Monika Hullová

Indikátory hybridných hrozieb – nástroj ich identifikácie a eliminácie

Anotácia: Autorka sa v predkladanej vedeckej štúdii venuje metodologickým, metodickým a praktickým aspektom identifikácie hybridných hrozieb. V prvej časti príspevku vymedzuje hybridné hrozby ako objekt identifikácie. Využíva metódu obsahovej analýzy dokumentov, kauzálnu, komparatívnu a historickú analýzu. V druhej časti sa zameriava na analýzu procesu identifikácie hybridných hrozieb prostredníctvom ich indikátorov. Indikátory ako určité signály, symptómy alebo prvotné poznatky o konaní alebo jave majú v sebe potenciál eliminovať, resp. minimalizovať riziká plynúce z hybridných hrozieb. Autorka poznáva, skúma a hodnotí prácu s indikátormi využitím analyticko-syntetickej metódy, metódy modelovania a projektovania.

Kľúčové slová: hybridná hrozba, hybridná vojna, klasická (totálna) vojna, hybridný konflikt, riziko, hrozba, bezpečnostná situácia, identifikácia, interpretácia, indikátor, analýza, analytická činnosť

Úvod

Hybridné hrozby nie sú novodobým fenoménom napriek tomu, že vystupujú do popredia hlavne v poslednej dekáde, v kontexte aktuálneho vývoja globálnej bezpečnostnej situácie. Zastávame názor, že hybridné hrozby ako potenciálne aj reálne bezpečnostné riziká opodstatnene vyžadujú záujem kompetentných subjektov vrátane odbornej verejnosti. Cieľom týchto koordinovaných aktivít je prehĺbenie a zefektívnenie procesov ich identifikácie a eliminácie, prípadne minimalizácie škodlivých následkov. V týchto intenciách budeme pod identifikáciou rozumieť *„... špecifický proces poznávania objektov (identifikovaných a identifikujúcich). Umožňuje identifikujúcim subjektom definovať na identifikovanom objekte systémový model vlastnosťami, ktoré charakterizujú jeho správanie. Základným predpokladom naplnenia týchto zámerov a cieľov je dosiahnutie takej úrovne a hĺbky poznania o objekte, aby ho bolo možné systémovo modelovať."*[1] Našou ambíciou v predkladanej vedeckej štúdii je poznávať, skúmať, analyzovať, hodnotiť, vysvetľovať a projektovať model identifikácie hybridných hrozieb prostredníctvom indikátorov ako súčasť širšej vedeckej stratégie. [2]

1 Hybridné hrozby – objekt identifikácie

V rámci bezpečnostnej komunity neexistuje univerzálna definícia hybridných hrozieb, ktorá by komplexne pokrývala zložitosť tohto problému vo všetkých reálne existujúcich významových rovinách. V intenciách riešenej tematiky je potrebné uviesť, že definície hybridných hrozieb sa, aj vzhľadom na ich premenlivý a heterogénny charakter rôznia, v každom prípade sú založené na spoločnom významovom základe.

F. G. Hoffman vo svojej štúdii *(2001)* konštatuje, že *„... hybridné hrozby inkorporujú konvenčné schopnosti, iregulárne taktiky a formácie, teroristické útoky zahŕňajúce bezhlavé násilie, nátlak a kriminálne nepokoje. Hybridné vojny môžu byť páchané na jednej strane štátom a na druhej strane aj neštátnymi aktérmi. Tieto multimodálne aktivity môžu byť realizované separátnymi jednotkami alebo dokonca tou istou jednotkou, ale vo všeobecnosti sú*

[1] LISOŇ, M., 2012. *Teória operatívneho policajného poznania*, s. 22.

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

operačne a takticky riadené a koordinované z hlavného bojového priestoru, s cieľom dosiahnuť synergické efekty prejavujúce sa v hmotnej a psychologickej dimenzii konfliktu.“[3]

