predstavuje očakávané škody a straty (*na životoch, zdraví, škody na majetku, v ekonomike, morálke, ...*) zavinené spoločenskou situáciou, t. j. zmenou vonkajších a vnútorných podmienok, spôsobené aktivitami v konkrétnom priestore a čase (*udalosťou a jej dôsledkami*).[2]

Riziko je kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera hrozby. Je to predpoklad vzniku udalosti a jej dôsledkov (*je spojené s početnosťou a rozsahom udalostí*), ktoré sú eminentnými (*obligatórnymi*) prvkami spoločenskej situácie. V daných súvislostiach situácia predstavuje súbor faktorov, ktoré ovplyvňujú existenciu a prejavy existencie rizikových javov. Z uvedených dôvodov je pri skúmaní rizík potrebné vziať do úvahy čas, priestor a príčiny, podmienky a okolnosti ich vzniku.

Hybridná hrozba sa vzťahuje na činnosť vykonávanú štátnymi alebo neštátnymi subjektmi, ktorej cieľom je poškodiť vymedzený objekt ovplyvňovaním jeho rozhodovania na miestnej, regionálnej, štátnej alebo inštitucionálnej úrovni.[3]

Z analogického výkladu tejto charakteristiky je zrejmé, že v daných súvislostiach hybridná hrozba predstavuje 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. Vo vzťahu k týmto skutočnostiam je možné uviesť, že hybridná hrozba predstavuje realitu, ktorú je možné posudzovať z hľadiska realizácie konkrétnych aktivít, ako aj dosiahnutými účinkami a efektmi súvisiacimi s použitím tohto prostriedku v konkrétnom čase a priestore (*v realizačnom štruktúrovanom systéme - vo východiskovom, výkonnom a výstupnom štádiu*). Jej aktérom, aktívnym účastníkom je štátny alebo neštátny subjekt. Vzhľadom k existujúcim politickým zvyklostiam medzi štátnymi aktérmi, významnú pozíciu a rolu zohráva subjekt (*na určitej politickej pozícii*),

[2] BUZALKA, J. 2012. *Teória bezpečnostných rizík*, s. 10.

[3] *Hybridné hrozby.* 2021. Dostupné [online] z: http:// www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html

ktorý vydá rozhodnutie o potrebe realizácie tejto činnosti pre konkrétne orgány štátnej správy (*osobitne spravodajské služby*). Samozrejme, toto rozhodnutie môžu príslušníci spravodajských služieb ovplyvniť (*iniciovať*) výsledkami analýz existujúcej a predestinovanej spoločensko-politickej, ekonomickej, bezpečnostnej a inej situácie, ktoré pre rozhodovací orgán vypracujú a pod. Je nepravdepodobné, aby do tejto činnosti neboli zapojení príslušníci spravodajských služieb, pretože eventuálne by mohli použitie tohto prostriedku (*a to už aj v jej východiskovom štádiu*) paralyzovať. Inú skupinu aktérov hybridných hrozieb tvoria subjekty, ktoré nevykonávajú činnosť v pozícii orgánov štátnej správy. V tejto činnosti pri rozhodovaní a používaní tohto prostriedku je u nich iná motivácia, sledovaný účel a vytýčené ciele. Osobitne práve tieto znaky používania hybridných hrozieb vykazujú špecifiká v jeho východiskovom štádiu. Nami oslovení odborníci z policajno-bezpečnostnej praxe nám potvrdili, že v ďalších znakoch *modus operandi* vo výkonnom štádiu a výstupoch rozdiely nie sú registrované.

Je zrejmé, že motívy (*vnútorná pohnútka – preto lebo*), účel (*preto, aby*) a ciele používania hybridných hrozieb sú obligatórne znaky tohto špecifického konania. Motív a účel sú priamo spájané s jeho realizátormi (*aktérmi*), cieľ nielen s aktérmi, ale aj adresátmi. Totižto aktéri chcú jeho použitím dosiahnuť konkrétny cieľ, ktorý stanovujú na základe analýzy situácie, a to vo vzťahu k záujmom adresáta, a to aj bez formálneho vyhlásenia vojny - agresie.[4] Účelovo, v tomto konštatovaní je uvedená eventualita, pretože na použitie tohto prostriedku pôsobí celý rad faktorov, ktorých syntézu tvorí prostredie (*spoločenské, ekonomické, politické, bezpečnostné, kriminálne a iné, ktorých štruktúru tvorí situácia a udalosti*), a to rôznou intenzitou a charakterom (*objektívne, subjektívne*). Na základe štúdia odbornej literatúry, ako aj z výsledkov riadenej komunikácie s odborníkmi, ktorí v podmienkach Slovenskej republiky skúmajú, hodnotia a vysvetľujú existenciu hybridných hrozieb, sme dospeli k jednoznačnému záveru, ktorý využívame pri charakteristike ich ďalšieho povinného znaku.

Podľa nášho názoru, hybridnú hrozbu netvorí použitie ozbrojenej sily voči protivníkovi s cieľom ovládnuť alebo podrobiť si ho. Nasadenia ozbrojených síl funkčne predstavujú formy vojny, napríklad anexie - *násilné pripojenie územia alebo časti územia iného štátu jednostranným aktom anektujúceho štátu, a to v rozpore s medzinárodným právom*. Použitím hybridných hrozieb sú vytvárané vhodné logistické podmienky pri dosahovaní týchto cieľov.

2 Registrované formy hybridných hrozieb

V súčasnosti existujú desiatky foriem 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 pôsobenia môžu byť *masívne dezinformačné kampane*[5] *a využívanie sociálnych médií na propagandu alebo radikalizáciu, nábor a priame ovládanie vytypovaných adresátov*. O hybridnú hrozbu môže ísť, ak ich aktéri pri napĺňaní stanoveného účelu a dosahovaní vytýčených cieľov používajú aj iné formy násilia.

