Radoslav Ivančík

Aktuálne východiská skúmania problematiky hybridných hrozieb

Anotácia: V prvých dvoch dekádach tretieho milénia došlo k zásadným zmenám v globálnom i regionálnom bezpečnostnom prostredí a k transformácii tradičných bezpečnostných hrozieb. Tie sa stali v posledných rokoch viacrozmernými, viacvrstvovými a v zložitých podmienkach existencie ľudskej spoločnosti nadobudli hybridný charakter. Využívajú zraniteľnosti krajín a snažia sa oslabiť základné demokratické hodnoty a slobody. Hybridné hrozby totiž súvisia s využívaním širokej škály rôznych prostriedkov, akými sú dezinformácie, hoaxy, propaganda, kybernetické útoky, organizovaný zločin, ekonomický, politický a spoločenský nátlak, terorizmus a ďalšie nástroje, pričom všetky vedú k podkopávaniu demokratických základov a destabilizácii politických, ekonomických a sociálnych prvkov spoločnosti. Aj preto sa autor vo svojom príspevku, s využitím relevantných metód kvalitatívneho teoretického vedeckého výskumu, zaoberá problematikou hybridných hrozieb, no – vzhľadom na aktuálny vývoj bezpečnostného prostredia a bezpečnostnej situácie – aj potrebou prijímania efektívnych, účelných a účinných opatrení zacielených na ich elimináciu.

Kľúčové slová: bezpečnosť, hybridné hrozby, bezpečnostné prostredie, spoločnosť.

Úvod

Globálne i regionálne bezpečnostné prostredie sa v posledných rokoch výrazne zmenilo. Je komplikovanejšie, premenlivejšie, nestabilnejšie a zároveň vo vysokej miere ovplyvnené nedostatočným riešením pretrvávajúcich globálnych problémov ľudstva a nerovnomernosťou vývoja jednotlivých regiónov. Došlo v ňom k viacerým zásadným zmenám. Ich výsledkom je transformácia už známych konvenčných hrozieb, ktoré získali v dôsledku vývoja nových technológií úplne novú dimenziu a zvýšila sa aj ich intenzita a dopad na spoločnosť. Zároveň sa objavili nové hrozby a výzvy úzko súvisiace so zintenzívnením procesov geopolitickej konfrontácie, rozširovaním oblastí nestability a výskytom nových kríz a konfliktov v regiónoch v bližšom aj vzdialenejšom okolí teritória Európskej únie (ďalej len „EÚ“ alebo „Únia“).

Bezpečnostná situácia EÚ a jej členských štátov – Slovenskú republiku nevynímajúc – sa tým pádom v posledných rokoch a zvlášť po minuloročnom napadnutí Ukrajiny vojskami Ruskej federácie dramaticky zmenila. Rastúce problémy so zabezpečením mieru a stability vo východnom a južnom susedstve Únie jasne naznačujú, že EÚ ako celok na nadnárodnej úrovni a členské štáty individuálne na národnej úrovni musia adekvátne reagovať, musia prispôsobiť a znásobiť svoje vojenské i civilné spôsobilosti a kapacity, aby mohli zaistiť bezpečnosť a ochranu svojich občanov. Zamerať sa pritom musia aj na stále väčšiu prepojenosť medzi vonkajšou a vnútornou bezpečnosťou. Množstvo problémov v oblasti zaisťovania vnútornej bezpečnosti totiž – okrem premenlivého charakteru hrozieb – v súčasnosti spôsobuje najmä vyššie zmienená nestabilita a konflikty a krízy v krajinách a regiónoch, ktoré bezprostredne susedia s EÚ.

Bezpečnostné hrozby sa stali viacrozmernými, viacvrstvovými a v zložitých podmienkach existencie súčasnej ľudskej spoločnosti nadobudli hybridný charakter. Súvisia s využívaním rôznych prostriedkov, akými sú dezinformácie, propaganda, kybernetické útoky, organizovaný zločin, politický, ekonomický a spoločenský nátlak, terorizmus atď. Všetky vedú k podkopávaniu demokratických základov, hodnôt a slobôd a k destabilizácii politických, ekonomických a sociálnych prvkov našej spoločnosti. Aj preto aktuálne bezpečnostné prostredie charakterizuje vysoká miera dynamiky vývoja a nízka miera predvídateľnosti, ktoré vyplývajú z rastúceho počtu aktérov a faktorov ovplyvňujúcich bezpečnosť a z miery ich vzájomnej previazanosti. Mnohé tieto prvky sú v bezpečnostnom

prostredí nové a súčasné bezpečnostné systémy zatiaľ nemajú dostatočné schopnosti efektívne im čeliť.

Pozorované negatívne javy a procesy prebiehajúce v bezpečnostnom prostredí a nové trendy v oblasti hybridných foriem a metód destabilizácie bezpečnostnej situácie vyvolávajú potrebu serióznej analýzy orientovanej smerom k prijímaniu nevyhnutných opatrení a k budovaniu potrebných spôsobilostí a kapacít na boj proti hybridným hrozbám. Aj preto sa autor v predloženej vedeckej štúdii, s využitím relevantných metód kvalitatívneho teoretického vedeckého výskumu, zaoberá problematikou hybridných hrozieb, predovšetkým teoreticko-metodologickými východiskami ich skúmania, no – vzhľadom na aktuálny vývoj bezpečnostného prostredia a bezpečnostnej situácie – aj potrebou prijímania efektívnych, účinných a účelných opatrení zacielených na ich elimináciu so zameraním na Slovenskú republiku (ďalej len „SR“).

Aktuálne východiská skúmania problematiky hybridných hrozieb v kontexte vývoja bezpečnostného prostredia

Konvenčný vojenský konflikt – ako to potvrdzuje aj viac ako rok prebiehajúci konflikt na Ukrajine – má v súčasnosti podstatne vyššie politické, finančné, ľudské, materiálne a morálne náklady, a preto sa čoraz viac štátnych a neštátnych aktérov pri realizácii ich aktivít spolieha na využívanie nevojenských prostriedkov tak, aby nemuseli formálne vyhlásiť vojnu. Paralelným použitím hybridných foriem v podobe rôznych nátlakových a podvratných činností, konvenčných a nekonvenčných metód (napr. nepriateľská propaganda, šírenie dezinformácií, hoaxov, podpora extrémizmu, radikalizmu, využívanie národnostných alebo náboženských komunít nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru atď.) môžu destabilizovať spoločnosť v cieľových štátoch – spravidla v demokratických štátoch – a oslabiť ich tak, aby boli ľahšie ovplyvniteľné alebo v krajnom prípade aj menej odolné voči použitiu konvenčnej vojenskej sily.[1]