Nový Bi-strategický Capstone NATO koncept boja proti hybridným hrozbám z roku 2010 vymedzuje hybridné hrozby ako aktivity *„zo strany protivníka, so schopnosťou simultánne a adaptabilne využívať konvenčné a nekonvenčné prostriedky pri sledovaní svojich cieľov... Sú charakteristické úzkym prepojením jednotlivcov a skupín, ktoré hľadajú viac príležitostí pre spoluprácu (pre bezpečnostné prostredie sú typické neočakávané spojenectvá na nejasne definovanej taktickej, operatívnej a strategickej úrovni medzi jednotlivými aktérmi), často využívajú dezinformáciu v médiách pre dosiahnutie strategických efektov (za využitia informačných systémov a sietí), ako aj diverzifikované prostriedky a spôsoby (predstavujú fúziu smrtiacich a nesmrtiacich nástrojov, vrátane konvenčných zbraní, chemických, biologických, rádiologických a nukleárnych materiálov, terorizmu, špionáže, kybernetických útokov a kriminality, opierajúcu sa o podvratné informačné operácie a legitímne obchodné organizácie) a v neposlednom rade zneužívajú všeobecne uznávané pravidlá a zákony (účelovo interpretujú medzinárodné právo a reštriktívne opatrenia).“*[4]

Podľa Koncepcie pre boj Slovenskej republiky proti hybridným hrozbám *(2018)* je hybridnú hrozbu možné chápať ako: *„súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Sú realizované aktivitami charakterizovanými centrálne riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené.“*[5]

Podľa terminologického slovníka NATO *(2021)* ide o *„druh hrozby, ktorá kombinuje konvenčné, nepravidelné a asymetrické aktivity v čase a priestore“*.[6]

Z prezentovaných vymedzení hybridnej hrozby je zrejmé, že sa vyznačuje nasledovnými charakteristikami:

- ✓ *Aktér (subjekt pôsobenia):* Realizátorom týchto aktivít sú heterogénne subjekty *(štátne aj neštátne, militantné aj nemilitantné)*.
- ✓ *Referenčný objekt pôsobenia:* Objekt pôsobenia má heterogénny charakter, v tom najširšom zmysle slova ide o spoločnosť, štát, viaceré štáty, nadnárodné štátno-mocenské zoskupenie.

---

[3] HOFFMAN, F. G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars.* [online]. [2023-1-19]. Dostupné na internete: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, s. 8.

[4] NATO, 2010. Bi-SC *Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

[5] NBÚ, 2018. Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám. [online]. [2023-1-19]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

[6] *NATO Glossary of Terms and Definitions (English and French): AAP-06*: Edition 2021., s. 65 [online]. [cit. 2023-1-19]. Dostupné na internete: https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600,

- ✓ *Spôsob realizácie:* Ide o cieľavedomú, účelovú, systémovú, spravidla skrytú kombináciu konvenčných a nekonvenčných, vojenských a nevojenských aktivít, metód a foriem *(napr. diplomatických, vojenských, ekonomických a technologických)*.
- ✓ *Cieľ aktivít:* Cieľom týchto aktivít je minimalizovať obete a materiálne škody *(okrem iného z dôvodu potreby šetrenia síl a prostriedkov na potenciálny neskorší konvenčný spôsob vedenia vojny)*, zneužívať zraniteľnosť objektu, vytvárať neprehľadné situácie, narušovať rozhodovacie procesy, manipulovať verejnú mienku, destabilizovať a polarizovať spoločnosť, narušovať legitimitu, dôveryhodnosť, akcieschopnosť štátu, a v konečnom dôsledku tak ohrozovať demokraciu, ústavnosť, celistvosť a obranyschopnosť štátu prípadne nadštátneho celku *(okrem iného s cieľom vytvárať podmienky pre potenciálne neskoršie použitie konvenčnej vojenskej sily)*.