---

[4] *Hybridné hrozby*. 2021. Dostupné [online] z: http:// www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html

[5] *Hybridné hrozby*. 2021. Dostupné [online] z: http:// www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html

Z informácií, ktoré publikujú pracovníci Národného bezpečnostného úradu (*potvrdzujú to aj účastníci GLOBSEC Bratislava - Global Security Forum*) z hľadiska závažnosti pre spoločnosť v našom štáte predstavujú mimoriadne hrozby zahraničné zasahovania do informačného priestoru (*slovenský ekvivalent: foreign manipulative interference in the information space*). V danom prípade, za použitia rôznych techník manipulácie a nástrojov sú realizované škodlivé útoky (*narúšanie slobodného formovania a vyjadrenia politickej vôle jednotlivcov*) zahraničným štátnym aktérom alebo jeho agentmi, často ako súčasť širšej hybridnej operácie v priestoroch šedej zóny.[6]

Týmito skutočnosťami sme sa snažili zvýrazniť, že hybridné hrozby sú rôznorodé. Aktéri ich použitím pôsobia na adresátov *naprieč doménami infraštruktúry kybernetického priestoru*[7]*, vesmíru, ekonomiky, obrany, kultúry, spoločnosti, verejnej správy, práva, spravodajských služieb, diplomacie, politiky a informácií.*

Slovenská republika sa najčastejšie stretáva s pokusmi o ovplyvňovanie verejnej mienky, a to nielen v kybernetickom prostredí, ktoré má samo o sebe hybridnú povahu (*nie je vlastnený ani prevádzkovaný výlučne verejnými alebo súkromnými subjektmi*), ale aj na iné, akceptujúc vzniknuté a vznikajúce situácie a prebiehajúce udalosti v spoločnosti.

K objektivizácii uvedeného uvádzame niektoré formy, na ktoré nás v procesoch riadeného rozhovoru orientovali odborníci z policajno-bezpečnostnej praxe. Tí na našu otázku: *„Ktoré formy hybridných foriem registrujú u nás?*“ uviedli[8]:

1. Kybernetická bezpečnosť

Informačné a komunikačné technológie predstavujú vzhľadom na ich vplyv na chod štátu jeden z hlavných cieľov hybridného útoku na krajinu. Útočiaca krajina je s relatívne nízkymi nákladmi a z bezpečia kancelárií domovskej krajiny schopná spôsobiť rozsiahle ekonomické škody, dokonca až ochromiť chod krajiny. Útoky (*napríklad znefunkčnenia štátnych webstránok zahltením, ...*) sú realizované v dôsledku politických kríz medzi spoločenstvom štátov, resp. bipolárnymi štátmi.[9] Za dôležité je možné uviesť, že útoky týmito formami smerujú do virtuálneho sveta.[10]

Tieto názory potvrdzujú aj renomovaní odborníci, ktorí konštatujú, že funkčnosť štátov je pod stálymi hrozbami, pretože je závislá na informačno-komunikačných technológiách. Tieto predstavujú účinný prostriedok v medzinárodných konfliktoch.[11]

---

[6] Pod pojmom „*Šedá zóna*“ označujeme prostredie, v ktorom sa vedie politická a informačná vojna, pričom sa využíva nejednoznačnosť vnútroštátneho a medzinárodného práva. Konanie štátu (*využitím účelovo motivovaných aktérov, frekventovane pôsobiacich v prostredí adresátov)*, ktoré škodí inému štátu, pričom právne nejde o vojnové činy.

[7] Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025 schválila vláda Slovenskej republiky 7. januára 2021 uznesením č. 5/2021. Ide o východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti.

[8] Uvádzané názory si vytvorili na základe štúdia, resp. priamym pozorovaním. Vzhľadom k našej pozícii (*vedecko-pedagogickí pracovníci Akadémie Policajného zboru v Bratislave*) pozitívne hodnotíme, že respondenti v procese tohto prieskumu boli konkrétni a svojimi argumentmi nás dostatočne presvedčili, že tejto problematike venujú pozornosť.

[9] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v Slovenskej republike komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň do slovenského právneho poriadku transponuje európsku smernicu o sieťovej a informačnej bezpečnosti (NIS).

[10] POŽÁR, J., BARIČIČOVÁ,Ľ, HAJDÚKOVÁ, T., MURDZA, K. a kol. 2020. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.*

[11] DRAXLER, P. 2018. Kybernetická bezpečnosť. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 15.1.2021]. Dostupné [online] z:

2. Energetická bezpečnosť

V podmienkach Slovenskej republiky e*nergetická infraštruktúra patrí medzi jedny z najrozvinutejších v EÚ. Predovšetkým kybernetické hrozby môžu zasahovať aj túto vysoko sofistikovanú a elektrizovanú energetickú infraštruktúru (napríklad elektrifikačné siete (vrátane rozvodní), plynovody, ropovody, skladiská ropy a ropných produktov, zásobníky plynu a iné).* Vo vzťahu k uvedenému, nami oslovení odborníci (*unisono*) v procesoch riadených rozhovorov uviedli, že hybridné útoky môžu mať značné následky nielen z pohľadu energetickej bezpečnosti (neočakávané výpadky dodávok rôznych druhov energie), ale taktiež pre oblasť tzv. „*hard security*" (*napríklad pri kybernetickom útoku na jadrovú elektráreň*). Niektorí analytici zaraďujú medzi hybridné hrozby aj vysokú závislosť na dodávkach energetických surovín z tretích krajín.[12]

3. Paramilitárne a extrémistické skupiny

Z výstupov z analýz bezpečnostnej situácie, ktoré sú spracované príslušníkmi Prezídia Policajného zboru (P PZ), Slovenskej informačnej služby (SIS) a Vojenského spravodajstva (VS) je zrejmé, *že polovojenské a extrémistické skupiny a hnutia spochybňujú suverenitu a legitimitu štátnej moci.* Ich subjekty pri napĺňaní tohto účelu používajú účelovo vypracované stratégie a taktiky koordinovane aj so zahraničnými aktérmi. Je predpoklad, že zahraničná podpora má rôzne formy. Nie je obmedzená len na priame financovanie, ale napríklad môže ísť o sprostredkovanie kontaktov, ideologickú, informačnú, technologickú či komunikačnú podporu.[13]

Táto realita korešponduje aj v názoroch nami oslovených respondentov. Tí uviedli, že *paramilitárne a politicko extrémistické skupiny, napojené personálne, organizačne či ideologicky na cudziu moc, odmietajú existujúce usporiadanie spoločnosti vrátane geopolitickej orientácie a členstva našej krajiny v integračných zoskupeniach (EÚ, NATO). Sú preto prirodzenými spojencami cudzích mocností snažiacich sa tieto zoskupenia oslabiť a pod.*

4. Strategická korupcia

V daných súvislostiach sú realizované formy, kedy sa štáty alebo iné vplyvné subjekty snažia systematicky využívať korupčné praktiky na získavanie politického vplyvu u nás. Tento vplyv využívajú na presadzovanie vlastných geopolitických cieľov. Je predpoklad, že v našom prostredí sú spájané predovšetkým s mocenskými ambíciami Ruska, Číny a USA.

