

TERMINOLOGICKÉ A KONCEPTUÁLNE VÝCHODISKÁ PROBLEMATIKY HYBRIDNÝCH HROZIEB¹

TERMINOLOGICAL AND CONCEPTUAL FOUNDATIONS OF HYBRID THREATS²

JUDr. Patrícia Krásná, PhD., LL.M.

Akadémia Policajného zboru v Bratislave

Sklabinská 1, 835 17 Bratislava, Slovenská republika

patricia.krasna@akademiapz.sk

Abstrakt: Téma „hybridné hrozby“ rezonuje v rámci spoločnosti už dlhšiu dobu. V rámci realizácie riadených rozhovorov, ktoré sme realizovali aj pre účely spracovania tejto vedeckej štúdie nám vzišlo, že odborníci, ale aj široká verejnosť eviduje tento pojem, avšak nie úplne presne dokážu definovať, čo hybridné hrozby sú. V rámci maximálnej stručnosti je možné uviesť, že hybridné hrozby predstavujú komplexný fenomén súčasného bezpečnostného prostredia, ktorý kombinuje vojenské a nevojenské nástroje s cieľom ovplyvňovať stabilitu a fungovanie štátu. Vedecká štúdia sa zameriava na terminologické a konceptuálne východiská problematiky hybridných hrozieb, analyzuje základné pojmy, elementárne piliere ich konceptu a charakterizuje jednotlivé fázy hybridného pôsobenia. Súčasne poukazuje na význam strategickej komunikácie ako efektívneho nástroja budovania odolnosti Slovenskej republiky voči hybridným hrozbám. Zdôrazňuje potrebu komplexného prístupu k posilňovaniu bezpečnosti a odolnosti štátu v podmienkach dynamicky sa meniaceho bezpečnostného prostredia.

¹ Predložená vedecká štúdia je spracovaná ako výstup z národného projektu „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“, kód projektu: 314011CDW7.

² The present scientific study was prepared as an output of the national project “Enhancing Slovakia’s Resilience to Hybrid Threats through Strengthening Public Administration Capacities” (Project Code: 314011CDW7).

Kľúčové slová: hybridné hrozby, strategická komunikácia, odolnosť, bezpečnosť.

Abstract: The topic of hybrid threats has resonated within society for a considerable period of time. Based on the structured interviews conducted for the purposes of this scientific study, it emerged that both experts and the general public are familiar with the term; however, many are unable to define precisely what hybrid threats actually entail. In its broadest and most concise sense, hybrid threats may be understood as a complex phenomenon of the contemporary security environment that combines military and non-military instruments with the aim of influencing the stability and functioning of a state. This scientific study focuses on the terminological and conceptual foundations of hybrid threats, analysing the key concepts, the fundamental pillars of the hybrid threat framework, and the individual phases of hybrid activities. Furthermore, it highlights the importance of strategic communication as an effective tool for strengthening the resilience of the Slovak Republic against hybrid threats. The study emphasises the need for a comprehensive approach to enhancing national security and resilience in the context of a dynamically evolving security environment.

Key words: hybrid threats, strategic communication, societal resilience, security.

ÚVOD

Národné, ale aj medzinárodné bezpečnostné prostredie sa neustále vyvíja. Je závislé od vývoja vo vnútri štátu, ale podlieha aj vplyvom z vonkajšieho prostredia. V súvislosti s daným, tak postupom času prešlo bezpečnostné prostredie na národnej, ale aj medzinárodnej úrovni významnými a zásadnými zmenami. Výsledkom týchto konverzií je opodstatnene i zmena už známych, identifikovaných hrozieb, ktoré podmieňujú ohrozenie bezpečnostného prostredia. Hrozby získali v dôsledku rozvoja technológií, ale aj spoločnosti ako takej, úplne novú dimenziu, zvýšila sa ich intenzita, efektívnosť, ale aj zložitosť. Práve ich zložitosť je dôvodom na zdôraznenie a uvedomenie si skutočnosti, že identifikujeme potrebu predvídať vždy a za každých okolností narušenie bezpečnostného prostredia, resp. rôzne útoky, ktoré nás ohrozujú na národnej, ale i nadnárodnej úrovni. Vyplýva to aj zo skutočnosti, že jednotlivé hrozby a ohrozenia v rýchlom slede a rozmanitosti enormne vzrástli, ale vzrástla aj ich viacrozmernosť.

Dôležitá konštanta poukazuje na to, že národné bezpečnostné prostredie je v súčasnosti podmienené nielen našim bezprostredným okolím, ale aj širokým celosvetovým rozmerom. Tento medzinárodný, celosvetový, priestor určuje aj pre našu krajinu priame alebo nepriame bezpečnostné hrozby, ktorým môžeme byť vystavení a voči ktorým je potrebné zaujať adekvátne stanovisko. Koordinovaná medzinárodná spolupráca je nevyhnutnosťou z aspektu globálneho efektu hybridných hrozieb. Zameranie by malo byť najmä na výmenu informácií, spoluprácu a organizovanie spoločných cvičení s inými krajinami v kontexte posilnenia schopností na kolektívnu reakciu voči hybridným hrozbám.³

Autorka v predloženej vedeckej štúdií poukazuje na samotnú podstatu hybridných hrozieb, pretože v rámci výskumu identifikovala bezpodmienečnú potrebu vymedzenia elementárnej podstaty hybridných hrozieb, ale aj následnej špecifikácie, ktorá čitateľovi poskytne ucelený náhľad na skúmanú problematiku. Autorka pred spracovaním vedeckej štúdie realizovala prieskum medzi študentmi Akadémie Policajného zboru v Bratislave (30 respondentov), ďalej už len „študenti“, odborníkmi z bezpečnostnej praxe (8 respondentov), ďalej už len odborníci a laickou verejnosťou (15 respondentov), ďalej už len „verejnosť“. Zisťovala povedomie o hybridných hrozbách a ich celkovej štruktúre. V rámci prieskumu boli sumarizované nasledovné výsledky. U študentov 73 % uviedlo, že sa s pojmom „hybridné hrozby stretlo. U odborníkov sa s daným pojmom stretlo 91 % respondentov a pri spoločnosti to bolo 68 % respondentov. Je zjavné aj z týchto výsledkov, že špecifikácia hybridných hrozieb je potrebná. Následne sme sa dopytovali na význam pojmu „hybridné hrozby“. U študentov 46 % vedelo aspoň z časti definovať tento pojem, odborníci vedeli definovať pojem v rozsahu 81 % a verejnosť v rozsahu 25 %. Tiež nám to potvrdilo potrebu definovať a jasne vymedziť tento pojem a poukázať na jeho podstatu a význam.

Následne v rámci predloženej štúdie autorka bude definovať základné pojmy a východiská spojené s problematikou hybridných hrozieb.

TEORETICKÉ VÝCHODISKÁ A ZÁKLADNÉ POJMY SPOJENÉ S PROBLEMATIKOU HYBRIDNÝCH HROZIEB

³ GLÄNZEL, W., THIJS, B. Using hybrid methods and ‘core documents’ for the representation of clusters and topics: the astronomy dataset. *Scientometrics* 111, s. 1075. <https://doi.org/10.1007/s11192-017-2301-6>.