Hybridné hrozby predstavujú *„reálne bezpečnostné riziká“*[7] pre štáty, skupiny štátov, medzinárodné spoločenstvá, sú druhom intolerancie, skrytého boja určitých záujmových či spoločenských zoskupení *(vrátane štátno-mocenských celkov)*, frekventovane využívajúc nové *(napr. informačné)* technológie a formy ovplyvňovania názorov, postojov, či verejnej mienky, založené najmä na manipulácii, dezinformácii a propagande. Ich riziko tkvie v tom, že oproti konvenčným formám vedenia vojny, súčasťou ktorých je inváziа, otvorená manifestácia použitia vojenskej sily a techniky voči inému, realizácia vojenských *(bojových)* operácií na súši, vo vzduchu a na mori *(či v mori)*, pri hybridných hrozbách dominujú úplne odlišné, na prvý pohľad skryté, avšak z kvalitatívneho hľadiska – sofistikované metódy a formy, ktoré majú širokospektrálne simultánne efekty. V oboch prípadoch však možno hovoriť o deštruktívnych aktivitách namierených voči *(vojenskému)* nepriateľovi za účelom jeho paralýzy a následnej eliminácie. Napriek tomu, že dezinformačné kampane sa na prvý pohľad javia ako neškodné, opak je pravdou. Podkopávajú spoločnosť a dôveru občanov v štát a demokraciu, podporujú nepokoje, propagujú extrémizmus a násilie, využívajú negatívne javy v spoločnosti za účelom vytvárania chaosu a destabilizácie systému. Agresívnejšou alternatívou novodobej *„informačnej vojny“* sú kybernetické *(hackerské)* útoky, ktorých cieľom je narúšať hospodárstvo a verejný či štátny sektor. Do sféry prejavov hybridných hrozieb možno zaradiť aj interferenčné snahy o zmenu politického režimu, politickej situácie, či politickej scény, prostredníctvom podpory a propagácie určitých politických strán a hnutí, využívania strategickej korupcie, ovplyvňovania volebných procesov cudzou mocou, politického nátlaku a diskreditácie namierených na najvyšších štátnych predstaviteľov a štátne inštitúcie, vytvárania politického a ekonomického tlaku, ekonomickej a sociálnej manipulácie *(vrátane ekonomických sankcií či ekonomickej blokády, ale aj ovplyvňovania etnických, náboženských a kultúrnych menšín)*, zneužívania krízovej situácie *(napr. vojnového stavu, utečeneckej krízy, energetickej krízy, pandemickej situácie)*, príp. negatívnych javov v spoločnosti *(napr. negatívny vývoj kriminálnej scény)* na presadzovanie svojich parciálnych cieľov. Súčasťou tejto širšej vojenskej *(bojovej)* stratégie, okrem zmienených nenásilných foriem, môže byť hrozba použitia vojenskej sily, výzvedné a podvratné aktivity tajných služieb, ale aj podporovanie

[7] *„Hrozby“* a *„riziká“* sú súčasťou bezpečnostnej reality a patria do bezpečnostnej terminológie, hoci sa často zamieňajú. Oba pojmy sa týkajú chránených hodnôt, chránených záujmov, ktoré sú predmetom ochrany, napr. ústavnou alebo zákonnou cestou. Hodnoty sú však zraniteľné. Hrozby sú takými stavmi alebo aktivitami, ktoré chránenú hodnotu môžu poškodiť alebo zničiť. Hrozba je vždy primárna, nezávisle existujúca, neodvodený fenomén, ktorý chce alebo môže poškodiť nejakú chránenú hodnotu. Je to vonkajší fenomén *(činiteľ)*, existuje nezávisle na chcení človeka. Závažnosť hrozby je *(priamo)* úmerná povahe chránenej hodnoty a tomu, ako je táto hodnota cenená. Rozlišujeme neintencionálne hrozby *(napr. prírodné katastrofy)* a intencionálne hrozby *(napr. hrozba teroristickej akcie)*. Riziko predstavuje nebezpečenstvo neúspechu, nezdaru alebo straty. Riziko je vždy odvodené a odvoditeľné z konkrétnej hrozby. Mieru rizika, teda pravdepodobnosť škodlivých následkov vyplývajúcich z hrozby a zo zraniteľnosti záujmov, je možné posúdiť na základe analýzy rizík. Riziko je vyjadrením pravdepodobnosti vzniku hrozby. In JANOŠEC, J., 2010. *Hrozba a riziko v bezpečnostní terminologii, s. 8-9.*

militantných a semimilitantných skupín *(napr. prostredníctvom materiálnych a finančných dotácií)*, vojenská pomoc *(personálna, technická aj taktická)* a ich propagácia *(napr. prejavovanie sympatií, schvaľovanie a ospravedlňovanie ich konania a správania)*. V extrémnych prípadoch sa tu stretávame aj s aktmi násilnej povahy *(politické vraždy na objednávku, atentáty na ústredných predstaviteľov spoločnosti a štátu, teroristické útoky, sabotáže namierené na kľúčovú infraštruktúru a pod.)*.

Z tohto neukončeného výpočtu negatívnych prejavov *(metód a foriem)* hybridných hrozieb je zrejmé, že konvenčný vojnový konflikt má podstatne vyššie náklady a aj preto sa určité subjekty spoliehajú na nevojenské prostriedky bez formálneho vyhlásenia vojny.