5. Ovplyvňovanie volebných procesov

---

https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf

[12] MIŠÍK, M. 2018. Energetická bezpečnosť. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 21.1.2021]. Dostupné [online] z: https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf

[13] MILO, D. 2018. Paramilitárne a extrémistické skupiny. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 21.1.2021]. Dostupné [online] z: https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf

Slobodné, priame a férové voľby sú základným stavebným kameňom demokratického právneho štátu. Ovplyvňovanie volebných procesov je však neoddeliteľnou súčasťou hybridných hrozieb. Takéto snahy majú väčšinou podobu kombinácie informačného pôsobenia, kybernetických útokov a následného zverejnenia ukradnutých informácií, skrytého financovania politických kampaní alebo celých politických strán a vyvíjania politického či ekonomického tlaku s cieľom ovplyvniť výsledok volieb želaným smerom.

Hybridné hrozby sú formy aktivít namierené voči zraniteľnému prostrediu adresáta. V súčasnej dobe, rešpektujúc existujúcu spoločensko-politickú situáciu vo vzťahu k agresii, ktorú formou vojny realizujú predstavitelia Ruskej federácie na Ukrajine, je potvrdené, že táto zraniteľnosť je vytvorená rôznymi formami. Osobitne použitím:

- ✓ takzvanej historickej pamäte a v neposlednom rade ideológiou (*verejná mienka vo vzťahu k spoločensko-politickým zmenám, ktoré vníma spoločnosť po roku 1989 nie je jednotná*),
- ✓ legislatívy (*príkladom sú zverejňované komentáre k: Dohode o spolupráci v oblasti obrany (Defense Cooperation Agreement), ktorá je rámcová dohoda pre realizáciu spolupráce v oblasti obrany, ktorú USA ponúkajú svojim partnerom (vrátane investícií vlády USA do obranných spôsobilostí a infraštruktúry partnera*).
- ✓ starých praktík (*napríklad pozícia a rola USA, Veľkej Británie, ... vo vojne s Irakom, ...*) ,
- ✓ geostrategických faktorov (*ekonomicko-politické záujmy v priestore Strednej a Východnej Európy – USA, Ruska, Číny, ...*)
- ✓ silnej politickej polarizácie spoločnosti (*pri presadzovaní politických cieľov, nielen v podmienkach Slovenskej republiky, nie je rešpektovaná základná idea politiky, politika je umením spravovať veci verejné, umením riadiť štát a obhajovať záujmy jedného štátu voči druhému, vytvárať a udržovať vzťahy medzi týmito štátmi),* ktorej bez pátosu sú spájané s bojom koaličných politických strán s opozíciou a pod.
- ✓ technologických prostriedkov.[14]

Nami oslovení odborníci potvrdili, že citlivo vnímajú možné následky spôsobené použitím hybridných hrozieb. Sú si vedomí, že manažéri (*ale aj bezprostrední realizátori*) hybridných hrozieb sú profesionáli, ktorí pri dosahovaní vytýčených cieľov akceptujú zraniteľnosť prostredia adresáta. Preto považujú za potrebné hybridné hrozby a riziká systémovo poznávať. Identifikovať ich genézu, realizačnú štruktúru ich prvkov a interakcií (*určovaním zdrojov a veľkosťou*), a to najmä za účelom predikcie rozsahu negatívneho vplyvu na určité prostredie spoločenského systému a samozrejme prijímania adekvátnych protiopatrení (*osobitne v prípade vzniku krízovej situácie*). Dokonca uviedli, že si uvedomujú, že od nich sa očakáva, aby dokázali systematicky a dostatočne konštruktívne vytvárať predpoklady pre hodnoverné priradenie skutku konkrétnemu aktérovi: *vymedziť sledované ciele (význam) aktérov hybridných hrozieb, v najširšom slova zmysle realizovať jej atribúciu – objektu, situácií, určenie autorstva*.[15]

[14] HAJDÚKOVÁ, T. 2017. Pozitíva verzus negatíva používania moderných technológií vo vzťahu ku deťom a mládeži. In: *Právo-Bezpečnost-Informace.*

[15] Úzka koordinácia medzi verejným a súkromným sektorom, ako aj civilno-vojenská interakcia, pričom sa musí jednať o celospoločenský prístup k riešeniu tohto problému.

V praxi, na základe diskusie s kompetentnými orgánmi sme dospeli k záveru, že pri identifikácii hybridných hrozieb ich poznanie je orientované na zistenie:

- ✓ koordinácie a synchronizácie akcií, ktorými sa účelovo zameriavajú jej aktéri na zraniteľné miesta demokratických štátov a inštitúcií, a to aj pomocou už nami uvádzaných foriem,
- ✓ aktivít, ktoré sú na prahu medzi vojnou a mierom a sťažujú ich detekciu v konkrétnom vzťahu na ich aktérov,
- ✓ ciele, ktoré ovplyvňujú rozhodovanie na lokálnej, štátnej alebo inštitucionálnej úrovni,
- ✓ účel, ktorý je naplnený vytváraním podmienok pre dosiahnutie týchto cieľov, a to bez formálneho vyhlásenia vojny,
- ✓ schopnosti a možnosti používania tohto prostriedku pri dosahovaní vojenských cieľov.