Tak ako vnútorné hrozby a riziká, resp. vnútorná bezpečnosť, tak i vonkajšie hrozby, riziká, resp. vonkajšia bezpečnosť sú neoddeliteľné a sú zložkami toho istého javu - bezpečnosti alebo nebezpečnosti. Preto aj keď v istej fáze poznania sú skúmané oddelene, v záujme hlbšieho vystihnúť ich podstaty a charakteru je v konečnej fáze žiadúca ich syntéza, resp. uplatnenie aplikovaného racionalizmu.⁴ Vnútorná, ale i vonkajšia bezpečnosť štátu sú vzájomne prepojené a preto je potrebné prihliadať na ich odolnosť s aplikáciou prvku zodpovednosti a dôslednosti. Jednou z podstatných foriem, ktoré podporujú efektívne uplatnenie zodpovednosti a dôslednosti pri aplikácii prvkov zabezpečenia informovanosti o existencii a boji proti hybridným hrozbám je teoretická substancia poznatkov a výskumný aparát, ktorý špecifikuje jednotlivé paradigmy. Je preto opodstatnené, že skúmaniu každej problematiky predchádza aj priblíženie teoretického pozadia, ktoré je veľmi úzko previazané práve s následnou analýzou praktických problémov vznikajúcich v aplikačnej praxi.⁵ Veľmi dôležité je aj poskytovanie efektívnej a účelnej edukácie. Pretože ak budeme širokú odbornú, vedeckú a laickú verejnosť informovať a vzdelávať o podstate hrozieb a tiež ako predchádzať týmto hrozbám, či eliminovať ich, budeme vedieť zabezpečiť to, že akékoľvek hrozby budú mať na našu spoločnosť minimálny dopad. Informovanosť, spolupráca kompetentných subjektov na multidisciplinárnej úrovni a neustále napredovanie v oblasti zamedzenia vzniku ohrozenia na národnej, či medzinárodnej úrovni sú rozhodujúce. Súčasťou zvyšovania odolnosti Slovenskej republiky pred hybridnými hrozbami je tiež zvýšenie úrovne bezpečnostného povedomia verejnosti a predstaviteľov verejnej moci o rizikách spojených s ich prejavmi. Pretože veľmi často sa štátni aj neštátni aktéri snažia svoje politické ciele dosiahnuť práve prostredníctvom otvorených, ale i skrytých aktivít koordinovaných v rámci celej škály nástrojov moci, bez ohľadu na prípadnú kolíziu s medzinárodným poriadkom založeným na pravidlách. Práve v tomto kontexte sa objavil aj pojem „hybridné hrozby“, resp. „hybridný boj“.

Objektmi útokov hybridných hrozieb však nemusia byť iba individuálne štáty, hybridné hrozby presahujú ich hranice a môžu byť súbežne vedené proti viacerým štátom, prípadne medzinárodným zoskupeniam. V

⁴ VOLNER, Š. BEZPEČNOSŤ, RIZIKÁ A HROZBY 21. STOROČIA. In Univerzita Obrany. Ustav Strategických Studii. Obrana a Strategie; Brno Vol. 2005, Iss. 2, s. 78. doi:10.3849/1802-7199.

⁵ VRTÍKOVÁ, K., MOKRÁ, I. Spolupracujúci obvinený v trestnom konaní v intenciách aplikačnej praxe a úvahy de lege ferenda. Praha: Leges, 2023, s. 17.

medzinárodnom meradle môžu byť zamerané na narúšanie súdržnosti medzinárodných zoskupení, ktorých členom je aj Slovenská republika a oslabovanie vzájomnej solidarity medzi nimi. Problematika hybridných hrozieb sa dotýka celého sveta a je potrebné na základe tejto skutočnosti tak pristupovať aj k ich samotnému vnímaniu. Boj proti tomuto typu hrozieb preto vyžaduje intenzívnu medzinárodnú spoluprácu a koordináciu na nadnárodnej úrovni.

V súvislosti s vymedzením základných pojmov a východísk máme za to, že je podstatne dôležité charakterizovať samotný pojem „bezpečnosť“. Najprv je bezpodmienečne potrebné uviesť, že každý vníma bezpečnosť s prvkom odlišnosti, resp. so znakom diferencie. Bezpečnosť je každodennou súčasťou nášho života. Každý z nás pravidelne robí rozhodnutia na základe subjektívnych a objektívnych faktorov tak, aby sa cítil bezpečne a aby nič neohrozovalo jeho bezprostrednú existenciu. Vo všeobecnosti ale môžeme uviesť, že ide o stav, kedy daný objekt (či už ide o jednotlivca, štát a podobne) nepocituje nebezpečenstvo, resp. bezprostredné ohrozenie. Tak ako každý človek, aj rôzne krajiny chápu pojem bezpečnosť odlišne a z tohto dôvodu je i vnímanie samotných hybridných hrozieb odlišné.

Bezpečnosť síce nepatrí medzi najzákladnejšie ľudské potreby, ale pocit bezpečia, istoty definuje mieru slobody človeka a to, do akej miery sa pri svojom konaní obmedzuje rôznymi externými faktormi. Práve na základe týchto externých faktorov rozlišujeme objektívnu a subjektívnu bezpečnosť. V prípade objektívnej bezpečnosti ide o skutočný, objektívny stav vývoja rizika a miery jeho eliminácie. Subjektívna bezpečnosť predstavuje skôr celý komplex subjektívneho vnímania, pociťovania, vnútorného prežívania, posudzovania a hodnotenia rizika zo strany človeka, masmédií, politikov a iných subjektov. Pritom vzťah medzi objektívnou bezpečnosťou a jej subjektívnym odrazom nemusí byť vždy jednoduchým súladom, môžu sa v určitých prípadoch rozchádzať.⁶

Bezpečnosť je s určitosťou dôležitou súčasťou každej spoločnosti a jej konkrétne vnímanie je možné iba v tom prípade, ak poznáme a rozoznávame aj jednotlivé ohrozenia, ktoré môžu narušiť jej konštrukt. Najlepšou zárukou bezpečnosti, mieru, rozvoja a stability sú štáty rešpektujúce demokratické

⁶ BUZALKA, J. BLAŽEK, V. Metodológia a metodika vypracovania analýzy vnútorného ohrozenia bezpečnosti SR a z nej vyplývajúcich ohrození a rizík. In Metodológia a metodika analýzy zdrojov ohrozenia vnútornej bezpečnosti SR. Bratislava: Akadémia PZ - K krízového manažmentu vo verejnej správe, 2011, s. 18.

hodnoty a ľudské práva, ktoré predvídateľne pôsobia v medzinárodnom rámci založenom na pravidlách. Dodržiavanie zásad a noriem medzinárodného práva a pravidiel správania sa poskytuje základnú ochranu osobitne menším štátom.⁷ Bezpečnosť ako taká nie je jasne zadefinovaná, avšak je možné uviesť, že bezpečnosť je mimoriadne komplexným a viacrozmerným fenoménom, ktorý obsahuje značné množstvo oblastí a dimenzií. Jednou z nich je aj vnútroštátna bezpečnosť. Vnútornú bezpečnosť môžeme definovať ako „súhrn vnútorných bezpečnostných podmienok, legislatívnych noriem a opatrení, ktorými štát zabezpečuje demokraciu, ekonomickú prosperitu, bezpečnosť občanov, ako aj presadzovanie právnych a morálnych noriem.“ Bezpečnosť = „snaha o odstránenie hrozby“.⁸

Nebezpečenstvo je „potenciálne škodlivá fyzická udalosť, jav alebo ľudská činnosť, ktorá môže spôsobiť straty na životoch, škodu na majetku, sociálny a hospodársky rozvrat alebo poškodenie životného prostredia“.⁹ Čiže nebezpečenstvo je čokoľvek, čo má potenciálnu schopnosť spôsobiť ujmu, poškodenie.