Aj napriek tomu, že pojem hybridné hrozby ako koordinovaná kombinácia rôznych druhov pôsobenia na účel dosiahnutia strategických, politických a geopolitických cieľov sa začal používať pomerne nedávno, uvedený prístup je vo vojenstve známy už stáročia. Napr. čínsky vojenský stratég Sun Tzu (*„majster Slnka“)* vo svojej knihe *„Umenie vojny“* z približne 6. stor. pred Kristom, ktorá je rozčlenená do 13 kapitol, pojednáva o kľúčových formách vojenskej stratégie a taktiky. Toto nadčasové filozofické dielo ovplyvnilo nielen východný a západný spôsob vojenského myslenia, ale stalo sa inšpiráciou v oblasti politiky, manažmentu, leaderstva, športu, či životného štýlu.[8]

Koncept hybridného vojenstva, hybridnej vojny, nie je skutočne ojedinelým prístupom, ale rezonuje aj v dielach iných autorov, napr. východných vojenských stratégov *(Liang-a, Xiangsui-a, Mao ce Tung-a)*, ruských stratégov *(Dugina, Panarina, Chekinova, Bogdanova, Gerasimova)* či západných stratégov *(Hoffmana, Walkera, Simsona, Williamsona, Mansoora, Fridmana)* atď.[9] Podľa niektorých bezpečnostných analytikov praktická akceptácia týchto konceptov bola výrazne determinovaná konfliktom medzi Hizballáhom a Izraelom v Libanonu *(2006)*, Rusko-gruzínskym stretom *(2008)*, anexiou Ruskej federácie na Ukrajine *(2014)*.[10]

Z prezentovaného je zrejmé, že pri snahách o pojmové vymedzenie tohto negatívneho javu je potrebné rozlišovať medzi hybridnou hrozbou, hybridným konfliktom, hybridnou vojnou, aj keď na prvý pohľad je zrejmá ich súvzťažnosť, okrem iného determinovaná použitím adjektíva *„hybridný, hybridná“*.[11]

„Hybridná hrozba“ je jav, ktorý je výsledkom konvergencie a vzájomného prepojenia rôznych elementov *(faktorov)* vytvárajúcich komplexnú a multidimenzionálnu hrozbu. Hybridný konflikt a hybridná vojna sú dve špecifické kategórie, ktoré slúžia štátu na to, aby prostredníctvom niektorých foriem hybridnej taktiky dosiahol strategické ciele.

„Hybridný konflikt“ je situácia, keď sa účastnícke strany konfliktu vyhýbajú otvorenému použitiu vojenskej sily, namiesto toho uprednostňujú kombináciu vojenského zastrašovania, zneužívania ekonomickej a politickej zraniteľnosti, diplomatických alebo technologických prostriedkov sledujúc pritom dosiahnutie svojich cieľov.

---

[8] Wikipedia. *Sun-c’,* 2022. [online]. [cit. 2023-1-19]. Dostupné na internete: https://sk.wikipedia.org/wiki/Sun-c%E2%80%99.

[9] HAVLÍK, M., 2021. *Koncepty hybridního válčení a Armáda ČR*. In *Vojenské rozhledy.* [online]. 2021, č. 30 (1). 038-051. ISSN 1210-3292 (print), 2336-2995 (online). [cit. 2023-1-19]. Dostupné na internete: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/koncepty-hybridniho-valceni.

[10] KŘÍŽ, Z. – SHEVCHUK, Z. – ŠTEVKOV, P., 2016. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. [online]. [cit. 2023-1-19]. Dostupné na internete: http://data.idnes.cz/soubory/na_knihovna/A161212_M02_021_HH16_PP-V1.PDF.

[11] Podľa slovníka cudzích slov prívlastok *„hybridný“* značí krížený, vytvorený krížením, zmiešaním, spojením rôznorodých zložiek do jedného celku. Ide o pojem, ktorý sa používa v botanike, chémii, geológii, lingvistike atď. a v prenesenom význame symbolizuje kombinovaný, zmiešaný charakter. In Slovník cudzích slov. [online]. [cit. 2023-1-19]. Dostupné na internete: http://slovnikcudzichslov.sk/slovo/hybrid.

„Hybridná vojna“ je situácia, v ktorej krajina používa otvorenú vojenskú silu voči inej krajine v kombinácii s inými prostriedkami vedenia vojny *(napr. ekonomickými, politickými, diplomatickými).* [12]

„Vojna“ v duchu Clausewitzovej[13] teórie je chápaná ako pokračovanie politiky štátu násilnými prostriedkami, ktoré sú použité k donúteniu protivníka vykonať našu vôľu. Primárnu úlohu tu zohráva práve použitie ozbrojeného násilia v jeho symetrickej alebo asymetrickej forme. *„Hybridná vojna“* síce slúži tomu istému účelu, teda k dosiahnutiu politických cieľov, ktoré môžu byť veľmi rozmanité, avšak od vojny v klasickom poňatí sa v mnohých aspektoch líši.