Objektmi takýchto hybridných aktivít však nemusia byť iba individuálne štáty (napr. Slovenská republika a ďalšie členské štáty EÚ). Hybridné hrozby presahujú ich hranice a môžu byť súbežne vedené proti viacerým štátom, prípadne medzinárodným zoskupeniam (napr. proti celej EÚ). V medzinárodnom meradle môžu byť zamerané hlavne na narušanie súdržnosti medzinárodných zoskupení, ktorých členom je Slovenská republika, najmä už spomenutej EÚ, ale aj Severoatlantickej aliancie (ďalej len „NATO“ alebo „Aliancia“), a taktiež na oslabovanie vzájomnej solidarity medzi ich členskými štátmi. Boj proti hybridným hrozbám si preto vyžaduje intenzívnu medzinárodnú spoluprácu a koordináciu na nadnárodnej úrovni.[2]

V nadnárodnom (európskom) i národnom (slovenskom) kontexte má stále častejšie využívanie hybridných aktivít zo strany štátnych i neštátnych aktérov voči Únii i jej členským štátom – bez ohľadu na formu hybridných hrozieb – výrazný vplyv na inštitucionálny rozvoj politických a operačných prvkov a spoluprácu s partnermi, najmä s NATO a ďalšími partnerskými organizáciami a krajinami v boji proti hybridným hrozbám. Z politického hľadiska je dôležitá signalizácia, ako EÚ a jej členské štáty vnímajú a hodnotia hybridné hrozby a ich mnohostranný potenciál. Z operačného hľadiska podčiarkuje zámer a schopnosť chrániť a rýchlo reagovať na nový rozmer a rozsah asymetrických bezpečnostných hrozieb. Aj

[1] NBÚ. 2018. Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám. In *Národný bezpečnostný úrad*, s. 2.
[2] Tamtiež.

preto EÚ vo svojej globálnej stratégii označila hybridné hrozby ako jednu z najvážnejších bezpečnostných výziev Únie.[3]

SR je parciálnou súčasťou súčasného komplexného a dynamicky sa vyvíjajúceho bezpečnostného prostredia, čelí rovnakým typom hrozieb ako iné členské štáty EÚ a NATO, a preto tento typ hrozieb nemôže ignorovať. Napríklad teroristické útoky, ako uvádzajú Trifunovič a kol.,[4] môže dnes zasiahnuť kohokoľvek, kdekoľvek a kedykoľvek. Podobne ako hrozby šírené cestou internetu a sociálnych sietí.[5] Hybridné pôsobenie proti záujmom SR sa tak za posledných niekoľko rokov zintenzívnilo a presunulo z periférie do hlavného prúdu na takmer všetky úrovne spoločnosti, preto je nevyhnutné efektívne a účinne zmierňovať rozvratné pôsobenie hybridných aktérov.

Tí pod prahom zvyčajnej reakcie priamo vplývajú na verejnú mienku, zhoršujú existujúce pnutia a vyvolávajú nové napätie v spoločnosti, znižujú dôveru verejnosti v štátne inštitúcie, erodujú spoločenský konsenzus o správnosti demokratického usporiadania a euroatlantického ukotvenia SR, podporujú radikalizmus a extrémizmus a zároveň propagujú toxickú formu nacionalizmu, ktorá má tendenciu vyčleňovať a znevýhodňovať určité skupiny občanov, legitimizovať autokratické formy vládnutia a marginalizovať kľúčovú dôležitosť ľudských práv a princípov právneho štátu.[6] Z uvedených dôvodov je v súčasnosti aj vzhľadom na aktuálny vývoj bezpečnostnej situácie a bezpečnostného prostredia absolútne nevyhnutné skúmať problematiku hybridných hrozieb a prostredníctvom vedeckého výskumu prispieť k ich eliminácii a zmierňovaniu následkov realizovaných hybridných aktivít.

Teoreticko-metodologické východiská skúmania hybridných hrozieb

Z teoreticko-metodologického hľadiska, napriek v posledných rokoch rastúcemu záujmu a rozvíjajúcej sa akademickej i odbornej diskusii o hybridných hrozbách, zatiaľ stále neexistuje žiadna spoločná jednotná, unifikovaná a všeobecne akceptovaná definícia tejto kategórie hrozieb. Z toho dôvodu je možné stretnúť sa s ich viacerými definíciami. Z pohľadu medzinárodných organizácií NATO definuje hybridné hrozby ako *„kombináciu vojenských a nevojenských, ako aj skrytých a otvorených prostriedkov vrátane dezinformácií, kybernetických útokov, ekonomického tlaku, nasadzovania nepravidelných ozbrojených skupín a použitia bežných síl.“* Hybridné metódy sa používajú na rozmazanie hraníc medzi vojnou a mierom a snažia sa zasiať pochybnosti do myslí cieľovej populácie. Ich cieľom je destabilizovať a podkopať spoločnosti.[7]

Európska únia používa širšiu definíciu, podľa ktorej: *„Hybridné hrozby kombinujú konvenčné a nekonvenčné, vojenské a nevojenské aktivity, ktoré môžu byť koordinovaným spôsobom využívané štátnymi alebo neštátnymi aktérmi na dosiahnutie konkrétnych politických cieľov. Hybridné kampane sú multidimenzionálne, kombinujú donucovacie a podvratné opatrenia využívajúce konvenčné aj nekonvenčné nástroje a taktiky. Sú navrhnuté tak, aby bolo ťažké ich odhaliť alebo priradiť. Tieto hrozby sa zameriavajú na kritické zraniteľné miesta a snažia sa vytvoriť zmätok, ktorý by bránil rýchlemu a efektívnemu rozhodovaniu.“* Hybridné hrozby pritom môžu siahať od kybernetických útokov na kritické

---

[3] Bližšie pozri: EÚ. Shared Vision, 2016. *Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*. In *European External Action Service*.

[4] Bližšie pozri: TRIFUNOVIC, D. a kol., 2021. *Conceptualization of Terrorism as a Modern Form of Political Violence*. In *Political Sciences*, Roč. 24, č. 2, s. 108 –124.

[5] Bližšie pozri: ZACHAR KUCHTOVÁ, J., 2022. *Bezpečnosť na sociálnych sieťach*. In *Bezpečnosť elektronickej komunikácie: zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*, s. 237 – 247.