Riziko je situačná charakteristika činnosti, ktorá spočíva v tom, že výsledok danej činnosti je neistý. Riziko predstavuje tiež vyjadrenie pravdepodobnosti a závažnosti poškodenia pôsobením nebezpečenstva. Prečo je potrebné poznať a posudzovať riziká? Hlavným cieľom posudzovania rizík je ochrana bezpečnosti jednotlivcov, ale aj celej spoločnosti. Práve posudzovanie rizík pomáha minimalizovať možné poškodenie, ktoré vzniká pôsobením nebezpečenstva. Efektívny prístup, systém vyhodnocovania jednotlivých rizík je predpokladom k zamedzeniu a šíreniu rizika v bezpečnostnom prostredí. Je tiež veľmi dôležité skúmať ako posudzovať riziká. Riziká je možné posudzovať podľa daných krokov, ktorými sú zbieranie informácií, identifikovanie nebezpečenstiev, ohrození a posúdenie rizík vyplývajúcich z ohrození (odhad pravdepodobnosti a závažnosti následkov a rozhodnutie, či je riziko akceptovateľné). Následne je ale potrebné aj realizovať plánovanie postupu na odstránenie alebo obmedzenie

⁷ Bezpečnostná stratégia 2021. [online]. [cit. 2025. 12. 08.] Dostupné na internete: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

⁸ KAČMÁR, R. ZaBEZPEČ si vedomosti: Čo je to bezpečnosť? SLOVENSKÝ INŠTITÚT PRE BEZPEČNOSTNÚ POLITIKU, 2016, s. 2.

⁹ EU-OSHA. [online]. [cit. 2026. 01. 15.] Dostupné na internete: <https://osha.europa.eu/sk/tools-and-resources/eu-osha-thesaurus/term/62115d>.

rizík, či opakovanie posudzovania rizík a dokumentovanie posudzovania rizík.¹⁰ Kľúčové je, aby sa posudzovanie rizík neustále opakovalo na periodickej báze a vyhodnocovalo za účelom efektívnej eliminácie vzniku akýchkoľvek rizík.

Hrozba je pojem používaný v riadení rizík pre označenie zdroja určitej negatívne udalosti, sily, objektu alebo aktivity, ktorá chce alebo môže poškodiť určitú hodnotu. Hrozba má negatívny vplyv na bezpečnosť alebo môže spôsobiť škodu, stratu, nežiaducu zmenu, či iný nežiaduci jav. Hrozbou môžu byť v príklade živelné pohromy (napr. povodeň, požiar, kalamita), havárie (napr. dopravná nehoda, kontaminácia vody, výbuch, radiácia), spoločenské javy (napr. vojnový konflikt, kriminalita), rôzne ekonomické javy (napr. finančná kríza, pohyb menového kurzu, nedostupnosť úverov) alebo správanie sa jednotlivcov (napr. zneužitie právomoci). Hrozba sa vyvíja v určitých fázach, využíva zraniteľnosť a spôsobuje škody. Základnou a veľmi podstatnou charakteristikou hrozby je úroveň hrozby, teda nebezpečnosť hrozby, schopnosť hrozby spôsobiť škodu. Efektívne je tiež realizovať ako analýzu rizík aj analýzu hrozieb, tak, aby bolo možné vykonať účinné protiopatrenia na ich zníženie, resp. na ich predchádzanie.¹¹

Podstatne dôležité je následne i vymedzenie jednotlivých pojmov, ktoré charakterizujú hybridné hrozby. Už elementárne vymedzenie pojmu hybridná hrozba poukazuje na skutočnosť, že ju nemožno ponímať v podobnom zmysle, v akom nahliadame na väčšinu ostatných hrozieb, ktoré predstavujú ohrozenie. U hrozieb vo všeobecnosti chápeme pôsobenie vo väčšine iba v jednej dimenzii. U hybridných hrozieb vždy ide o súbor aktivít, pretože nie každá samostatná hrozba je hneď hybridnou. To, čo je možné chápať pod pojmom hybridná hrozba, je primárne metóda, spôsob, akým je vedená konfrontácia, resp. konflikt, boj. Tento spôsob vedenia konfliktu predstavuje širokú, komplexnú, prispôsobivú a integrovanú kombináciu špecifických prostriedkov.

Hybridné hrozby definujeme ako:

- súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne

¹⁰ AVEN, T. A risk and safety science perspective on the precautionary principle. *Safety Science*, Volume 165, 2023, ISSN 0925-7535, <https://doi.org/10.1016/j.ssci.2023.106211>.

¹¹ ENGELHARD, I., M., UIJEN, S. L., SETERS, N., VELU, N. The Effects of Safety Behavior Directed Towards a Safety Cue on Perceptions of Threat. <https://doi.org/10.1016/j.beth.2014.12.006>.

aj neštátne subjekty koordinovaným spôsobom (pôsobia súčasne, sú súčasťou širšej kampane) využívať na dosiahnutie konkrétnych cieľov (rozvrat demokracie je hybrid, finančný zisk nie je hybrid) bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie (je náročne voči nim zasiahnuť, pretože obchádzajú alebo dokonca využívajú existujúce legislatívne rámce). Práve aj z tohto dôvodu je ich náročné, dokonca v niektorých prípadoch nemožné postihovať. Taktiež aj aktér, ktorý ich vykonáva, nie je vždy ľahko identifikovateľný a preto je voči nemu ťažké aj zakročiť.

Hybridné hrozby:

- sú realizované aktivitami charakterizovanými centrálnou riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Cieľom je teda polarizovať spoločnosť, vnášať do spoločnosti neistotu, tým podkopávať legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií, demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené.¹²

V súvislosti so špecifikáciou pojmu hybridné hrozby je tiež podstatné vnímať a chápať konkrétne pojmy identifikujúce ich kontext a nebezpečenstvo. Nátlak zahŕňa prinútenie subjektu, aby konala nedobrovoľne, použitím hrozieb, vrátane hrozieb použitím sily proti tejto strane. Zahŕňa súbor násilných akcií, ktoré porušujú slobodnú vôľu jednotlivca s cieľom vyvolať požadovanú reakciu. Podvracanie je akt, ktorým sa má v celej oblasti, na ktorú má vplyv, zmeniť štruktúra a tým sa zmení, resp. ohrozi jej bezpečnosť. Či už je to umelecká, morálna, sociálna, ale najmä politická oblasť. V prípade podvracania nestačí, že sa zmení jeden prvok alebo faktor, má za cieľ zmeniť čo najviac elementov. Subverzia je radikálna zmena od miestnej úrovne. To znamená, že sa snaží úplne zmeniť prvky, ktoré definujú zloženie spoločnosti.¹³

¹² KONCEPCIA PRE BOJ SLOVENSKEJ REPUBLIKY PROTI HYBRIDNÝM HROZBÁM. [online]. [cit.2023.09.06.]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>.

¹³ MASCHMEYER, L. A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*. <https://doi.org/10.1080/01402390.2022.2104253>.

Minulosť traďuje konvenčné vojenské konflikty, ktoré destabilizovali jednotlivé krajiny, ale aj celý svet. Avšak konvenčný vojenský konflikt má v súčasnosti podstatne vyššie politické, finančné, ľudské a morálne náklady. Z tohto dôvodu sa čoraz viac štátnych a neštátnych aktérov spolieha na nevojenské prostriedky tak, aby nemuseli formálne vyhlásiť vojnu. Paralelným použitím nátlakových a podvratných činností, konvenčných a nekonvenčných metód môžu destabilizovať spoločnosť cieľových štátov a oslabiť ich tak, aby boli ľahšie ovplyvniteľné alebo v krajnom prípade aj menej odolné voči použitiu konvenčnej vojenskej sily.