Napriek tomu, že v odbornej literatúre existuje celý rad názorov na to, čo možno chápať pod pojmom hybridná vojna, najvýraznejším demarkačným kritériom medzi hybridnou vojnou a *„klasickou (totálnou) vojnou“* sú podľa mnohých autorov práve dominujúce použité prostriedky. Napr. kolektív autorov Kříž, Bechná a Števkov vo svojej štúdii *(2016)* konštatujú, že pre hybridné vojenstvo, resp. hybridné vedenie boja je dôležité, *„... že nevojenské prostriedky subverzívnej povahy majú zohrávať hlavnú úlohu. V ideálnom prípade nemusí byť vojenská sila útočiacim štátom otvorene použitá vôbec“.* V týchto intenciách je hybridná vojna vnímaná ako *„... ozbrojený vojenský konflikt vedený kombináciou nevojenských a vojenských prostriedkov s cieľom ich synergického efektu prinútiť protivníka k takým krokom, ktoré by sám od seba neurobil. Aspoň jednou stranou konfliktu je štát. Hlavnou úlohou pri dosiahnutí cieľov vojny hrajú nevojenské prostriedky v podobe psychologických operácií a propagandy, ekonomických sankcií, embarg, kriminálnych aktivít, teroristických aktivít a iných subverzných aktivít obdobného charakteru. Vojenské operácie útočníka sú vedené inkognito nepravidelnými silami kombinujúcimi symetrické a asymetrické spôsoby vedenia bojovej činnosti proti celej spoločnosti a hlavne proti jej politickým štruktúram, orgánom štátnej správy, ekonomike štátu, morálke obyvateľstva a ozbrojeným silám.“*[14] Z uvedeného vyplýva, že základnou stavebnou jednotkou predloženého konceptu hybridnej vojny je tzv. *„subverzia“ (alias podvratná činnosť, prevrat)*, ktorá vychádza z marxisticko-leninského konceptu uplatňovaného počas studenej vojny. Podstata subverzie spočíva v aktivitách kontinuálne rozčlenených do štyroch relatívne samostatných etáp, konkrétne etapy demoralizácie cieľovej spoločnosti, destabilizácie cieľovej spoločnosti, vyvolania krízy v cieľovej spoločnosti a prevzatia kontroly nad cieľovou spoločnosťou vnútornými silami napojenými na útočníka. Subverzia v kontexte hybridnej vojny sa tak stáva *upgradovanou stratégiou a taktikou* v tomto novodobom koncepte.

V mnohých ohľadoch netradičný, avšak nesporne inšpiratívny prístup k chápaniu tohoto problému, poskytuje vo svojom príspevku P. Zůna, ktorý poukazuje na vzájomnú determinovanosť hybridných hrozieb a hybridných vojen. Podľa jeho názoru sú hybridné hrozby *„výsledkom hybridného spôsobu vedenia vojnovej činnosti (hybrid warfare)“* a zároveň platí, že koncept hybridných vojen je *„založený na konštrukcii hybridných hrozieb“*. Na základe interpretácie uvedeného možno uviesť, že hybridné hrozby a hybridné vojny majú spoločný

---

[12] PAWLAK, P., 2015. *Understanding hybrid threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/.

[13] Carl von Clausewitz bol pruský generál a vojenský teoretik, ktorý žil v rokoch 1780 – 1831. Zúčastnil sa ťaženia Pruska proti Francúzsku a neskôr sa zapojil do vojny proti Napoleonovi na stranu Ruska. Jeho významným počinom, ktorým sa zapísal do dejín vojenskej stratégie je nedokončené dielo *„O Vojne“ (nem. Vom Kriege)*, ktoré malo výrazne filozofický rozmer. Popísal v ňom novodobé aspekty vedenia vojny *(napr. mobilizáciu, vojnovú propagandu)*. Základom jeho konceptu bola myšlienka, že *„... do vojnového konfliktu sa má zapájať celý národ, nielen armáda, pričom jeho cieľom má byť celkové zničenie nepriateľa“,* čo bolo v protiklade s klasickým konceptom vojny podľa *Rousseaua (podľa ktorého „... účasť občana na vojnovom konflikte je len prechodnou úlohou“).*