3 Identifikácia hybridných hrozieb

Samotné procesy identifikácie hybridných hrozieb sú realizované kompetentnými orgánmi štátnej správy. V Slovenskej republike sú to predovšetkým príslušníci Národného bezpečnostného úradu. Národný bezpečnostný úrad je ústredným orgánom štátnej správy pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby.[16]

V súvislosti s určením pre kybernetickú bezpečnosť od 1. januára 2016 úrad zriadil útvar Národná jednotka SK-CERT (Slovak Computer Emergency Response Team) a od 1. septembra 2019 ho transformoval na Národné centrum kybernetickej bezpečnosti SK-CERT. Útvar zabezpečuje národné a strategické aktivity v oblasti riadenia kybernetickej bezpečnosti, v oblasti analýzy hrozieb, ale aj koordinácie riešenia kybernetických bezpečnostných incidentov na celonárodnej úrovni, výuky, vzdelávania, tréningov, ako aj výskumu.[17]

Národný bezpečnostný úrad od 1. júla 2020 prevádzkuje *Pracovisko pre hybridné hrozby a dezinformácie*. Jeho zriadenie nadväzuje na celoštátne aj celoeurópske úsilie bojovať proti hybridným hrozbám a dezinformáciám. Vláda Slovenskej republiky sa vo svojom programovom vyhlásení zaviazala pripraviť akčný plán na koordináciu boja proti hybridným hrozbám a šíreniu dezinformácií, či vybudovať adekvátne centrálne kapacity pre jeho realizáciu.

Úlohou pracoviska pre hybridné hrozby a dezinformácie je systematicky sledovať, vyhodnocovať, analyzovať a reagovať na aktivity, ktoré majú potenciál polarizovať spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov Slovenskej republiky.

Pracovisko pre hybridné hrozby a dezinformácie úzko spolupracuje s Národným centrom kybernetickej bezpečnosti SK-CERT, ale aj ďalšími útvarmi úradu. Svoje výstupy poskytuje Situačnému centru Slovenskej republiky, ktoré pôsobí pri Úrade vlády Slovenskej republiky, a Národnému bezpečnostnému analytickému centru, ktoré je analytickým, komunikačným a kooperačným pracoviskom Slovenskej informačnej služby založeným na aktívnej participácii slovenských bezpečnostných orgánov.[18]

---

[16] Zákonom č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, bol zriadený Národný bezpečnostný úrad ako ústredný orgán štátnej správy. Národný bezpečnostný úrad plní úlohy vyplývajúce mu z uvedeného zákona, z uznesení vlády a z prevzatých záväzkov voči NATO a EÚ.

[17] *O nás* ~ SK-CERT. 2018. Dostupné [online] z: https://www.sk-cert.sk/sk/o-nas/index.html.

[18] *Hybridné hrozby*. 2021. Dostupné [online] z: http:// www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html.

Pracovisko pre hybridné hrozby a dezinformácie je v rámci organizačnej štruktúry úradu začlenené pod námestníka riaditeľa úradu.

Túto realitu sme pri spracovaní tejto vedeckej štúdie akceptovali. Pri spracovaní jej následnej časti využívame logickými operáciami spracované poznanie, ktoré nám prezentovali v procese riadeného rozhovoru oslovení respondenti (*piati príslušníci NBÚ, január- február rok 2022*). Tí uviedli, že sa v praxi od nich očakáva, že dokážu identifikovať *kto – pre koho, s kým; čo – ciele; ako – postup; čím – prostriedky a metódy; kde – prostredie – situácie, udalosti; kedy – obdobie, doba, časový rozmer; prečo* používa (*použil*) hybridnú hrozbu. Pri tejto činnosti je vhodné, ak akceptujú, že hybridná hrozba:

- ✓ je realizovaná intencionálne, nielen cieľavedome, ale aj účelovo,
- ✓ je realizovaná v určitom prostredí, viazaná na udalosť, čas a priestor, podmienky, okolností,
- ✓ sa vyvíja v čase, má príčinu svojej existencie (*vznik i zánik*), nevzniká náhodne a bezdôvodne,
- ✓ dôvod pre vznik rizík je zakódovaný v samotnom prejave a v podstate hybridnej hrozby, na ktorú sa viaže,
- ✓ každej forme hybridnej hrozby sú priradené isté druhy rizík.[19]

V procesoch realizácie spravodajskej činnosti je cieľom analýzy rizík identifikovať hybridné hrozby a stanoviť ich pôsobenie na bezproblémový život v spoločnosti (*ohodnotenie aktív*), nájsť možné zdroje ohrozenia (*hrozby*), zhodnotiť aktuálny spôsob ochrany i existujúce slabiny takýchto ochranných opatrení (*zraniteľnosti*) a určiť výslednú veľkosť rizík, ohrozujúcich dané aktíva. V daných súvislostiach je možné konštatovať:

- ✓ hybridnú hrozbu môžu aktéri realizovať v rôznych prostrediach (*S. Popov „ ... súhrn všetkých podmienok, ktoré obklopujú človeka a priamo alebo nepriamo ho ovplyvňujú. ...“)* [20] , v ekonomike, riadení, politike, vo veciach verejných a súkromných, ...
- ✓ identita rizika vo vzťahu ku konkrétne realizovanej hybridnej hrozbe (*aktér, aktivity, adresát*) vykazuje konkrétne špecifiká,
- ✓ rizikové dôsledky hybridnej hrozby môžu mať permanentný charakter, vyskytujú sa trvalo a neustále, môžu vzniknúť náhle, nečakane, spôsobiť nežiaduce následky, môžu vzniknúť iba v konkrétnom čase, prostredí - sú viazané na istú udalosť a situáciu,
- ✓ realizáciu hybridných hrozieb identitou rizík je možno spravidla predvídať podľa istých indícií,
- ✓ realizácia hybridných hrozieb môže mať vnútroštátny, resp. medzinárodný charakter, je ich možné kontrolovať,
- ✓ každá hybridná hrozba je spravidla porovnateľná s inými druhmi, alebo aj s podobnými účelovo realizovanými aktivita v minulosti,
- ✓ pôsobenie hybridných hrozieb je závislé od postoja adresátov k hodnoteniu rizík,
- ✓ realizácia hybridných hrozieb je intencionálna činnosť (nie je to náhoda a bez príčiny), je istou mierou ovplyvnená konaním človeka a pod.

[19] BUZALKA, J. 2012. *Teória bezpečnostných rizík,* s. 15.

[20] *Čo je to definícia sociálneho prostredia*. *Sociálne prostredie.*2020. Dostupné [online] z: https://ik-ptz.ru/sk/matematika/chto-takoe-socialnaya-sreda-opredelenie-sreda-socialnaya-s-samogo-rannego.html.