Konvenčný ozbrojený konflikt predstavuje typ ozbrojeného konfliktu, kedy jednotlivé strany používajú konvenčné zbrane - všetky zbrane okrem zbraní hromadného ničenia, jadrových, biologických a chemických zbraní, pričom bojujú otvorene na zemi, vo vzduchu či na mori. Sily oboch bojujúcich strán sú jasne definované a organizované. Základným cieľom konvenčnej vojny je oslabiť alebo zničiť nepriateľské ozbrojené sily, obsadiť územie a narušiť jeho schopnosť ďalej viesť konvenčnú vojnu. Za konvenčný konflikt sa obyčajne považujú bojové operácie vedené v súlade s medzinárodným vojnovým právom (definované Haagskym dohovorom, Ženevskými konvenciami a ďalšími dokumentmi), kde sa dodržiavajú práva vojnových zajatcov, civilistov a podobne.¹⁴

Nekonvenčný konflikt predstavuje viacero foriem a nástrojov, ktoré majú za cieľ oslabiť adresný štát, spoločnosť, napr. nepriateľská propaganda, podpora extrémizmu, využívanie národnostných alebo náboženských komunít nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru a tiež kyberútoky.

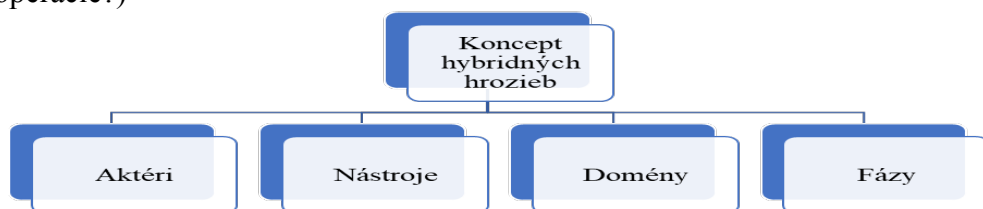
Vojenský konflikt predstavuje vojnu, medzinárodný ozbrojený konflikt alebo zdĺhavý ozbrojený konflikt na území štátu medzi vládnyimi orgánmi a organizovanými ozbrojenými skupinami alebo medzi takýmito skupinami navzájom s výnimkou vnútorných nepokojov a napätí, ako sú vzbury, izolované a ojedinelé akty násilia alebo iné akty podobnej povahy.¹⁵

KONŠTITUTÍVNE PRVKY KONCEPTU HYBRIDNÝCH HROZIEB

¹⁴ POSEN, B. R. Inadvertent escalation: Conventional war and nuclear risks. Cornell University Press, 2014, s. 51. 321 s. ISBN 978-0-8014-2563-9.

¹⁵ VEJMEĽKA, O. a kol. Vojenský výkladový slovník vybraných operačných pojmov. Správa doktrín Ředitelství výcviku a doktrín, Vyškov, 2005, s. 46.

V prípade, keď chceme dosiahnuť, že konceptu hybridných hrozieb budú všetci rozumieť a budú ho chápať je bezprostredne potrebné poznať konkrétne piliere, ktoré ho tvoria. Tieto piliere sú identifikované ako: Aktéri (kto) a ich Strategické ciele (prečo), Nástroje (ako) používané aktérmi, Domény (kde), ktoré sú cieľom hybridných hrozieb a Fázy (vrátane typov činností pozorovaných v každej fáze, teda ako môže vyzeráť priebeh hybridnej operácie?)



Obrázok 1: Koncept hybridných hrozieb.

Zdroj: vlastné spracovania na základe odbornej literatúry.

Aktéri hybridných hrozieb - Aktéri hybridných hrozieb využívajú kombináciu rôznych nástrojov tak, aby dosiahli strategické ciele. Ich cieľom je ovplyvniť systémové zraniteľné miesta demokracie za využitia všetkých dostupných nástrojov. Podľa toho, aké nástroje využívajú, vieme následne aj diferencovať samotných aktérov na štátnych, neštátnych aktérov a ich ciele. Každý nástroj, ktorý využívajú aktéri sa zameriava najčastejšie na viacero dôležitých domén, ale tiež i na citlivé „rozhranie“, resp. „hranicu“ týchto domén. Aktéri hybridných hrozieb sa sledovaný cieľ snažia dosiahnuť buď priamym alebo postupným účinkom. Z uvádzaného je zrejmé, že dosiahnutie cieľov nie je iba o konkurencii, resp. porážke konkurenčných štátov, ale zahŕňa aj neštátnych aktérov, ktorých praktiky nie sú namierené na vojenské získanie územia, ale na získanie kontroly obyvateľstva. Hybridné hrozby sú prezentáciou kreatívneho spôsobu prepojenia nových a starých nástrojov a stávajú sa dôležitým taktickým konaním, nástrojom, pre tých, ktorým chýbajú schopnosti alebo príležitosti presadiť svoje strategické záujmy inak. Takýto druh „sily“ je možné nazvať aj silou slabých.¹⁶ Pretože v prípade, aj ak slabší aktér dokáže účelne skombinovať nástroje útoku, ktoré má k dispozícii, dokáže zaútočiť aj na toho najsilnejšieho súpera. Takáto kombinácia nástrojov útoku napomáha aktérovi k dosiahnutiu jeho strategického cieľa bez jeho detegovania, bez odporu voči nemu a bez akejkoľvek reakcie na jeho útok.

¹⁶ CULLEN, P. et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 2021, s. 42. <http://www.doi.org/10.2760/44985>.

Zároveň využitie sily hybridných hrozieb umožňuje aktérovi minimalizovať riziko otvoreného konfliktu.

Aktéri hybridných hrozieb sa preto často prikláňajú k ovplyvňovaniu samotného rozhodovacieho procesu, teda aj rozhodovacieho centra, v rámci ich cieľa. Môže ísť napr. o vplyv na rozhodovanie v malom rozsahu, ale aj na rozhodovanie veľkého rozsahu. Môžeme hovoriť napr. o obchodných operáciách, rozhodnutiach jednotlivcov počas volieb, rozhodnutiach tých, ktorí praktizujú, ktorí formujú politiky a legislatívu, ktorí vykonávajú činnosť vo verejnom záujme, v štátnom záujme a podobne. Konanie aktéra môže byť úspešné aj v prípade, ak využije iba niektoré prvky hybridných hrozieb a preto je potrebné bezpochyby skúmať a sledovať aj počiatočné štádiá vplyvu hybridných hrozieb prostredníctvom ich aktérov, ktorí sú charakteristickí autoritárskymi a totalitnými názormi na moc. Ich cieľom je ovplyvniť systémové zraniteľné miesta demokracie za využitia všetkých nástrojov, ktoré má k dispozícii autoritársky štát. Demokratické štáty sa však môžu stretnúť aj s interferenciou operácií z iných demokratických štátov, ale v takýchto prípadoch je potrebné rozlišovať výrazné rozdiely medzi činnosťou demokratických a autoritárskych štátov.¹⁷

Štátni aktéri. Autoritárske štáty čoraz častejšie využívajú hybridné hrozby ako nástroj v boji proti demokratickým štátnym systémom, pretože ich vnímajú ako existenčnú hrozbu pre svoje mocenské postavenie. Toto vnímanie je jedným z dôvodov, prečo cítia potrebu pokúsiť sa podkopať a oslabiť schopnosti demokratických štátov. Manipulatívne zasahovanie do informačnej domény je jedným z ich hlavných aktív. Štátni aktéri sa v súčasnosti veľmi intenzívne snažia manipulovať konkrétny objekt ich záujmu aj prostredníctvom dezinformácií na sociálnych sieťach. Práve sociálne siete zvyšujú šance ovplyvniť objekt a naplniť cieľ aktéra. Svoje konanie aktéri smerujú v rámci ich pôsobenia na určité publikum i prostredníctvom mikrotargetingu. Mikrotargeting je plošné využitie individuálnych psychometrických informácií o veľkom množstve konkrétnych jedincov populácie v politickej alebo marketingovej kampani.¹⁸

¹⁷ Foreign interference in all democratic processes in the European Union, including disinformation. [online]. [cit. 2026. 02. 12.] Dostupné na internete: <https://osha.europa.eu/sk/tools-and-resources/eu-osha-thesaurus/term/62115d>.