[14] Informačné centrum o NATO. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*: Výzkumně prezentační projekt Jagello 2000 realizovaný ve spolupráci s Fakultou sociálních studií Masarykovy univerzity v Brně a se Zastoupením Evropské komise v České republice. [online]. [cit. 2023-1-19]. Dostupné na internete: http://data.idnes.cz/soubory/na_knihovna/A161212_M02_021_HH16_PP-V1.PDF, s. 10-11.

významový základ a podobný charakter *(z pohľadu realizátorov, cieľov, sféry pôsobenia a použitých nástrojov).* Tento autor vymedzuje hybridné hrozby ako spôsob vedenia boja súčasne s kombinovaným použitím rôznych prostriedkov vedenia boja, či už ide o štátnych alebo neštátnych aktérov, rôznych typov konvenčných a nekonvenčných zbraňových systémov alebo materiálov dvojakého využitia. Na druhej strane, napriek tomu, že analyzuje koncept hybridných vojen z rôznych aspektov, je jedným z jeho mála oponentov. Podľa jeho názoru ide skôr o pojem, ktorý sa presadil viac kvôli svojej atraktivite, než na základe faktického prínosu pre chápanie komplexnosti novodobých bezpečnostných javov, cieľov a spôsobov riešenia. Pri typológii konfliktov odporúča viac ich členenie podľa Clausewitza na totálnu a čiastočnú vojnu, podľa podstaty *(cieľov)* vojny, podľa štruktúry nasadených síl a prostriedkov *(civilných a vojenských nástrojov)*, podľa foriem a metód vedenia bojovej činnosti *(civilných, vojenských, ich kombinácie)*. Za zamyslenie stojí jeho návrh substituovať pojem *„hybridné spôsoby vedenia bojovej činnosti" (angl. hybrid warfare)* pojmom *„kombinované používanie síl a prostriedkov".* V týchto intenciách sa prikláňame k názoru M. Havlíka, že hybridizácia *(kombinované pôsobenie viacerých faktorov, nástrojov apod.)* nie je v oblasti vojenstva ničím novým, ale ide o terminologicky nové kodifikované použitie pojmu *„hybridné vojenstvo"* pro mnohé súčasné typy konfliktov *(ak nie dokonca všetkých)*. Na druhej strane, v posledných rokoch, predovšetkým v prvých dvoch dekádach 21. storočia, došlo k zásadnej zmene v proporcionalite využívania jednotlivých nástrojov moci. V tejto súvislosti došlo k významnému potlačeniu nástrojov čisto vojenských, typu *„hard power"* a do popredia sa naopak dostali hlavne nástroje informačného, ekonomického, politického či spravodajského charakteru, t. j. nástroje typu *„soft power"* a *„smart power".*[15]

P. Zůna poukazuje aj na ďalší podstatný aspekt v kontexte hybridných vojen, a to na pomyselnú súvzťažnosť hybridných vojen s tzv. *„compound warfare".* [16] Podľa jeho názoru, pre tento typ vedenia vojny je typická synergia a kombinácia rôznych metód vedenia boja a použitím rôznych nástrojov na strategickej úrovni. Hybridné vojny, na rozdiel od vyššie zmienených vojen prinášajú komplexnosť, fúziu, simultánnosť a kombináciu na operačnej a taktickej úrovni v priestore bojovej činnosti.[17]

Na margo pojmového vymedzenia *„compound warfare",* T. M. Huber pod týmto termínom rozumie simultánne využitie regulárnych alebo hlavných bojových síl *(angl. regular or main force)* spolu s neregulárnymi alebo partizánskymi silami *(angl. irregular or guerrilla force)* proti nepriateľovi. Inými slovami, operujúci aktér je schopný zvyšovať svoje možnosti militantného pôsobenia využitím oboch typov síl súčasne, t. j. konvenčnej a nekonvenčnej sily. S týmto typom vedenia vojny sa podľa jeho názoru najčastejšie stretávame vtedy, keď celé územie alebo jeho časť je okupované silným interventom. Uvedený model vedenia vojny sa tak stáva vhodnou alternatívou pre slabšieho protivníka, ako za takýchto okolností uspieť vo vojnovom konflikte. [18] Z dostupnej prezentácie je zrejmé, že termín *„compound warfare"* je

---

[15] HAVLÍK, M., 2021. *Koncepty hybridního válčení a Armáda České republiky*. In *Vojenské rozhledy,* 2021, 30 (1), 038-051. ISSN 1210-3292 (print), 2336-2995 (on-line). [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/koncepty-hybridniho-valceni#_ftn18.