[6] MOSR, 2021. *Akčný plán koordinácie boja proti hybridným hrozbám*. In *Ministerstvo obrany Slovenskej republiky*.

[7] NATO, 2023. *NATO's response to hybrid threats*. In *North Atlantic Treaty Organisation*.

informačné systémy, cez narušenie kritických služieb, ako sú dodávky energie alebo finančné služby, až po podkopávanie dôvery verejnosti vo vládne inštitúcie alebo prehlbovanie sociálnych rozdielov.[8]

Európske centrum výnimočnosti pre boj proti hybridným hrozbám charakterizuje hybridné hrozby ako *„koordinovanú a synchronizovanú akciu, ktorá sa zámerne zameriava na systémovú zraniteľnosť demokratických štátov a inštitúcií prostredníctvom širokej škály prostriedkov, napríklad činnosti, ktoré využívajú prahy detekcie a pripisovania, ako aj rôzne rozhrania (vojna – mier, vnútorná – vonkajšia bezpečnosť, miestne – štátne a národné – medzinárodné), ako aj činnosti zamerané na ovplyvňovanie rôznych foriem rozhodovania na miestnej (regionálnej), štátnej alebo inštitucionálnej úrovni a navrhnuté tak, aby podporovali a/alebo napĺňali strategické ciele agenta a zároveň podkopávali a/alebo poškodzovali cieľ“*.[9] Experti z Haagskeho centra strategických štúdií charakterizujú hybridné hrozby veľmi jednoducho ako *„spektrum nežiaducich aktivít od násilných po nenásilné realizovaných vo vojenskej aj civilnej oblasti“*.[10]

Podľa Národného bezpečnostného analytického centra hybridné hrozby predstavujú *„súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny“*. Hybridné hrozby sú charakteristické simultánnym použitím viacerých nástrojov koordinovaným spôsobom s cieľom využiť zraniteľnosti (slabé miesta) protivníka a následne oslabiť jeho rozhodovacie procesy pri zachovaní určitého stupňa hodnoverného popretia. Strategickým cieľom týchto hrozieb je oslabenie dôvery verejnosti v demokratické inštitúcie, prehĺbenie nezdravej polarizácie na národnej a medzinárodnej úrovni, spochybnenie základných hodnôt demokratických spoločností, ako aj zisk geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných a ovplyvňovania demokratických rozhodovacích procesov.[11]

Ďalší rozmer definovania hybridných hrozieb možno nájsť v správe o globálnych hrozbách, v ktorej je uvedené, že *„hybridné hrozby sú kombináciou rôznych typov hrozieb a útokov, ktoré zahrňujú kombináciu digitálnych a fyzických prvkov, pričom sa snažia využiť slabiny a zraniteľnosti v oboch týchto sférach s cieľom dosiahnuť neoprávnený prístup, spôsobiť škody alebo získavať citlivé informácie“*. Digitálna časť hybridných hrozieb zahŕňa kybernetické útoky a techniky, ako sú napríklad phishing, ransomware, malvér, sociálne inžinierstvo a iné. Tieto útoky sú vykonávané prostredníctvom počítačových sietí a systémov s cieľom narušiť, zneužiť alebo získať kontrolu nad digitálnymi prostriedkami a údajmi. Fyzická časť hybridných hrozieb sa zameriava na využitie fyzických prvkov alebo akcií na realizáciu rôznych typov útokov s cieľom narušiť, poškodiť alebo znefunkčniť fyzickú infraštruktúru protivníka. Hybridné hrozby tak využívajú kombináciu digitálnych a fyzických techník s cieľom maximalizovať svoj dosah a účinnosť. Ich cieľom môže byť spôsobenie škôd, získavanie citlivých informácií, vyvolávanie zmätku a/alebo vytváranie nepriateľského vplyvu v digitálnom a fyzickom prostredí.[12]

Spomedzi autorov, ktorí sa vo svojich prácach bližšie zaoberajú hybridnými hrozbami, Glenn definuje hybridné hrozby ako *„nepriateľa, ktorý súčasne a adaptabilne používa rôzne kombinácie politických, ekonomických, sociálnych a informačných prostriedkov a zároveň konvenčné, nepravidelné, katastrofické, teroristické a rozvratné kriminálne metódy vedenia*

[8] EÚ, 2018. *A Europe that Protects: Countering Hybrid Threats*. In *European External Action Service*.
[9] Hybrid CoE., 2023. *Hybrid threats as a concept*. In: *The European Centre of Excellence for Countering Hybrid Threats.*
[10] HCSS., 2022.*Hybrid Threats*. In *The Hague Centre for Strategic Studies*.
[11] NBAC, 2021. *Hybridné hrozby*. In: *Krátky slovník hybridných hrozieb*.
[12] GW, 2023. *Global Threats Report*. In *Gatewatcher*.

boja“.[13] Podľa Hoffmana *„hybridné hrozby zahŕňajú celú škálu konvenčných i nekonvenčných spôsobov boja a neregulárnej taktiky, ako aj kriminálne a teroristické činy, ktoré zahŕňajú neobmedzené násilie, nátlak, spoločenské nepokoje a rozvrat“*.[14]

Pre lepšie pochopenie skúmanej problematiky a vytvorenie si komplexného obrazu o tom, čo to vlastne sú hybridné hrozby, čo zahŕňajú, čo je ich obsahom, cieľom, v čom spočíva ich nebezpečenstvo a pod., je potrebné – v rámci teoreticko-metodologických východísk skúmania problematiky hybridných hrozieb – spomenúť aj ďalšie úzko súvisiace pojmy, ako sú hybridné ovplyvňovanie, hybridná aktivita (akcia) a predovšetkým hybridná vojna.

Hybridné ovplyvňovanie predstavuje čin, ktorého výsledky dosahuje podnecovateľ prostredníctvom množstva vzájomne sa doplňujúcich metód a prostredníctvom využitia zraniteľností cieľovej komunity. Hybridné ovplyvňovanie je pritom realizované s využitím a prostredníctvom ekonomických, politických alebo vojenských nástrojov. Môže byť taktiež vykonávané s použitím technológií a sociálnych sietí, pričom dané metódy môžu byť použité súčasne alebo postupne. Hybridné ovplyvňovanie je ťažké rozpoznať.[15]

Hybridná aktivita (akcia) je činnosť vyznačujúca sa nejednoznačnosťou, ktorá vzniká kombináciou využívania konvenčných a nekonvenčných prostriedkov – dezinformácií, zasahovania do politickej diskusie či volieb, narušením funkčnosti či útokmi na kritickú infraštruktúru, realizáciou kybernetických operácií, rôznych foriem kriminálnych aktivít a asymetrického využívania vojenských prostriedkov a vedenia vojny.[16]

Používaním konvenčných a nekonvenčných prostriedkov sa hybridní aktéri snažia zahaliť svoju činnosť do nejasnosti a nejednoznačnosti, čo komplikuje pripisovanie a odozvu. K hybridným aktivitám patrí aj využívanie rôznych sprostredkovateľov alebo zástupných aktérov, čo jednak podporuje dosiahnutie stanovených cieľov a jednak sťažuje možnosti ako zabrániť hybridnej akcii alebo reagovať na ňu. Hybridné akcie môžu zahŕňať napríklad aj zneužívanie právnych pravidiel a procesov, podporu polovojenských a extrémistických skupín alebo strategickú korupciu.