¹⁸ JONGEPIER, F., WIELAND, J. W. Microtargeting people as a mere means 1. In: The Philosophy of Online Manipulation. Routledge, 2022, s. 160.

Na základe špecifického konania jednotlivých štátnych aktérov v rámci hybridného pôsobenia je možné členiť ich na revizionistických štátnych aktérov (revizionisti) a darebáckych štátnych aktérov (darebáci). Revizionistickí štátni aktéri sa objekt svojho záujmu snažia ovplyvniť tak, že ten je presvedčený o svojom konaní, považuje ho za správne a má za to, že je vykonávané z jeho vôle. Darebácki štátni aktéri sa už paranoidne odchyľujú od pravidiel reálnych politík, čo podľa bezpečnostných stratégií nemôže vyústiť v nič iné ako vo vojnový konflikt. Vyznačujú sa aj tým, že národné bohatstvo zneužívajú pre osobný prospech vodcov alebo pre megalomanské plány na získanie zbraní hromadného ničenia. Darebácki štátni aktéri využívajú hybridné hrozby na to, aby prispeli k rozpadu súčasného systému objektu a pretvorili ho na podobu fungovania svojho režimu. Tiež významnú úlohu v týchto prípadoch zohrávajú finančný zisk a vôľa uškodiť objektu v čo najväčšom rozsahu.¹⁹

Neštátni aktéri môžu byť pôvodcami hybridných hrozieb vo svojom vlastnom záujme s vlastnými strategickými cieľmi. Títo neštátni aktéri môžu byť zároveň „proxy“ aktérmi (zástupnými), ktorých využívajú štátni aktéri na naplnenie svojich strategických cieľov, na presadenie vlastných bezpečnostných, ekonomických či zahranično-politických záujmov bez priameho, otvoreného, angažovania sa v konflikte. Takýmto spôsobom štátni aktéri sťažujú svoju skutočnú atribúciu. „Proxy“ aktéri môžu byť motivovaní finančne, ideologicky a môže ísť aj napr. o záujmovú skupinu, hackerov, ale aj o jednotlivcov.

Nástroje a domény hybridných hrozieb - Aktéri hybridných hrozieb sa snažia svoje ciele dosiahnuť čo najefektívnejšie a najúčelnejšie. Na ich dosiahnutie, je potrebné, aby disponovali konkrétnymi a špecifickými nástrojmi, na základe ktorých dokážu profitovať zo svojej činnosti. Tieto nástroje môžu aktéri využívať naprieč viacerými doménami. V súčasnosti je vo všeobecnej rovine charakterizovaných približne 50 nástrojov hybridného pôsobenia a je veľký predpoklad, že tento počet sa bude neustále zvyšovať. Aktéri sa budú snažiť získať a využívať všetky dostupné možnosti, teda aj nástroje, k tomu, aby dosiahli svoj strategický cieľ čo najefektívnejším spôsobom.

¹⁹ CULLEN, P. et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 2021, s. 42. <http://www.doi.org/10.2760/44985>.

Vybranými nástrojmi hybridných hrozieb sú napr.: fyzické operácie proti infraštruktúre. Vytváranie a využívanie závislosti na infraštruktúre (vrátane civilno-vojenskej závislosti). Vytváranie alebo využívanie ekonomických závislostí. Priame zahraničné investície. Priemyselná špionáž. Narušanie národného hospodárstva protivníka. Ovpływňovanie volieb. Narušenie vzdušného priestoru. Zneužívanie migrácie. Ovpływňovanie a zasahovanie do médií. Práve používanie aj týchto nástrojov hybridných hrozieb môže slúžiť na dosiahnutie konkrétnych cieľov, bez toho, aby došlo k formálnemu vyhláseniu vojny.²⁰ Nie každý nástroj a nie každá činnosť, ktorá smeruje na konkrétnu doménu je hybridnou hrozbou a teda aj pre aktéra hybridnej hrozby nie sú všetky aktivity v rámci domény dôležité. Podstatné je si uvedomiť, že hybridná hrozba je vždy kombináciou konkrétnych nástrojov, ale nie všetky kombinácie nástrojov sú aj hybridnou hrozbou.²¹

Pri vedení hybridných konfliktov sú uplatňované nástroje z celého spektra spôsobov známych aj pod skratkou DIMEFIL - základné nástroje DIME [Diplomacy, Information, Military and Economics], v prostredí FIL [Financial, Intelligence and Law enforcement].

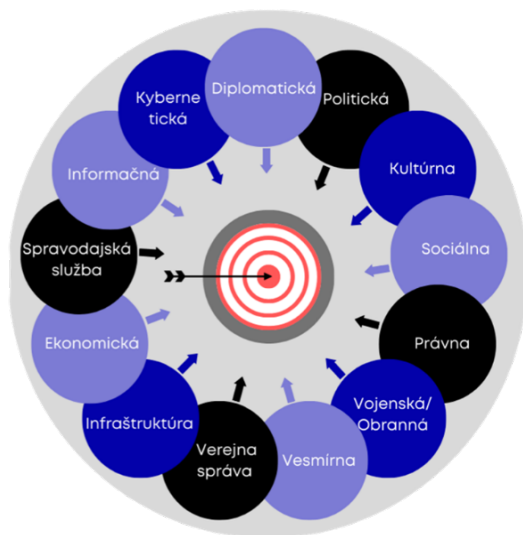
- D - Diplomacia/politika – uplatnenie vplyvu a vyvíjanie nátlaku ústami a činmi oficiálnej politickej reprezentácie.
- I) Informácie - médiá, sociálne siete a iné prostriedky šírenia informácií, ich manipulatívne využitie, dezinformačná kampaň a propaganda.
- M - Ozbrojené sily - môže ísť o otvorené použitie ako vyhrážka - demonštrácia vojenskej prítomnosti a pohotovosti, či priamo bojové použitie alebo o rôzne formy skrytého nasadenia jednotlivcov, malých skupín a infiltrácie napadnutého štátu s ich využitím.
- E - Ekonomika - rôzne formy nátlaku ekonomickej povahy - uvalenie cla, embarga, odopretie dodávok surovín či energie, zákaz používania dopravnej alebo prepravnej cesty, destabilizácia kľúčových odvetví, podnikov a podobne.
- F - Finančníctvo - destabilizácia meny, trhu s akciami a dlhopismi, bankového sektora, ovpływňovanie kľúčových finančných inštitúcií.

²⁰ CULLEN, P. et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 2021, s. 50. <http://www.doi.org/10.2760/44985>.

²¹ KORAUS, A., KRÁSNA, P., ŠIŠULÁK, S., VESELOVSKÁ, S. Integrated security strategies in the context of hybrid threats in the Slovak Republic. *Entrepreneurship and Sustainability Issues*, 11(1), 2023, s. 238. [http://doi.org/10.9770/jesi.2023.11.1\(14\)](http://doi.org/10.9770/jesi.2023.11.1(14)).