[16] Termín *„compound warfare"* nemožno doslovne preložiť. Aj odbornej literatúre neanglického *pôvodu (napr. v uvedenom českom titule)* sa autori často ani nesnažia prekladať tento termín doslovne, skôr využívajú jeho významovú interpretáciu. Voľný preklad tohto termínu by mohol znieť – zložený, doplnkový, zmiešaný, kombinovaný spôsob vedenia vojny.

[17] ZŮNA, P., 2010. *Kritický pohled na koncept hybridních válek*. In *Vojenské rozhledy*, 2010, roč. 19 (51), č. 3, s. 33-45, ISSN 1210-3292. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/kriticky-pohled-na-koncept-hybridnich-valek.

[18] HUBER, T. M. et al., 2002. *Compound Warfare: The Fatal Knot*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf, s. 13-14.

významovo veľmi príbuzný s termínom *„hybrid warfare“ (hybridný spôsob vedenia boja, hybridné vojenstvo)*, minimálne z pohľadu kombinácie a paralelného používania konvenčných a nekonvenčných vojenských síl vo vojnovom konflikte, s tým rozdielom, že termín *„compound warfare“* sa vo vojenskej stratégii a taktike z historického uhla pohľadu začal požívať o čosi skôr *(približne v druhej polovici 90. rokov 20. storočia)*. Samozrejme, nemôžme v týchto intenciách opomenúť ďalší podstatný aspekt, a to je nemilitantný spôsob vedenia boja, ktorý sa často aplikuje práve v hybridnom štýle alebo fenoméne vojenstva.

J. J. McCuen poukazuje na to, že rozhodujúce bitky v novodobých hybridných vojnách sa neodohrávajú na konvenčnom bojom poli, ale na asymetrických bojových poliach vrátane populácie žijúcej v konfliktnej zóne, či už ide o domáce obyvateľstvo alebo obyvateľstvo medzinárodnej komunity *(angl. „population battlegrounds”)*. Práve tieto neregulárne, asymetrické boje, podľa jeho názoru jednoznačne rozhodujú o výhre alebo porážke vo vojne. Je presvedčený, že hybridné vojny ako novodobý fenomén vyžadujú viac simultánne než postupné *(sekvenčné)* úspechy na tomto diverzifikovanom bojom poli. Učiac sa na chybách z minulosti, ešte stále nevieme plne oceniť účinok a komplexnosť rôznorodého *„ľudského terénu“ (angl. „human terrain“)*.[19]

Na druhej strane, F. G. Hoffman poznamenáva, že klasifikácia konfliktu na *„veľký a konvenčný“* verzus *„malý alebo neregulárny“* by bola príliš simplifikujúca a nedostatočne reflektujúca na evolúciu a revolúciu vo vojenstve, pretože novodobí nepriatelia využívajú kombináciu oboch spôsobov vojenstva pri dosahovaní svojich cieľov.[20]

Podľa niektorých odborníkov novodobý koncept hybridného vojenstva *(hybridného spôsobu vedenia vojny)* sa začal formovať po 11. 9. 2001, kedy sa odohral útok na veže Svetového obchodného centra v New Yorku. Táto udalosť iniciovala vznik nového konceptu, označovaného aj ako *„4GW“* , prípadne ako *„štvrtá generácia vojenstva“*. W. S. Lind, K. Nightengale, J. Schmitt a G. I. Wilson vo svojej štúdii *(2001)* vidia podstatu novej vojenskej stratégie vo využívaní konvenčných a nekonvenčných prostriedkov, vrátane terorizmu a informácií, za účelom podkopávať záujmy štátu, delegitimizovať ho a stimulovať vnútroštátny sociálny rozpad.[21] Aj tieto skutočnosti viedli v roku 2001 k vytvoreniu Centra pre novovznikajúce hrozby a možnosti pre potreby námorníctva *(Center for Emerging Threats and Opportunities – CETO).* V Národnej obrannej stratégii USA z roku 2005 *(National Defence Strategy – NDS)* sa už otvorene hovorí o existencii nových hrozieb a problémov, ktorým musia štáty čeliť *(hybridné hrozby, hybridné spôsoby vedenia vojny, ktoré postupne prenikajú do tradičných prístupov a konceptov vojenskej a obrannej stratégie štátu)*.[22]

Obavy z novodobých hybridných hrozieb boli oficiálne formulované aj v Strategickom koncepte 2010 pod záštitou NATO, ktorý bol prijatý na summite NATO v Lisabone, v novembri 2010. Tento dokument poukazuje na zmeny v bezpečnostnom prostredí, ktorých súčasťou je enormné a znepokojujúce vytváranie, hromadenie a šírenie nukleárnych zbraní a zbraní hromadného ničenia, terorizmu, extrémizmu, transnacionálnej kriminality, kybernetických útokov a technologických trendov vytvárajúcich podmienky pre tzv.