Aktuálne prebiehajúca tranzícia v medzinárodných mocenských štruktúrach poskytuje veľmi úrodné prostredie pre hybridné akcie. Narastajúci konflikt hodnôt medzi liberálnymi demokratickými štátmi a autoritárskymi režimami narúša medzinárodné normy a inštitúcie a robí z otvorených demokratických spoločností ciele komplexných hybridných akcií. Hybridní aktéri prostredníctvom hybridných aktivít zvyšujú polarizáciu a napätie v spoločnostiach a snažia sa narušiť jednotnosť tak v rámci jednotlivých členských krajín EÚ alebo NATO, ako aj medzi členskými štátmi uvedených organizácií navzájom, čím sa stávajú zraniteľnejšími voči vonkajším zásahom. Vznik nových sociálnych médií, sietí a platforiem v úzkej súvislosti s dynamickým vývojom v oblasti moderných informačných a komunikačných technológií, systémov a prostriedkov a zvyšujúca sa vzájomná previazanosť poskytujú hybridným aktérom silné nástroje a možnosti, ako prostredníctvom nich šíriť hybridné hrozby.

V kontexte uvedeného Hybrid CoE charakterizuje hybridné hrozby ako:

- koordinované a synchronizované akcie, ktoré sú zámerne zacielené na systémovú zraniteľnosť demokratických štátov a ich inštitúcií prostredníctvom širokej škály prostriedkov;
- činnosti, ktoré využívajú prahy detekcie a pripisovania, ako aj rôzne rozhrania (vojna – mier, vnútorná – vonkajšia bezpečnosť, miestna – štátna, národná – medzinárodná);

---

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

[14] HOFFMAN, F. G., 2007. *Conflict in the 21st Century*: *The Rise of Hybrid Wars*. In: *Potomac Institute for Policy Studies*, s. 8.

[15] YT, 2017. *Security Strategy for Society*. In: *Yhteiskunnan Turvallisuus*, s. 95.

[16] ZANDEE, D. a kol., 2021. *Hybrid threats: searching for a definition*. In *Netherlands Institute of International Relations.*

- činnosti zamerané na ovplyvňovanie rôznych foriem rozhodovania na miestnej (regionálnej), štátnej alebo inštitucionálnej úrovni a ktoré sú navrhnuté tak, aby podporovali a/alebo napĺňali strategické ciele aktéra a zároveň podkopávali a/alebo poškodzovali cieľ.[17]

So skúmanou problematikou hybridných hrozieb, ako už bolo naznačené vyššie, veľmi úzko súvisí pojem hybridná vojna. Ide o pojem, pod ktorým možno chápať *„široké spektrum nepriateľských aktivít, v ktorých úloha vojenského komponentu je skôr malá, pretože politický, informačný, ekonomický a psychologický vplyv sa stáva hlavným prostriedkom vedenia boja. Takéto metódy pomáhajú dosiahnuť významné výsledky: teritoriálne, politické a ekonomické straty nepriateľa, chaos a rozvrat systému výkonu štátnej moci a oslabenie morálky spoločnosti“*.[18] Hybridnú vojnu možno tiež chápať ako *„súbor letálnych a neletálnych prostriedkov, ktoré štátny alebo neštátny aktér využíva k presadeniu svojich záujmov proti vôli iného aktéra. Hybridná vojna pritom kombinuje hneď niekoľko spôsobov vedenia boja: klasické vojenské operácie, operácie v kybernetickom priestore alebo kybernetické útoky, špionáž, šírenie nepravdivých informácií s cieľom pôsobiť na verejnú mienku nepriateľa a pod.“*.[19]

Ďalšia z definícií hovorí, že *„hybridná vojna je ozbrojený konflikt vedený kombináciou nevojenských a vojenských prostriedkov s cieľom ich synergickým efektom prinútiť protivníka k vykonaniu takých krokov, ktoré by sám o sebe nevykonal. Aspoň jednou stranou konfliktu je štát. Hlavnú úlohu pri dosiahnutí cieľov vojny hrajú nevojenské prostriedky v podobe informačných a psychologických operácií, propagandy, ekonomických sankcií, embárg, kriminálnych aktivít, teroristických aktivít a iných subverzívnych aktivít podobného charakteru, ktoré sú vedené proti celej spoločnosti, najmä proti jej politickým štruktúram, orgánom štátnej správy a samosprávy, ekonomike štátu, morálke obyvateľstva a ozbrojeným zložkám“*.[20]

Celkovo sa dá konštatovať, že *„v prípade hybridnej vojny ide o spôsob vedenia moderného ozbrojeného konfliktu. Konfliktu, ktorý nezačína výstrelom a už vôbec nie vyhlásením vojny. Konfliktu, o ktorom napadnutá spoločnosť spočiatku ani nevie, dokonca ani netuší alebo si nepripúšťa, že bola napadnutá a nachádza sa vo vojne. Ide o dynamickú kombináciu vojenských a nevojenských (politických, diplomatických, ekonomických, technických/technologických, humanitárnych, diverzných, teroristických, kriminálnych atď.) aktivít realizovaných štátnymi i neštátnymi aktérmi, pravidelnými i nepravidelnými formáciami, pri využití dezinformácií, propagandy, sankcií a ďalších nástrojov a metód a realizácii informačných, kybernetických a psychologických operácií“*.[21]

Ako vidieť, vyššie uvedené definície hybridných hrozieb, hybridných aktivít/akcií, hybridného ovplyvňovania a hybridnej vojny sú rôzne. Niektoré sa zhodujú viac, niektoré menej, záleží to hlavne od ich autorov, ich uhla pohľadu, profesionálneho či vedného zamerania, príslušnosti a pod. Aspoň zatiaľ však takáto variabilita vôbec nie je na škodu. Definície by totiž nemali zväzovať ani súčasných ani budúcich výskumníkov, naopak, mali by zostať flexibilné, aby mohli reagovať na premenlivú povahu, rôznorodosť a mnohostrannosť hybridných hrozieb.