- I - Spravodajstvo - aktivity spravodajských služieb, špionáž, získavanie spolupracovníkov - najmä štátnych či politických činiteľov k protištátnej činnosti.
- L - Verejný poriadok a právny štát - využitie rôznych rozvrtných činností útočiacich na hodnotové, právne a ďalšie aspekty spoločenského usporiadania, napr. podnecovanie nepokojov v napadnutej krajine s využitím etnických, náboženských či sociálnych deliacich línií v spoločnosti, alebo použitie širokej škály teroristických útokov a ďalších typicky kriminálnych metód, napríklad - únosy, vydieranie a zastrašovanie.²²

Domény sú kľúčovými oblasťami národnej bezpečnosti a rozhodovacej schopnosti štátu. Podstatným dôvodom, prečo je tak dôležité identifikovať oblasti záujmu, resp. kritické oblasti, domény, na ktoré hybridné hrozby pôsobia je bezpodmienečná potreba zabezpečenia ich ochrany. Je žiadúce, aby štát zabezpečil ochranu domén pred aktivitami hybridných hrozieb. Konkrétne domény spolu veľmi úzko súvisia a tak ohrozenie jednej domény a prienik do jej štruktúry ovplyvňuje niekoľko ďalších domén, čím je narušená podstatná časť národnej bezpečnosti. Nie je preto účelné, aby sa koncept zabezpečenia ochrany zameral len na jednu doménu. Domény by sa nemali skúmať, vnímať, oddelene, ale v súvislostiach, pretože pôsobenie na jednu doménu môže vyvolať následný dopad na inú, ďalšiu, doménu.



²² FILIPEC, O. „Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats.” *Central European Journal of Politics* 8 (1): 1–18), 2021. https://doi.org/10.24132/cejop_2022_1.

Obrázok 2: Domény hybridných hrozieb.
Zdroj: Inštitút správnych a bezpečnostných analýz.

Názornú predstavu o vplyve jednotlivých nástrojov hybridných hrozieb na konkrétne domény prezentuje následná tabuľka, z ktorej je zrejmé, že jeden nástroj môže ovplyvňovať niekoľko domén súčasne.

Nástroje	Ovplyvnené domény
Fyzické operácie proti infraštruktúre	Infraštruktúra, ekonomická, kybernetická, vojenská/obranná, verejná správa
Vytváranie a využívanie závislosti na infraštruktúre (vrátane civilno-vojenskej závislosti)	Infraštruktúra, ekonomická, kybernetická, vojenská/obranná, verejná správa
Vytváranie alebo využívanie ekonomických závislostí	Ekonomická, diplomatická, politická, verejná správa
Priame zahraničné investície	Ekonomická, infraštruktúra, kybernetická, vojenská/obranná, verejná správa, politická
Priemyselná špionáž	Ekonomická, infraštruktúra, kybernetická, informačná
Kybernetická špionáž	Infraštruktúra, kybernetická, vojenská/obranná, verejná správa

Obrázok 1: Koncept hybridných hrozieb.
Zdroj: vlastné spracovania na základe odbornej literatúry.

Fázy (typy činností pozorované v každej fáze) - Príprava. Vo fáze prípravy je konečným cieľom aktéra hybridnej hrozby, že objekt dobrovoľne učiní škodlivé rozhodnutie a bude konať nesprávne, avšak bude konať v prospech aktéra. Podstatou tejto fázy je skutočnosť, aby si aktér zabezpečil také prostredie, ktoré mu efektívne napomôže pri naplňaní svojho strategického cieľa. Vo fáze prípravy sú aktivity aktéra veľmi ťažko detekovateľné, nie je jasný ich zámer. Cieľom týchto aktivít je prinútiť objekt,

štát (terč hybridného pôsobenia), aby začal robiť škodlivé rozhodnutia v súlade so záujmami aktéra.

Destabilizácia. Fáza destabilizácie je štádiom, v ktorom aktér zintenzívňuje svoju činnosť a agresivitu, napr. spôsobom kampane (realizácia viacerých operácií). Cieľom aktéra v rámci tejto fázy je získať čo najviac informácií, aby mohol svoj cieľ čo najefektívnejšie ohroziť. V tomto štádiu sú aktivity aktéra čoraz viditeľnejšie, avšak k ich vykonávaniu sa nepriznáva a cieľový štát nemá dostatok dôkazov na to, aby to dôveryhodne preukázal. Pohnútkou aktéra môže byť vedomý predpoklad alebo len výhodná príležitosť na výraznejšiu zmenu aktuálneho stavu, ktorá je v súlade s jeho strategickým záujmom. Prechod do fázy destabilizácie v informačnej doméne môže signalizovať, napr. zvýšenie tempa informačných operácií na podporu určitého naratívu protivníka, zvýšenie objemu šírených dezinformácií, zapojenie nástrojov automatizovaného šírenia dezinformácií alebo kybernetický útok na verejnoprávne informačné kanály. Destabilizačná fáza môže prejsť do fázy donucovania, ale aj deeskalovať späť do fázy prípravy, predovšetkým ak sa protivníkovi podarí naplniť jeho ciele.²³

Nátlak. Hybridná vojna. V tejto fáze už prekračujú aktivity aktéra rámec nenápadnosti a možno ju označiť za hybridnú vojnu. Hybridná vojna predstavuje vrchol eskalačného spektra činností hybridných hrozieb. Hybridná vojna je v zásade kombináciou skrytých a otvorených vojenských operácií v kombinácii s politickými a ekonomickými opatreniami, rozvratom, informačnými, dezinformačnými operáciami, propagandou a falošnými správami. Kľúčovým prvkom je použitie sily na dosiahnutie aktérovho zámeru, napr. prostredníctvom teroru, sabotáže, či konvenčnej vojny.

Jednotlivé fázy môžu opätovne eskalovať aj deeskalovať, a to so zámerom náročnejšej identifikácie aktéra a jeho zámeru.

STRATEGICKÁ KOMUNIKÁCIA AKO EFEKTÍVNY PRVOK BUDOVANIA ODOLNOSTI VOČI HYBRIDNÝM HROZBÁM

Efektívne riešenie hybridných hrozieb a budovanie odolnosti Slovenskej republiky voči hybridným hrozbám vyžaduje spoločné porozumenie medzi odborníkmi z aplikačnej praxe, vedcami, tvorcami politik a politikmi. Kľúčové sú tiež včasná identifikácia činnosti hybridnej hrozby,

²³ NBÚ. [online]. [cit. 2026. 03. 12.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>.

identifikácia medzier v prevencii, medzier v pripravenosti a v konkrétnych reakciách. V súvislosti s uvádzaným je prioritné identifikovať konkrétne oblasti a činnosti možného ohrozenia. Po zrejmej identifikácii je potrebné následne prostredníctvom efektívnych nástrojov vypracovať správne opatrenia na podporu odolnosti, tak ako na národnej tak aj na medzinárodnej úrovni. Jedným z efektívnych prvkov budovania odolnosti Slovenskej republiky voči hybridným hrozbám je s určitosťou aj strategická komunikácia. Implementácia princípov strategickej komunikácie štátnymi inštitúciami je rovnako jedným z kľúčových predpokladov efektívnej reakcie štátu na hybridné pôsobenie.