Z uvedeného je zrejmé, že pri identifikovaní podstaty hybridných hrozieb je vhodné, ak akceptujú:

- ✓ aký názor na riziká, ktoré sú zakódované do týchto aktivít (*vznik, existenciu*) má občan, spoločnosť,
- ✓ ako tieto aktivity posudzujú (*odhaľujú, skúmajú, hodnotia*) odborníci a experti z realizačného prostredia (*osobitne policajno-bezpečnostné orgány*); akú majú kompetenciu (*zodpovednosť*) za predvídanie (*resp. kontrolu*) tieto subjekty,
- ✓ aké negatíva a dôsledky budú spôsobené realizáciou hybridných hrozieb bezprostredne, resp. v budúcnosti (*výsledky a efekty*),
- ✓ či je možné realizáciu hybridných hrozieb použiť pri realizácii protiopatrení, ak áno, tak aké, kedy, kde (*osobitne pre realizáciu policajno-bezpečnostných činnosti*).[21]

Tak, ako je tomu aj vo vedeckom poznávaní (*napríklad sociologický výskum*), realizáciu identifikácie tohto objektu je možné charakterizovať z hľadiska procesuálneho (*štruktúrovaným obsahom realizácie*) a informačného (*ontológia, gnozeológia*). Prax potvrdzuje, že kompetentné orgány štátnej správy (*príslušníci NBÚ*) sú povinné túto činnosť realizovať systémovo, konštruktívne, plánovite, rešpektujúc existujúcu realitu (*osobitne skúsenosti*). Identifikácia hybridných hrozieb je forma (*funkčné použitie prostriedkov v metódach*) za účelom poznania.

Postup pri realizácii foriem identifikácie pozostáva väčšinou z týchto základných krokov:

1. vymedzenie identifikačného problému,
2. štúdium reality (proces realizácie hybridných hrozieb, jeho determinanty a konštrukty),
3. formulácia domnienok s vymedzením,
4. voľba metodiky identifikácie,
5. poznávací cyklus.

Medzi základné výskumné otázky patria:

a) faktické otázky (*aký sociálny jav sa vyskytol*),
b) komparatívne otázky (*kde sa jav vyskytol*),
c) vývojové otázky (*kedy sa jav vyskytol*),
d) teoretické otázky (*prečo sa jav vyskytol*).[22]

To potvrdzuje, že proces identifikácie hybridných hrozieb (*obligatórne*) sa začína voľbou problému a formuláciou pojmového rámca, následne na to výberom skúmaného súboru a výberom metódy zberu dát a ich analýzou vo vzťahu k cieľu a účelu tohto špecifického poznania (*interpretácia a prezentácia výsledkov a záverov identifikácie*).

Z metodického hľadiska je dôležité pre úspešnú realizáciu identifikácie stanoviť konkrétne identifikačné úlohy, ktoré korešpondujú s uvedenými znakmi. V tomto smere je vhodné analýzou hybridných hrozieb, to znamená pri ich identifikácii, poznať odpovede najmä na tieto otázky:

---

[21] BUZALKA, J. 2012. *Teória bezpečnostných rizík*, s. 25.
[22] HAJDÚKOVÁ, T., LAVRINČÍK, M. 2018. *Aplikácia vedeckých metód na prípady z policajnej praxe*. 1. vyd.

- ✓ Prečo je potrebné realizovať identifikáciu (*impulzy*)?
- ✓ Kto je aktérom týchto hybridných hrozieb?
- ✓ Prečo sa rozhodol hybridné hrozby používať (*účel, cieľ)*?
- ✓ Akú formu hybridnej hrozby používal? (eventuálne pretože môže využívať paralelne niekoľko hybridných hrozieb)
- ✓ Kto je adresátom týchto hybridných hrozieb?
- ✓ Prečo túto hybridnú hrozbu používa v tomto čase a prostredí (*situácia, udalosť /udalosti/*)?
- ✓ Pred použitím hybridnej hrozby realizoval aktér určité prípravné aktivity?
- ✓ Kto je kompetentný ? (*akceptácie právnej regulácie a zodpovednosti*)
- ✓ Ako je možné pôsobiť pri eliminácii účinkov hybridnej hrozby?
- ✓ Ako je možné využiť identifikáciu hybridných hrozieb proti ich aktérom?

Ďalším krokom v procese identifikácie je konkrétna činnosť, ktorá súvisí so samotnou organizáciou a riadením identifikácie. V daných súvislostiach je dôležité zriadiť konkrétny subjekt, ktorý bude v súlade a rozsahu zákona hľadať odpovede na tieto otázky – realizovať samotný proces identifikácie. V tejto súvislosti je vhodné zdôrazniť, že proces identifikácie je ukončený spracovaním informačného výstupu, ktorý využije kompetentný orgán pri eliminovaní pôsobenia hybridných hrozieb. Vo väčšine prípadov týmito subjektmi sú štátne a politické orgány, ktoré sú oprávnené prijať a vydať konkrétne rozhodnutia, alebo prijať opatrenia smerujúce k samotnej eliminácii týchto hrozieb.

Informačné výstupy z procesov identifikácie hybridných hrozieb sú texty – bilaterálne kategórie (*výsledok, efekt*), ktoré majú obsahovú a formálnu stránku. Rešpektujúc účel tejto špecifickej činnosti, informačné výstupy (texty) majú potenciálny (očakávaný), resp. aktuálny poznávací charakter.

Realizátori identifikácie (v praxi) ukončujú formulovaním záverov, ktorých štruktúru tvoria odpovede na otázky:

- ✓ Aké boli dôvody realizácie procesov identifikácie?
- ✓ Ako bola odhalená a objasnená hybridná hrozba?
- ✓ Kto, kedy a využitím akých kompetencií realizoval procesy?
- ✓ Pre koho je spracovaný informačný produkt?
- ✓ Podľa akých vlastností je charakterizovaná hybridná hrozba? Aká je? Kto je tvorcom hybridnej hrozby?
- ✓ V akom štádiu realizácie je hybridná hrozba?
- ✓ Ktoré subjekty sú zainteresované na realizácii hybridný hrozieb?
- ✓ Čo je objektom záujmu hybridný hrozieb?
- ✓ S akým cieľom boli realizované hybridné hrozby? (analogicky cieľ, motív)
- ✓ Kde, kedy, ako často sú hybridné hrozby realizované?
- ✓ Akým spôsobom sú hybridné hrozby realizované?
- ✓ Ako je potrebné postupovať pri vykonávaní dôkazov? a pod.