---

[17] Hybrid CoE, 2023. *Hybrid threats as a concept*. In: *The European Centre of Excellence for Countering Hybrid Threats*.

[18] MANKO, O. a Y. MIKHIEIEV, 2018. *Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine*. In: *Information & Security: An International Journal*, s. 13.

[19] DANYK, Y. , MALIARCHUK, T. a C. BRIGGS, 2017. *Hybrid War: High-tech, Information and Cyber Conflicts*. In: *Connections*, s. 6.

[20] KŘÍŽ, Z.,SCHEVCUK, Z. a P. ŠTEVKOV, 2015. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy*, s. 8.

[21] IVANČÍK, R., 2016. *Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia*. In: *Medzinárodné vzťahy*. Roč. 14, č. 2, s. 148.

Dôležité je, aby sa prostredníctvom predkladaných definícií podarilo vystihnúť, resp. aby z nich vyplývalo, že ide o súbor rôznych nátlakových a podvratných činností zahŕňajúcich využívanie konvenčných aj nekonvenčných metód (napríklad diplomatických, vojenských, ekonomických, technologických, kriminálnych atď.), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele bez toho, aby formálne vyhlásili vojnu. Snahou je zneužívať zraniteľnosť protivníka a vytvárať neprehľadné situácie s cieľom narušiť rozhodovacie procesy.[22]

Všeobecne možno na záver tejto podkapitoly uviesť, že medzi autormi jednotlivých definícií hybridných hrozieb, ktoré môžeme nájsť v odbornej literatúre, panuje zhoda v tom, že tieto hrozby zahŕňajú kombinované použitie vojenských aj nevojenských prostriedkov a konvenčných aj nekonvenčných metód používaných štátnymi a neštátnymi aktérmi za účelom rozvratu a podkopania základov spoločnosti protivníka, narušenia prebiehajúcich politických, ekonomických, spoločenských, rozhodovacích a ďalších procesov, zvýšenia napätia a polarizácie spoločnosti, vyvolania nespokojnosti určitých skupín obyvateľstva, zvýšenia nedôvery v štát, demokratický ústavný poriadok, legitimitu a dôveryhodnosť inštitúcií, v schopnosť riešiť existujúce i vznikajúce problémy a pod. Hlavným cieľom hybridných hrozieb je využitie zraniteľnosti napadnutej spoločnosti na celkové oslabenie a zníženie jej odolnosti.

Aktuálny stav a opatrenia v oblasti boja proti hybridným hrozbám

Keďže boj proti hybridným hrozbám úzko súvisí so zaisťovaním národnej bezpečnosti a obrany, zachovaním práva a udržiavaním verejného poriadku, hlavnú zodpovednosť nesú členské štáty, pretože jednotlivé slabiny sú väčšinou špecifické pre jednotlivé krajiny. Súvisí to aj s tým, že hybridné stratégie sú založené na vysokej adaptabilite a iniciátori útokov prispôsobujú výber použitých prostriedkov slabým miestam konkrétneho cieľového štátu. Aj preto hlavnú zodpovednosť za identifikáciu týchto slabých miest, ktoré by útočník mohol využiť, a prijímanie adekvátnych opatrení nesie predovšetkým konkrétny štát.[23]

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

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- rozsiahle sabotáže proti kritickej infraštruktúre, ale aj proti akejkoľvek inej infraštruktúre, ktorá má zásadný význam pre štát a spoločnosť;
- kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely;
- hrozba použitia vojenskej sily.[24]

---

[22] ZANDEE, D. a kol., 2021. *Hybrid threats: searching for a definition*. In: *Netherlands Institute of International Relations*.
[23] NBÚ, 2018. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. In: *Národný bezpečnostný úrad*, s. 2.
[24] Tamtiež, s. 4.

Vyššie uvedené indikátory samé o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt ešte nemožno považovať za hybridnú hrozbu. Podstatnou črtou hybridného spôsobu boja je súčinnosť a prepojenie viacerých rôznych prvkov hybridnej hrozby a ich paralelné nasadenie a využívanie tak, aby vytvorili kvalitatívne vyššiu a zložitejšiu viacdimenzionálnu hrozbu. Hybridnou hrozbou sa tak rozumie až kombinované použitie niekoľkých – najmenej troch z vyššie uvedených indikátorov – v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku alebo kampane.[25]

V zákone č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov nie je žiadnemu štátnemu orgánu SR priamo vymedzená zodpovednosť za boj proti hybridným hrozbám. Z toho dôvodu v súčasnosti v SR žiadnemu zo štátnych orgánov nie je zverená do vecnej pôsobnosti problematika hybridných hrozieb. Žiaden z rezortov nedisponuje dostatočnými ľudskými, finančnými, materiálnymi, technickými a informačnými zdrojmi pre komplexné pokrytie tejto problematiky. Hybridné hrozby navyše majú prierezový, medziinštitucionálny charakter a spadajú do kompetencie viacerých štátnych orgánov. V rámci snáh o elimináciu hybridných hrozieb je preto nevyhnutne potrebné, aby všetky štátne orgány dôsledne uplatňovali právomoci v rámci tých kompetencií, ktoré im boli zverené. Z vyššie uvedeného je pochopiteľné, že by nebolo účelné – a s najväčšou pravdepodobnosťou ani možné – zveriť zodpovednosť za boj proti hybridným hrozbám a za plnenie všetkých s tým súvisiacich úloh do výlučnej pôsobnosti jediného rezortu.[26]

Princípy budovania a fungovania SR ako samostatného, nezávislého a zvrchovaného štátu sú deklarované stratégiami a upravené právnymi predpismi a ďalšími dokumentmi prijatými s cieľom zaistenia bezpečnosti a obrany a ochrany demokratických princípov fungovania štátu a na elimináciu možných ohrození štátu a jeho občanov.

Celé spektrum reakcií na možné zmeny bezpečnostného prostredia a nové bezpečnostné hrozby a výzvy vychádza z ústavného poriadku a Bezpečnostnej stratégie Slovenskej republiky. Tieto dokumenty sú základom pre tvorbu štátnej politiky a definovanie úloh krízového manažmentu, spravodajských služieb, obrany, vonkajšej a vnútornej bezpečnosti, ochrany kybernetického priestoru, kritickej infraštruktúry, zabezpečenia energetických zdrojov, ochrany životného prostredia, dopravnej infraštruktúry, finančného sektora, zdravotníctva, sociálneho zabezpečenia, vzdelávania, pre potláčanie prejavov extrémizmu a mediálnej podpory až po strategickú komunikáciu.