Organizované a cieľavedomé šírenie dezinformácií je jedným z hlavných nástrojov využívaných v rámci hybridných operácií. Vhodnou obranou a prevenciou pred pôsobením takýchto podvrtných informačných operácií je práve strategická komunikácia. Strategická komunikácia prináša ucelenosť komunikovaného obsahu, snaží sa nasmerovať cieľové publikum k dlhodobej zmene v zmýšľaní, prezentovať dlhodobé vízie a základné hodnoty spoločnosti.

Strategická komunikácia je jedným z kľúčových nástrojov pri budovaní bezpečnejšej krajiny, odolnejšej spoločnosti, ktorá je pripravená čeliť novodobým výzvam a krízam. Budovanie bezpečnejšej krajiny je realizované aj prostredníctvom systematickej, koordinovanej kooperácie ministerstiev, Úradu vlády Slovenskej republiky a ostatných ústredných orgánov štátnej správy. Pre potreby zadefinovania strategickej komunikácie, ktorá je prispôbená podmienkam a potrebám Slovenskej republiky je použitá definícia strategickej komunikácie z Terminologického slovníka krízového riadenia a Koncepcie strategickej komunikácie Slovenskej republiky vydané v roku 2023. Táto koncepcia vychádza i z poznatkov Komunikačnej agentúry Spojeného kráľovstva (Government Communication Service).²⁴ Spojené kráľovstvo je totiž dlhodobo svetovým lídrom v oblasti strategickej komunikácie.

Strategická komunikácia je systematická koordinovaná aktivita štátu, ktorá je zameraná na informovanie verejnosti a ostatných relevantných subjektov prostredníctvom využívania objektívnych informácií a dostupných zdrojov na dosiahnutie vopred stanovených cieľov. Je nástrojom verejných politik štátu a nemôže byť zamieňaná s politickou komunikáciou či politickým

²⁴ Government Communication Service. [online]. [cit. 2026. 02. 08.] Dostupné na internete: <https://ges.civilservice.gov.uk/>.

marketingom. Štátne inštitúcie a ich zamestnanci, ktorí pôsobia ako komunikátori v súvislosti s vykonávaním štátnej služby, postupujú podľa zásad a princípov Etického kódexu štátneho zamestnanca.²⁵ O etickom kódexe môžeme hovoriť ako o súhrne pravidiel správania sa v spoločnosti, v organizácii.²⁶ Strategická komunikácia pozostáva z komunikačných kampaní založených na vopred stanovených mýľníkoch podložených kvantitatívnym alebo kvalitatívnym výskumom a reflektuje dlhodobé strategické záujmy štátu. Výhody strategickej komunikácie spočívajú v zlepšenej schopnosti štátu brániť sa voči dezinformačným kampaniam, v intenzívnejšej spolupráci a komunikácii s občanmi ako s dôležitými partnermi, čo prispieva k posilneniu dôvery verejnosti v demokratický a právny štát. Dôležité je uvedomiť si, že efektívna strategická komunikácia nepozostáva len z verbálnych prejavov, opiera sa aj o činy, gestá a symboly. Reflektuje aktuálne potreby občanov a využíva široké zapojenie všetkých relevantných subjektov do celospoločenského prístupu k informačnej bezpečnosti.²⁷

Strategická komunikácia ministerstiev a ostatných subjektov štátnej správy, ktoré pracujú v prospech zvrchovanej, bezpečnej, prosperujúcej a demokratickej Slovenskej republiky je založená na nasledujúcich princípoch:

- Verejný záujem.
- Strategická komunikácia ako súčasť tvorby politík.
- Celospoločenský prístup.
- Kredibilita.
- Znalosť publika.
- Informačné prostriedky.
- Plánovanie.
- Koordinácia.
- Inklúzia.

²⁵ Rada pre štátnu službu. [online]. [cit. 2026. 03. 08.] Dostupné na internete: <https://radaprestatnuszsluzbu.vlada.gov.sk/eticky-kodex-statneho-zamestnanca/>.

²⁶ KOVÁČ, E. Etický kódex mediátora a sociálna práca. In Aplikovaná etika v sociálne práci a ďalších pomáhajúcich profesiách. Zborník z medzinárodnej vedeckej konferencie. Bratislava: Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, 2010, s. 153.

²⁷ Koncepcia strategickej komunikácie Slovenskej republiky. 2023. [online]. [cit. 2026.03.11.]. Dostupné na internete: https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrc=2433846761948488913.

- Merateľné výsledky.²⁸

Strategická komunikácia si vyžaduje dlhodobé komunikačné plánovanie a rôzne formy prístupu ku komunikácii, prostredníctvom ktorých sa systematicky budujú a rozvíjajú príbehy, naratívy a posolstvá vo vopred stanovených prioritných témach a oblastiach. Tieto priority môžu mať rôzne úrovne - celoštátnu, inštitucionálnu alebo sa môžu odvíjať od potrieb cieľovej skupiny.

ZÁVER

Tradičnými, konvenčnými, formálnymi metódami a nástrojmi, ale aj s použitím moderných technológií, sa v súčasnosti rad štátnych, štátni sponzorovaných ale aj neštátnych aktérov otvoreným alebo skrytým spôsobom snaží dosiahnuť svoje politické, ale aj ekonomické ciele. Realizujú to koordinovane naprieč celou škálou nástrojov moci. Zvyšuje sa relevancia hrozieb schopných vyvolať významné ekonomické straty z dôvodu prerušenia, poškodenia fungovania základných funkcií štátu alebo služieb, ktoré sú potrebné na jeho bežné fungovanie, ale aj bežný chod spoločnosti ako takej. Zvyšuje sa aj pripravenosť a schopnosti rôznych aktérov presadzovať svoje záujmy na úkor iných. Tento vývoj je daný meniacim sa charakterom moci a vplyvu, keď vzájomné závislosti, technológie a ich prepojenia dávajú štátom nové možnosti ovplyvňovať svojich konkurentov, všetko bez ohľadu na medzinárodné pravidlá alebo národné zákony. Do úvahy je však v tomto prípade potrebné brať aj historické súvislosti, ako aj súčasný stav práva, poznatky teórie, potreby aplikačnej praxe, vnútroštátne právne špecifiká i medzinárodnoprávne aspekty s prihliadnutím na potrebu vysokej garancie ochrany základných práv a slobôd.²⁹

Hybridné hrozby samy o sebe nepredstavujú v histórii nič nové. Za nówum je však potrebné považovať rozsah a spôsob, ako je škála nástrojov hybridných hrozieb kombinovaná a koherentne/vzájomne použitá na

²⁸ BEZPEČNOSTNÁ RADA SLOVENSKEJ REPUBLIKY. Terminologický slovník krízového riadenia a zásady jeho používania. [online]. [cit. 2023. 09. 08.] Dostupné na internete: <https://www.reserves.gov.sk/wp-content/uploads/2019/10/Terminologick%C3%BD-slovn%C3%ADk-kr%C3%ADzov%C3%A9ho-riadenia.pdf>.