To potvrdzuje, že spracovaný informačný výstup musí vyhovovať určitým formálnym a vecným požiadavkám. V prvom rade sú príslušníci NBÚ pri jeho spracovaní povinní rešpektovať právnu reguláciu účelovej identifikácie. Jej imanentnou súčasťou je manipulácia s informáciami a prístup k nim. V neposlednom rade sú povinní tento produkt spracovať presne, v predpísanej podobe (forme), a tak jednoznačne, aby mohol byť chápaný (interpretovaný) v tom istom zmysle, ako je prezentovaný, a nie inak.

Z vecnej stránky spracovaný informačný produkt z procesov identifikácie hybridných hrozieb musí vykazovať objektívne a adresne spracovaný dokument. Príslušníci NBÚ v tomto dokumente objektivitu spracovaného poznania potvrdzujú:

- ✓ opisom situácie (*východiská hybridných hrozieb*),
- ✓ prezentáciou realizovaného postupu (*pri získavaní, zbere a spracovaní informácií*),
- ✓ adresnou zodpovednosťou za spracované poznanie (*v žiadnom prípade nie z vlastných alebo iných subjektívnych predstáv, predpokladov, želaní, intuície*),
- ✓ hodnovernosťou a spoľahlivosťou (*reliabilitou*) informačných sietí,
- ✓ teoretickou a praktickou verifikáciou predkladaného poznania,
- ✓ logikou myslenia – logickými operáciami (jasnou, zrozumiteľnou, presvedčivou, bez vedomého alebo neuvedomeného zamlčovania dôležitých momentov),
- ✓ dôkaznou situáciou (*zoznamom stôp – materiálne, pamäťové, analytickými a transferovými informáciami*) a pod.

Z uvedeného (*aj napriek tomu, že to nie je nami explicitne vyjadrené*) vyplýva, že informačný výstup (*produkt*) z procesov identifikácie hybridných hrozieb je analytický dokument.[23] Realizátori - príslušníci NBÚ pri jeho vypracovaní cieľavedome, účelovo, systematicky a komplexne aplikujú induktívno-deduktívny postup, v ktorom využívajú kvalitatívne a kvantitatívne analýzy, komparáciu, analógiu, syntézu a iné logické operácie. Z týchto dôvodov (*rešpektujúc uvedené*) je vhodné, ak informačný výstup z týchto procesov spracujú vo forme dokumentu **–** *SPRÁVY*, ktorá má mať vo svojom obsahu tieto časti:

- ✓ úvod, v ktorom charakterizujú akceptovanú koncepciu, vymedzujú spoločenskú a spravodajskú potrebu identifikácie (*vecná časť*). Vo formálnej časti uvádzajú mená a funkcie (*pozícia, rola*) realizátorov týchto procesov (*kompetencie, zodpovednosť*);
- ✓ ciele, ktoré boli vytýčené v štádiu prípravy procesov identifikácie (*ich zdôvodnenie*);
- ✓ formulované domnienky vo vzťahu k charakteristike vlastností poznávaného javu (*zdôvodnenie ich využívania – východiskové poznatky o skúmanom objekte a pod*.) s uvedením predpokladov ich objektívnej verifikácie;
- ✓ charakteristika predmetu, ktorý bol akceptovaný pri saturácii absencie poznania (*procesy, systém realizačného prostredia – situácia – determinanty – konštrukty*);
- ✓ opis metodiky, realizovaných opatrení a úkonov, prostriedkov v metódach, operácií, techník (*čas, miesto, adresná kompetenčná zodpovednosť ich realizácie, resp. využívania a aplikácie*). Hodnotenie ich realizačného prínosu pri získavaní zdôvodneného tohto účelového poznania. Zdôvodnenie záujmu o identifikovaný objekt, resp. subjekt (*oprávnenosť zásahu*);
- ✓ prezentácia a opis získaného poznania a vecných, listinných a iných dokumentov (*príloh*). Analýzy poznania a vyvodenie objektívnych záverov (*generalizácia ich objektivity – ich platnosť*);
- ✓ záverečné zhrnutie poznania, verifikácia domnienok, úspech – poukázanie na jeho možnú aplikáciu v praxi (*prípadne nedostatky*). Poukázanie, čo je potrebné následne poznávať atď.;
- ✓ odkazy, vysvetlenie použitých skratiek, použitie registračných indexov, prílohy, počet výtlačkov, možnosti a prístup k spracovanému poznaniu;
- ✓ obsah.

Z praxe je zrejmé, že spracovanie informačného výstupu (*produktu*) z procesov identifikácie hybridných hrozieb je tvorivá ľudská aktivita, pri ktorej sa prejavujú schopnosti

[23] KULÍŠEK, M. 1997. *Analytická činnosť v rezorte MV SR*. 2. doplnené a prepracované vyd., s. 51.

jeho spracovateľa. Vo všeobecnosti platí, že informačný výstup je možné spracovať až vtedy, ak je k dispozícii požadovaná úroveň kvalitatívneho a kvantitatívneho poznania (*hovoriť iba vtedy, keď je čo povedať*). Zjednodušene povedané, v súlade s očakávaním realizátorov pri tvorbe a prezentácii informačného výstupu, sú povinní akceptovať konkrétne tematické ohraničenie dosiahnutého poznania (*konštruktívnosť*). Je to tak preto, lebo informačný výstup nadobúda zmysel až vtedy, keď ho prijme adresát. To potvrdzuje, že pri jeho tvorbe spracovateľ musí poznať subjekt, ktorý je oprávnený výstup využiť.