Súčasné nastavenie prijatých legislatívnych opatrení by malo byť zárukou adekvátnej reakcie štátu aj na možné hybridné hrozby a zároveň vytvárať predpoklady na zvyšovanie odolnosti štátu voči ich prejavom. Súčasťou zvyšovania odolnosti SR pred hybridnými hrozbami by malo byť zvýšenie úrovne bezpečnostného povedomia verejnosti a predstaviteľov verejnej moci o rizikách spojených s prejavmi hybridných hrozieb. Tam, kde je to účelné, by štátne orgány mali zapájať do edukatívnych podujatí aj akademickú obec, súkromný sektor a subjekty občianskej spoločnosti.[27]

Hoci boj proti hybridným hrozbám primárne súvisí so zaisťovaním národnej bezpečnosti a obrany a so zachovaním práva a verejného poriadku a hlavnú zodpovednosť zaň nesú členské štáty, pretože jednotlivé slabiny sú väčšinou špecifické pre jednotlivé krajiny, SR a mnoho ďalších členských štátov Únie sa stretáva aj so spoločnými hrozbami, ktorých cieľom sú cezhraničné siete alebo infraštruktúry. Takýmto hrozbám je možné efektívnejšie a

[25] NBÚ, 2018. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. In: *Národný bezpečnostný úrad*, s. 5.
[26] Tamtiež, s. 3.
[27] MOSR, 2021. *Akčný plán koordinácie boja proti hybridným hrozbám*. In *Ministerstvo obrany Slovenskej republiky*, s. 4.

účinnejšie čeliť pomocou spoločnej koordinovanej reakcie na nadnárodnej úrovni – na úrovni EÚ – prostredníctvom únijných politík a nástrojov, využitím európskej solidarity, vzájomnej pomoci a plného potenciálu Lisabonskej zmluvy. Politiky a nástroje EÚ totiž môžu zohrávať – a vo významnej miere už aj zohrávajú – zásadnú úlohu pri zvyšovaní informovanosti o hybridných hrozbách. Tým sa zvyšuje odolnosť členských štátov EÚ a zlepšuje ich schopnosť reagovať na spoločné hrozby.[28]

Cieľom spoločnej koordinovanej reakcie na úrovni EÚ je zavedenie komplexného prístupu, ktorý umožní Únii v koordinácii s jednotlivými členskými štátmi bojovať s konkrétnymi hrozbami hybridnej povahy tým, že sa medzi príslušnými nástrojmi vytvoria synergie a zlepší sa spolupráca medzi všetkými príslušnými aktérmi. Východiskom sú existujúce stratégie a sektorové politiky, ktoré prispievajú k dosiahnutiu vyššieho stupňa bezpečnosti. Medzi nástroje, ktoré môžu pomôcť v boji proti hybridným hrozbám, patrí najmä Európsky program v oblasti bezpečnosti[29], Globálna stratégia Európskej únie v oblasti zahraničnej a bezpečnostnej politiky[30], Akčný plán v oblasti európskej obrany[31], Stratégia kybernetickej bezpečnosti EÚ[32], Stratégia energetickej bezpečnosti[33] a ďalšie stratégie[34].

Keďže proti hybridným hrozbám bojuje aj NATO, SR v rámci úsilia o efektívnu a účinnú elimináciu a zmierňovanie dopadov hybridných hrozieb využíva nielen európsku úroveň spolupráce s členskými štátmi EÚ, ale aj transatlantickú úroveň spolupráce s ostatnými členskými štátmi Aliancie. Okrem toho využíva aj spoluprácu v rámci Európskeho centra výnimočnosti pre boj proti hybridným hrozbám[35] so sídlom v Helsinkách vo Fínsku, Kooperatívneho centra kybernetickej obrany NATO[36] so sídlom v Talline v Estónsku a Centra výnimočnosti NATO pre strategickú komunikáciu[37] so sídlom v Rige v Lotyšsku. Na doplnenie možno uviesť, že spolupráca sa zameriava hlavne na také prvky, ako je zlepšovanie informovanosti, posilňovanie odolnosti, prevencia, reakcia na krízu a obnova.

Záver

Na záver možno konštatovať, že hybridné hrozby so svojimi špecifickými vlastnosťami, komplexnosťou, mnohostrannosťou a rôznorodosťou ich prejavov budú v nasledujúcich rokoch aj naďalej patriť medzi najzávažnejšie výzvy pre bezpečnostné systémy všetkých súčasných spoločností, demokratických obzvlášť. Naliehavosť riešenia problematiky hybridných hrozieb ovplyvňujúcich tak nadnárodné (európske, transatlantické), ako aj národné (slovenské) bezpečnostné prostredie si preto vyžaduje okrem nastavenia možností adekvátnej reakcie na elimináciu ich prejavov aj účinnú prevenciu.

V prípade Slovenskej republiky, ako to vyplýva z Koncepcie pre boj proti hybridným hrozbám a Akčného plánu koordinácie boja proti hybridným hrozbám, je ambíciou zvyšovať efektívnosť a účinnosť prijímaných opatrení v rámci boja proti hybridným hrozbám, napríklad

---

[28] EÚ, 2016. *Joint Framework on Countering Hybrid Threats a European Union Response*. In: *Eur-Lex*.
[29] EÚ, 2015. *The European Agenda on Security*. In: *Eur-Lex*.
[30] EÚ, 2016.*Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. In: *European External Action Service*.
[31] EÚ, 2016. *European Defence Action Plan*. In: *Eur-Lex*.
[32] EÚ, 2020. *The EU's Cybersecurity Strategy for the Digital Decade*. In: *European Commission*.
[33] EÚ, 2015. *A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy*. In: *Eur-Lex*.
[34] Bližšie pozri napr.: EÚ, 2014. *For an open and secure global maritime domain: elements for a European Union maritime security strategy*. In: *Eur-Lex*.
[35] Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats
[36] CCDCoE. The NATO Cooperative Cyber Defence Centre of Excellence
[37] NSCCoE The NATO Strategic Communications Centre of Excellence

prostredníctvom zvýšenia povedomia spoločnosti o výskyte a prejavoch hybridných hrozieb alebo vytvorenia základov pre organizačno-inštitucionálne nastavenie identifikácie aktivít a informačných tokov k rozhodovacím orgánom ako reakcie na analýzu incidentov, ktoré môžu viesť k hybridným hrozbám.