²⁹ ČENTĚŠ, J., ŠANTA, J. Qualitative aspects of Criminal Code of the Slovak Republic and reasons for its amendment. In: Studia Prawnoustrojowe [print]: Journal of the Faculty of Law and Administration at UWM in Olsztyn, č. 41, s. 82. p. 79-96. ISSN 1644-0412. <https://www.cecol.com/search/article-detail?id=786268>.

dosiahnutie strategického cieľa. Jednotlivé prvky hybridnej kampane nemusia byť nutne nezákonné či predstavovať hrozbu samy o sebe. Nebezpečenstvo spočíva práve v ich sofistikovanej kombinácii, ktorá sa súčasne usiluje o zastretie pravého účelu ich jednotlivých cieľov. Hybridné stratégie sú založené na vysokej adaptabilite a aktéri útokov prispôsobujú výber použitých prostriedkov slabým miestam konkrétného cieľového štátu. Hlavnú zodpovednosť za identifikáciu týchto slabých miest, domén, ktoré by aktér hybridných hrozieb mohol využiť, nesie konkrétny štát. Hybridné konflikty slúžia na zvýšenie nejednoznačnosti, komplikujú rozhodovanie a spomaľujú koordináciu efektívnych činností v rámci obrany a ochrany štátu. Charakteristika a vymedzenie hybridných hrozieb nie je univerzálne, pretože ich progres, ktorý existuje na národnej a medzinárodnej úrovni sa neustále mení. Je veľmi dôležité vždy dbať na všetky aktuálne okolnosti, ktoré ohrozujú bezpečnosť štátu a teda aj na hybridné hrozby. Z tohto dôvodu je preto potrebné efektívne budovať povedomie o hybridných hrozbách, ale aj systém prvkov zabezpečujúcich odolnosť voči hybridným hrozbám.

V závere tiež považujeme za opodstatnené uviesť niekoľko otázok, ktoré sumarizujú a zároveň odpoveď na nich je kľúčová pri chápaní podstaty a významu hybridných hrozieb, ktorú sme zhrnuli aj v rámci predloženej vedeckej štúdie. „Ako sú definované 4 piliere ktoré je potrebné poznať pre pochopenie konceptu hybridných hrozieb?, Čo je to strategická komunikácia?, Je v rámci Vášho pôsobenia venovaná dostatočná pozornosť problematike hybridných hrozieb?, Ako je možné zefektívniť boj proti hybridným hrozbám?“

ZOZNAM POUŽITEJ LITERATÚRY

AVEN, T. A risk and safety science perspective on the precautionary principle. Safety Science, Volume 165, 2023, ISSN 0925-7535, <https://doi.org/10.1016/j.ssci.2023.106211>.

BEZPEČNOSTNÁ RADA SLOVENSKEJ REPUBLIKY. Terminologický slovník krízového riadenia a zásady jeho používania. [online]. [cit. 2023. 09. 08.] Dostupné na internete: <https://www.reserves.gov.sk/wp-content/uploads/2019/10/Terminologick%C3%BD-slovn%C3%ADk-kr%C3%ADzov%C3%A9ho-riadenia.pdf>.

Bezpečnostná stratégia 2021. [online]. [cit. 2025. 12. 08.] Dostupné na internete: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

BUZALKA, J. BLAŽEK, V. Metodológia a metodika vypracovania analýzy vnútorného ohrozenia bezpečnosti SR a z nej vyplývajúcich ohrození a rizík. In Metodológia a metodika analýzy zdrojov ohrozenia vnútornej bezpečnosti SR. Bratislava: Akadémia PZ - K krízového manažmentu vo verejnej správe, 2011, s. 16 - 39. ISBN 978-80-8054-517-8.

CULLEN, P. et al. The landscape of Hybrid Threats: A Conceptual Model (Public Version), 2021, 58 s. <http://www.doi.org/10.2760/44985>.

ČENTÉŠ, J., ŠANTA, J. Qualitative aspects of Criminal Code of the Slovak Republic and reasons for its amendment. In: Studia Prawnoustrojowe [print]: Journal of the Faculty of Law and Administration at UWM in Olsztyn, č. 41, s. 79-96. ISSN 1644-0412.

ENGELHARD, I., M., UIJEN, S. L., SETERS, N., VELU, N. The Effects of Safety Behavior Directed Towards a Safety Cue on Perceptions of Threat. <https://doi.org/10.1016/j.beth.2014.12.006>.

EU-OSHA. [online]. [cit. 2026. 01. 15.] Dostupné na internete: <https://osha.europa.eu/sk/tools-and-resources/eu-osha-thesaurus/term/62115d>.

FILIPEC, O. „Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats.” Central European Journal of Politics 8 (1): 1–18), 2021. https://doi.org/10.24132/cejop_2022_1.

Foreign interference in all democratic processes in the European Union, including disinformation. [online]. [cit. 2026. 02. 12.] Dostupné na internete: <https://osha.europa.eu/sk/tools-and-resources/eu-osha-thesaurus/term/62115d>.

GLÄNZEL, W., THIJS, B. Using hybrid methods and ‘core documents’ for the representation of clusters and topics: the astronomy dataset. Scientometrics 111, 1071–1087, 2017. <https://doi.org/10.1007/s11192-017-2301-6>.

Government Communication Service. [online]. [cit. 2026. 02. 08.] Dostupné na internete: <https://gcs.civilservice.gov.uk/>.

JONGEPIER, F., WIELAND, J. W. Microtargeting people as a mere means 1. In: The Philosophy of Online Manipulation. Routledge, 2022, s. 156 -179.

KAČMÁR, R. ZaBEZPEČ si vedomosti: Čo je to bezpečnosť? SLOVENSKÝ INŠTITÚT PRE BEZPEČNOSTNÚ POLITIKU, 2016, s. 2.

Koncepcia pre boj slovenskej republiky proti hybridným hrozbám. [online]. [cit.2023.09.06.]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf>.

Koncepcia strategickej komunikácie Slovenskej republiky. 2023. [online]. [cit.2026.03.11.]. Dostupné na internete: https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=2433846761948488913.

KORAUS, A., KRÁSNÁ, P., ŠIŠULÁK, S., VESELOVSKÁ, S. Integrated security strategies in the context of hybrid threats in the Slovak Republic. Entrepreneurship and Sustainability Issues, 11(1), 2023, s. 233-250. [http://doi.org/10.9770/jesi.2023.11.1\(14\)](http://doi.org/10.9770/jesi.2023.11.1(14)).

KOVÁČ, E. Etický kódex mediátora a sociálna práca. In Aplikovaná etika v sociálne práci a ďalších pomáhajúcich profesiách. Zborník z medzinárodnej vedeckej konferencie. Bratislava: Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, 2010, s. 152-157. ISBN 978-80-89271-89-4.

MASCHMEYER, L. A new and better quiet option? Strategies of subversion and cyber conflict. Journal of Strategic Studies. <https://doi.org/10.1080/01402390.2022.2104253>.

NBÚ. [online]. [cit. 2026. 03. 12.] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovník-hybridnych-hrozieb/index.html>.

POSEN, B. R. Inadvertent escalation: Conventional war and nuclear risks. Cornell University Press, 2014, s. 51. 321 s. ISBN 978-0-8014-2563-9.

Rada pre štátnu službu. [online]. [cit. 2026. 03. 08.] Dostupné na internete: <https://radaprestatnuszluozbu.vlada.gov.sk/eticky-kodex-statneho-zamestnanca/>.

VEJMELKA, O. a kol. Vojenský výkladový slovník vybraných operačních pojmu. Správa doktrín Ředitelství výcviku a doktrín, Vyškov, 2005, s. 41-46.

VOLNER, Š. BEZPEČNOST, RIZIKÁ A HROZBY 21. STOROČIA. In Univerzita Obrany. Ustav Strategických Studií. Obrana a Strategie; Brno Vol. 2005, Iss. 2, s. 71-86. doi:10.3849/1802-7199. ISSN 1802-7199.

VRTÍKOVÁ, K., MOKRÁ, I. Spolupracujúci obvinený v trestnom konaní v intenciách aplikačnej praxe a úvahy de lege ferenda. Praha: Leges, 2023, 188 s. ISBN 978-80-7502-639-4.