Spracovanie a interpretácia (*prezentácia*) informačného produktu z procesov identifikácie hybridných hrozieb predstavuje (*v určitom zmysle slova*) dosiahnutie vytýčenej méty – cieľa. Ako je to aj v iných činnostiach, po dosiahnutí cieľa dochádza k vzniku určitej situácie, na ktorú je potrebné adekvátne reagovať. Prax potvrdzuje, že je vhodné, ak príslušníci NBÚ pri identifikácii hybridných hrozieb túto skutočnosť (*vznik novej situácie*) akceptujú, a to vo všetkých štádiách realizácie týchto poznávacích procesov. Zjednodušene povedané, je pre realizátorov výhodné, ak sú pripravení na riešenie týchto situácií. Samotnou prípravou na ich zvládnutie vytvárajú potrebné predpoklady na úspešné zavŕšenie svojich aktivít v týchto procesoch (*dosiahnutie požadovanej účinnosti a efektov*).

Analógiou týchto konštatácií je možné dospieť k záveru, že po dosiahnutí cieľa z procesov identifikácie hybridných hrozieb vznikajú rôzne situácie. Ich javový charakter a podstatu dominantne ovplyvňujú konkrétne realizované identifikačné aktivity a využitie informačných výstupov z týchto procesov.

Aj napriek tomu, že to vyznieva ako určitý paradox, v praxi je najpozitívnejšie, ak realizátori v obsahu informačného výstupu z realizovaných procesov identifikácie konštatujú, že k hybridnej hrozbe nedošlo. V týchto intenciách je pri riešení tejto vzniknutej situácie povinnosťou realizujúceho subjektu:

- ✓ obhájiť adekvátnosť realizovaných opatrení pred svojím nadriadeným,
- ✓ v prípade, ak bol impulzom týchto procesov podnet (*oznámenie*), tento zdroj oboznámiť so zistenými faktami, ktoré vylučujú opodstatnenosť jeho oznámenia,
- ✓ oboznámiť subjekty o opatreniach, ktorými boli porušené ich práva a sloboda s požadovaným adekvátnym zdôvodnením (*dôvody, potreba, dosiahnuté výstupy a pod*.) a poučením o možnosti uplatnenia – právnej a inej kompenzácie,
- ✓ vhodným spôsobom informovať občana o tom, že skutok sa nestal, ktoré fakty túto skutočnosť objektivizujú (*samozrejme predovšetkým, ak do realizácie identifikácie boli občania zapojení, resp. o týchto procesoch boli upovedomení*) a pod.

Iná situácia je, ak v procese identifikácie nie je jednoznačne preukázané, že skutok sa nestal (*podozrenie z hybridnej hrozby stále existuje*). Pri riešení týchto situácií realizátor:

- ✓ vykoná analýzu – postupu a realizovaných opatrení v celom procese, ich determinantov a využitej logistiky, výsledky tejto analýzy predloží svojmu nadriadenému,
- ✓ vymedzí dôvody ďalšieho postupu,
- ✓ zdôvodní možné riziká spájané s pokračujúcim poznávaním a vymedzí možnosti ich eliminácie,
- ✓ spracuje návrh ďalšieho postupu s vymedzením konkrétnej zodpovednosti za plnenie odôvodnene zadaných úloh, tento návrh predloží nadriadenému na jeho schválenie,
- ✓ v súlade s identifikovanou potrebou vyžiada adekvátnu koordináciu,
- ✓ zdôvodní potrebu využitia potrebných prostriedkov (*spravodajskej činnosti*), pritom akceptuje princíp subsidiarity pri ich nasadení,

- ✓ v prípade potreby zváži zapojenie verejnosti do plnenia úloh a pod.

Záver

Na záver tejto prezentácie (*znova zdôrazňujeme, že sme spracovali názory respondentov*) považujeme za vhodné dodať, že základný predpoklad úspechu pri realizácii identifikácie hybridných hrozieb určuje úroveň koordinácie. Jej význam možno teoreticky zdôvodniť využitím analytickej a funkcionalistickej (*konštruktivistickej*) charakteristiky jeho realizačného systému. Následne je možné takto spracované teoretické poznanie využiť v praxi pri skúmaní koordinačných vzťahov, hodnotení ich prínosov (*pridanej hodnoty*) v štruktúrovanom procese identifikácie hybridných hrozieb a projektovaní opatrení k eliminácii z nich vyplývajúcich rizík.

Z empírie vyplýva, že základným znakom systému tohto špecifického poznania je neustála transformácia a cirkulácia informácií v dynamike vývoja realizácie hybridných hrozieb. Transformácia informácií v tomto systéme má prebiehať tým spôsobom, že výstup z jedného poznania je zároveň vstupom do ďalšieho. Vznik, kvantitatívna a kvalitatívna zmena informačného charakteru rizík z hybridných hrozieb (*vznik, rast, čiastočná paralyzácia, úplné znefunkčnenie*) tvoria pevný reťazec v prostredí a čase. Tieto skutočnosti sú povinní akceptovať všetci, ktorí zastávajú pozíciu a rolu orgánov štátnej správy. Osobitne policajno-bezpečnostné orgány, ktoré uplatnením svojich kompetencií participujú pri identifikovaní hybridných hrozieb a eliminovaní vzniku rizík. Tak, ako sme uviedli pri plnení týchto úloh, koordinátorom sú príslušníci NBÚ. Efektivita a účinnosť ich činností je závislá od kvantity a kvality informácií. Preto v systéme identifikácie rizík z hybridných hrozieb je potrebné pokladať problém koordinácie (*na rôznej hierarchickej úrovni*) za veľmi dôležitý. Pri jej skúmaní je vhodné sa prednostne orientovať na také stavy, prípady a situácie, v ktorých koordinačné vzťahy vznikajú, existujú a zanikajú (*vo svojom správaní sa menia*). Je tomu tak preto, lebo v tomto špecifickom poznaní tieto zmeny nemôžu mať chaotický charakter. Musia sa uskutočňovať kontinuálne a konštruktívne. Predpokladom toho je poznať (*odhaliť, objaviť*) určité spoločné pravidlá, ktoré podmieňujú istú príbuznosť (*afinitu*) a podobnosť realizovaných aktivít pri dosahovaní cieľa, a to aj na prvý pohľad úplne rozdielnych systémov. Ak vieme určiť tieto pravidlá usporiadania, môžeme prejsť k určeniu nevyhnutnosti koordinácie, a tak určiť *„zmeny“* realizačného systému hybridných hrozieb ako celku. Bez ohľadu na úplnosť, to vyžaduje poznať:

- ✓ stabilitu systému (*dispozícia kompetencií)*, jeho zotrvačnosť, akceptovanie výskytu náhody a nevyhnutnosti, možného pôsobenia okolia,
- ✓ konkrétny charakter delegovaných úloh,
- ✓ realizačné bezpečnostné situácie a pod.