Strategickým cieľom SR 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 vykonávané 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, ako aj posilnenie aktívneho pôsobenia SR pri rozvoji spolupráce na európskej a transatlantickej úrovni v rámci EÚ a NATO v oblasti boja proti hybridným hrozbám a posilňovania medzinárodnej spolupráce.

Kľúčovým predpokladom efektívnej a účinnej reakcie SR na hybridné pôsobenie je celospoločenský prístup k bezpečnosti a precízne nastavenie procesov zapojenia a vzájomnej koordinácie inštitúcií štátnej správy, verejného i súkromného sektora, akademickej sféry prostredníctvom vysokoškolských a výskumných inštitúcií, a taktiež občianskej spoločnosti. Celospoločenský prístup predpokladá sofistikovanú manipuláciu s otvorenými zdrojmi a transparentnú, vysoko koordinovanú a efektívnu strategickú komunikáciu štátu a z toho vyplývajúcu vysokú mieru verejnej diskusie a zapojenia verejnosti do eliminácie hybridných hrozieb všeobecne.

SR sa prostredníctvom prijímaných opatrení zároveň snaží reagovať na bezpečnostné riziká spojené so zahraničnými investíciami do kritickej infraštruktúry, médií alebo akademického sektora, na ovplyvňovanie volebných procesov, korupciu, či pôsobenie nelojálnych polovojenských skupín, so zvýšeným dôrazom na podvratné vplyvové aktivity štátnych aj neštátnych aktérov, ktorí využívajú propagandu, dezinformácie, hoaxy, šírenie nenávistných alebo extrémistických obsahov, a to aj verejne činnými osobami či dokonca predstaviteľmi verejnej moci. Ich cieľom je erózia spoločenského konsenzu o správnosti euroatlantického ukotvenia SR, dôvery v demokratické zriadenie a vo verejné inštitúcie, spochybňovanie štátnej identity, zdieľanej interpretácie histórie, viery v správnosť a dodržiavanie zákonov, či pocit občianskej spolupatričnosti.

Vláda SR v rámci úsilia o elimináciu hybridných hrozieb a zmierňovanie ich dôsledkov vychádza z predpokladu, že úspešná reakcia štátu na hybridné aktivity štátnych a/alebo neštátnych aktérov musí stáť na:

- koordinovanom zapojení relevantných ústredných orgánov štátnej správy, subjektov štátnej správy, ekonomického a akademického sektora a občianskej spoločnosti,
- vzniku a činnosti pracovísk pre boj s hybridnými hrozbami na relevantných ústredných orgánoch štátnej správy spolupracujúcich s Národným bezpečnostným analytickým centrom[38] ako národným kooperačným centrom pre hybridné hrozby,
- systémovej a koordinovanej implementácii konceptu strategickej komunikácie štátu zriadením a pôsobením útvaru strategickej komunikácie na Úrade vlády SR a taktiež relevantných ústredných orgánoch štátnej správy,
- kontinuálnom navyšovaní spôsobilostí ústredných orgánov štátnej správy a inklúzii širokej verejnosti.

[38] Národné bezpečnostné analytické centrum (NBAC) vzniklo 1. januára 2013 na základe projektu, ktorý schválila vláda SR uznesením č. 75 zo 7. marca 2012. Je definované ako analytické, komunikačné a kooperačné pracovisko Slovenskej informačnej služby s celoštátnou pôsobnosťou v oblasti bezpečnostných hrozieb. Medzi jeho hlavné úlohy patrí príprava komplexných analytických hodnotení bezpečnostných incidentov na základe hlásení prijatých od štátnych orgánov SR, monitorovanie bezpečnostnej situácie v SR z odkrytých zdrojov a poskytovanie analytických produktov o bezpečnostných hrozbách v SR určeným príjemcom. Bližšie pozri: SIS, 2023. *Národné bezpečnostné analytické centrum (NBAC)*. In: *Slovenská informačná služba*.

Úspešný prístup k zmierňovaniu dopadov hybridného ovplyvňovania a hybridných aktivít musí odrážať potreby súčasného komplexného a rýchlo sa meniaceho bezpečnostného prostredia, ktoré si vyžaduje celospoločenský prístup k bezpečnosti a obrane štátu. Preto je potrebné aj naďalej prijímať opatrenia zamerané na budovanie odolnosti obyvateľstva napríklad v podobe zavádzania moderných vzdelávacích programov do vzdelávacieho systému a riešení, ktoré zodpovedajú súčasným decentralizovaným možnostiam vzdelávania a technickým spôsobilostiam verejnosti. Súčasťou budovania odolnosti by mala byť tiež ochrana občianskej spoločnosti a transparentňovanie relevantných častí verejného priestoru.

V úplnom závere štúdie je možné v kontexte vyššie v texte uvedených informácií zdôrazniť, že prístupy v boji proti hybridným hrozbám si vyžadujú komplexnosť, flexibilitu, efektívnosť, účinnosť a účelnosť všetkých činností vykonávaných na strategickej úrovni, ktoré sú adekvátne podporené konkrétnymi opatreniami prijímanými a realizovanými na operačnej a taktickej úrovni. Zodpovedajúci strategický prístup – berúc do úvahy už viackrát zmienené členstvo SR v EÚ a NATO – by mal preto jednoznačne zahŕňať integrovaný model reakcie na hybridné hrozby, ktorý je kompatibilný so strategickými dokumentmi Únie a Aliancie v boji proti hybridným hrozbám.

Literatúra

CCDCoE, 2023. *The NATO Cooperative Cyber Defence Centre of Excellence*. In: *NATO*, 2023. [online] [cit. 2023-06-12] Dostupné na internete: <https://ccdcoe.org>.

DANYK, Y. , MALIARCHUK, T. a C.BRIGGS, 2017. *Hybrid War: High-tech, Information and Cyber Conflicts*. In: *Connections*, 2017, Roč. 16, č. 2, s. 5 – 24. ISSN 1812-1098.

EÚ, 2014. *For an open and secure global maritime domain: elements for a European Union maritime security strategy*. In: *Eur-Lex.* [online] [cit. 2023-06-11] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014JC0009>.

EÚ, 2015. *A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy*. In: *Eur-Lex*. [online] [cit. 2023-06-11] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:80:FIN>.

EÚ, 2015. *The European Agenda on Security*. In: *Eur-Lex.* [online] [cit. 2023-06-11] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52015DC 0185>.

EÚ, 2016. *Joint Framework on Countering Hybrid Threats a European Union Response*. In: *Eur-Lex*. [online] [cit. 2023-06-10] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018>.

EÚ, 2016. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. In: *European External Action Service*. [online] [cit. 2023-06-10]. Dostupné na internete: <https://www.eeas.europa.eu/sites/default/files/ eugs_review_web_0.pdf>.

EÚ, 2018. *A Europe that Protects: Countering Hybrid Threats*. In: *European External Action Service*. [online] [cit. 2023-06-06] Dostupné na internete: <https://www.dsn.gob.es/sites/ dsn/files/hybrid_threats_en_final.pdf>.

EÚ, 2020. *The EU's Cybersecurity Strategy for the Digital Decade*. In: *European Commission*. [online] [cit. 2023-06-11] Dostupné na internete: <https://digital-strategy.ec.europa.eu/en/ library/eus-cybersecurity-strategy-digital-decade-0>.

GW, 2023. *Global Threats Report*. In: *Gatewatcher*. [online] [cit. 2023-06-13] Dostupné na internete: <https://info.gatewatcher.com/en/gatewatcher-global-threats-report/>.

HCSS, 2022. *Hybrid Threats*. In *The Hague Centre for Strategic Studies*. [online] [cit. 2023-06-13] Dostupné na internete: <https://hcss.nl/research/hybrid-threats/>.

Hybrid CoE, 2023. *Hybrid threats as a concept*. In: *The European Centre of Excellence for Countering Hybrid Threats*.. [online] [cit. 2023-06-06] Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.

Hybrid CoE, 2023. *The European Centre of Excellence for Countering Hybrid Threats*. [online] [cit. 2023-06-12] Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats/>.

IVANČÍK, R., 2016. *Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia*. In: *Medzinárodné vzťahy.* Roč. 14, č. 2, s. 130 – 156. ISSN 1339 – 2751.

IVANČÍK, R., 2022. *Dezinformácie ako hybridná hrozba.* In: *Dezinformácie a právo – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru, s. 54 – 65. ISBN 978-80-8054-965-7.

JURČÁK, V. , JURČÁK, J. a J. SASARÁK, 2016. *Hybridné hrozby – výzva pre Európsku úniu*. In: *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava: Vydavateľstvo Ekonóm, s. 542 – 550. ISBN 978-80-225-4365-1.

JURČÁK, V. a J. TURAC, 2018. *Hybridné vojny – výzva pre NATO*. In: *Bezpečnostné fórum 2018 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Interpolis, s. 177 – 184. ISBN 978-80-972673-5-3.

KŘÍŽ, Z., SCHEVCUK, Z. a P. ŠTEVKOV, 2015. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy*. Ostrava: Jagelo, 16 s. ISBN 978-80-904850-2-0.

MANKO, O. a Y. MIKHIEIEV, 2018. *Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine*. In: *Information & Security: An International Journal.* Roč. 41, s. 11 – 20. ISSN 0861-5160.

MOSR, 2021. *Akčný plán koordinácie boja proti hybridným hrozbám*. In: *Ministerstvo obrany Slovenskej republiky*. [online] [cit. 2023-06-06] Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf >.

NATO. 2023. NATO's response to hybrid threats. In: *North Atlantic Treaty Organisation*, 2023. [online] [cit. 2023-06-06] Dostupné na: <https://www.nato.int/cps/en/natohq/topics_156338.htm>.

NBAC, 2021. *Hybridné hrozby*. In: *Krátky slovník hybridných hrozieb* [online] [cit. 2023-06-12] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>.

NBÚ, 2018. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám*. In: *Národný bezpečnostný úrad*. [online] [cit. 2023-06-06] Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>.

NSCCoE, 2023. *The NATO Strategic Communications Centre of Excellence*. In: *NATO*. [online] [cit. 2023-06-12] Dostupné na internete: <https://stratcomcoe.org>.

SIS, 2023. *Národné bezpečnostné analytické centrum (NBAC)*. In: *Slovenská informačná služba.* [online] [cit. 2023-06-14] Dostupné na internete: <https://www.sis.gov.sk/o-nas/nbac.html>.

TOMÁŠEK, R., 2022. *O hybridných hrozbách a hybridnej vojne*. In: *Národná a medzinárodná bezpečnosť 2022 – zborník vedeckých prác z 13. medzinárodnej vedeckej*

konferencie. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, s. 319-328. ISBN 978-80-8040-631-8.

TRIFUNOVIC, D., KAZANSKÝ.R. a P. NEČAS., 2021. *Conceptualization of Terrorism as a Modern Form of Political Violence*. In: *Politické vedy. R*oč. 24, č. 2, s. 108-124. ISSN 1335 – 2741.

YT, 2017. *Security Strategy for Society*. In: *Yhteiskunnan Turvallisuus.* [online] [cit. 2023-06-06] Dostupné na internete: <https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf>.

ZACHAR KUCHTOVÁ, J., 2022. *Bezpečnosť na sociálnych sieťach.* In: *Bezpečnosť elektronickej komunikácie: zborník príspevkov z vedeckej konferencie*. Bratislava: Akadémia Policajného zboru, s. 237 – 2477. ISBN 978-80-8054-968-8.

ZANDEE, D. a kol., 2021. *Hybrid threats: searching for a definition*. In: *Netherlands Institute of International Relations*. [online] [cit. 2023-06-06] Dostupné na internete: <https://www.clingendael.org/pub/2021/countering-hybrid-threats/2-hybrid-threats-searching-for-a-definition/>.

Keywords: security, hybrid threats, security environment, measures, society

Summary

In the first two decades of the third millennium, there were fundamental changes in the global and regional security environment and the transformation of traditional security threats simultaneously. In recent years, they have become multi-dimensional, multi-layered and, in the complex conditions of our society's existence, they have acquired a hybrid character. They exploit the vulnerabilities of countries and try to weaken basic democratic values and freedoms. Indeed, hybrid threats are related to the use of a wide range of different means, such as propaganda, disinformation, hoaxes, cyber-attacks, organized crime, economic, political, and social pressure, terrorism etc. All of them lead to the undermining of democratic foundations and the destabilization of the political, economic, and social elements of society. Therefore, the author, using relevant methods of qualitative theoretical scientific research, deals in this scientific study with the issue of hybrid threats and – considering the current development of the security environment and the security situation – also the need to take efficient and effective measures aimed at their elimination.

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

Recenzenti: doc. PhDr. Rastislav Kazanský, PhD., MBA, doc. Ing. Michal Orinčák, PhD.