Zastávame názor, že týmto poznaním je možné dostatočne zdôvodniť aplikačnú potrebu praktickej koordinácie v účelovo realizovaných činnostiach kompetentných policajno-bezpečnostných orgánov. Napríklad v danej súvislosti je potrebné poznať charakteristické *„statické“* parametre systému realizácie identifikácie hybridných hrozieb, ktoré je možné využiť pri plnení spoločnej úlohy. Najmä z hľadiska funkcionality výkonnosti, účinnosti a efektivity jednotlivých policajno-bezpečnostných orgánov (*právnu reguláciu ich činnosti a povinnú akceptáciu zodpovednosti*).

Z charakteristík realizácie identifikácie hybridných hrozieb vyplýva aj ich personálna, ekonomická, technická a iná náročnosť. Koordinujúce policajno-bezpečnostné orgány v tomto účelovom poznaní plnia zložité (*náročné*) úlohy, pri ktorých je nevyhnutné intenzívne

zasahovať do práv a slobôd občanov, čo vyžaduje osobitné postupy, kontrolu a pod. Podobne je možné hodnotiť aj výsledky a efekty identifikácie v ich kontinuálnej nadväznosti na realizáciu následného konania (*spoločenského, policajného, súdneho)*. Táto skutočnosť musí byť pri jeho realizácii identifikácii hybridných hrozieb akceptovaná a hodnotená najmä z hľadiska kvality, aktuálnosti, akcieschopnosti. V danej súvislosti niet argumentov, ktorými by bolo možné znížiť význam koordinácie pri realizácii tejto špecifickej poznávacej činnosti. Ako potvrdzuje aj táto prezentácia, nami oslovení respondenti profesionálne vnímajú spoločenskú závažnosť hybridných hrozieb. To považujeme za základný logistický prvok pre budovanie koordinačných vzťahov pre potreby identifikácie hybridných hrozieb.

Literatúra

BAKOŠOVÁ, Z. 1994. *Sociálna pedagogika* (Vybrané kapitoly). Bratislava: Filozofická fakulta Univerzity Komenského v Bratislave, 1994. ISBN 80-223-0817-X. s. 11,

BUZALKA, J. 2012. *Teória bezpečnostných rizík*. Bratislava: Akadémia Policajného zboru v Bratislave, 2012. 167 s., ISBN 978-80-8054-547-5.

Čo je to definícia sociálneho prostredia. Sociálne prostredie. 2020. Dostupné [online] z: https://ik-ptz.ru/sk/matematika/chto-takoe-socialnaya-sreda-opredelenie-sreda-socialnaya-s-samogo-rannego.html.

DRAXLER, P. 2018. Kybernetická bezpečnosť. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 15.1.2021]. Dostupné [online] z: https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf.

HAJDÚKOVÁ, T. 2017. Pozitíva verzus negatíva používania moderných technológií vo vzťahu ku deťom a mládeži. In: *Právo-Bezpečnost-Informace.* ISSN 2336-3657 . Zvláštní vydání mez. konf. Jihlava - speciál (2017), 11 s.

HAJDÚKOVÁ, T., LAVRINČÍK, M. 2018. *Aplikácia vedeckých metód na prípady z policajnej praxe*. 1. vyd. Bratislava: Akadémia Policajného zboru, 2018. 152 s. ISBN 978-80-8054766-0.

Hybridné hrozby. 2021. Dostupné [online] z: http:// www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/hybridne-hrozby/index.html.

KULÍŠEK, M. 1997. *Analytická činnosť v rezorte MV SR*. 2. doplnené a prepracované vyd. Bratislava, 1997, s. 51.

MILO, D. 2018. Paramilitárne a extrémistické skupiny. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 21.1.2021]. Dostupné [online] z: https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf.

MIŠÍK, M. 2018. Energetická bezpečnosť. In: *Mapovanie zraniteľnosti Slovenskej republiky v oblasti hybridných hrozieb* [cit. 21.1.2021]. Dostupné [online] z: https://www.globsec.org/wp-content/uploads/2018/08/Zranitelnost-SR-v-oblasti-hybridnych-hrozieb-web.pdf

O nás ~ SK-CERT. 2018. Dostupné [online] z: https://www.sk-cert.sk/sk/o-nas/index.html.

PAVLOVIČ, G. 1975. *Akcelerácia vývinu a socialistická škola.* Bratislava: Veda, 1975. 475 s.

POŽÁR, J., BARIČIČOVÁ,Ľ, HAJDÚKOVÁ, T., MURDZA, K. a kol. 2020. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných*

souvislostech. Praha: Policejní akademie České republiky, 2020. 328 s. ISBN 978-80-7251-505-9.

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Keywords: identification, threat, risk, hybrid threat, parties of hybrid threats, cyber security, energy security, paramilitary and extremist groups, strategic corruption, influencing the electoral processes, National Security Authority.

Summary

The characteristics of the hybrid threat identification also include its personnel, economic and technological demands. On this basis, the coordination of police and security authorities in performing their complex tasks, strongly interfering with citizens' rights and freedoms, requires specific procedures and control. The results and effects of identification can be evaluated as part of the ongoing monitoring of the follow-up procedures implementation.

This fact must be accepted and assessed in the identification of the hybrid threat, especially in terms of quality, timeliness, and operational capability. There is also no argument about the importance of coordination in carrying out this particular cognitive activity. As this presentation confirms, the professional respondents we addressed perceive the social consequences of hybrid threats. We believe that this is a fundamental logistical element in creating a coordinated approach to identifying hybrid threats.

prof. Ing. Miroslav Lisoň, PhD.
Katedra kriminálnej polície
Akadémie Policajného zboru v Bratislave
e-mail: miroslav.lison@akademiapz.sk

Mgr. Ľudovít Fidler
Katedra kriminálnej polície
Akadémie Policajného zboru v Bratislave
e-mail: ludovit.fidler@akademiapz.sk

Recenzenti: doc. JUDr. Antonín Nesvadba, PhD., doc. JUDr. Boris Lőffler, PhD.