---

[19] McCUEN, J., J., 2008. *Hybrid Wars*. [online]. [cit. 2023-1-24]. Dostupné na internete: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf, s. 1.

[20] HOFFMAN, F. G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, s. 5.

[21] HOFFMAN, F. G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online]. [2023-1-19]. Dostupné na internete: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, s. 18.

[22] HOFFMAN, F. G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online]. [2023-1-19]. Dostupné na internete: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf, s. 7.

elektronické vojenstvo *(angl. „electronic warfare")*.[23] Analogicky tomu bolo aj na summite vo Wales *(2014)*, Varšave *(2016)*, Londýne *(2019),* summitoch v Bruseli *(2018, 2021)* a v Madride *(2022)*, kde boli najvyššími štátnymi a vládnymi reprezentantmi prijaté súvisiace deklarácie.[24] O aktuálnych hybridných hrozbách, hybridných aktivitách, hybridných operáciách, hybridných prostriedkoch, hybridných taktikách a hybridných kampaniach sa hovorí aj v poslednom Strategickom koncepte z roku 2022[25] a vo výročnej správe Generálneho sekretariátu NATO z roku 2021.[26] Okrem uvedeného možno k strategickým dokumentom v gescii aliancie na tomto úseku zaradiť aj BI-SC Input for a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats *(2010)*[27] a Defending against Hybrid Threats: NATO Secretary GENERAL´s Anual Report 2019 *(2020)*.

Sme toho názoru, že bezpečnostnú situáciu na tomto úseku je potrebné vnímať v širšom kontexte, nakoľko problematika hybridných hrozieb má globálny charakter. Na druhej strane, ak sa aj na problém pozrieme z pohľadu zahraničnej bezpečnostnej politiky, ako aj vojenskej a obrannej stratégie Slovenskej republiky, je potrebné si uvedomiť, že náš štát je členom Severoatlantickej aliancie a Európskej únie, tzn. je súčasťou celkového bezpečnostného prostredia, od ktorého sa nemožno izolovať, čo logicky vyvoláva potrebu posilnenia medzinárodnej spolupráce na strategickej, taktickej a operačnej úrovni. Pod záštitou NATO sú na tieto účely zriadené centrá excelentnosti. De facto ide o medzinárodné vojenské organizácie, ktorých úlohou je školiť a vzdelávať lídrov z členských štátov NATO a partnerských krajín. Celkovo je vo svete vytvorených 28 takýchto centier, pričom problematike hybridných hrozieb sa venuje napr. Centrum excelentnosti NATO na strategickú komunikáciu *(NATO StratCom CoE)*, Spoločné centrum excelentnosti NATO na kybernetickú obranu *(NATO Cooperative Cyber Defence Centre of Excellence)*. Jedno takéto centrum je od roku 2011 dokonca zriadené aj na území Slovenskej republiky *(Centrum výnimočnosti pre oblasť likvidácie výbušných materiálov v Trenčíne)*. K ďalším významným organizačno-inštitucionálnym zložkám, ktoré sa orientujú na boj proti hybridným hrozbám *(najmä ich monitoring, analýzy prostredníctvom spravodajskej činnosti)*, patrí od roku 2017 Joint Intelligence and Security Division. Odbornú pomoc poskytuje aj Counter Hybrid Support Team *(CHST)*, ktorý tvoria vojenskí aj nevojenskí bezpečnostní experti na boj proti hybrid,m hrozbám.[28] Takýto tím bol prvýkrát zostavený v roku 2019, v Čiernej hore. V týchto intenciách možno spomenúť aj pôsobenie tímu v Litve, kde v septembri 2021 monitorovali situáciu na hraniciach s Bieloruskom v súvislosti s migračnou krízou.[29]

V euro priestore sme sa na oficiálnej úrovni prvýkrát stretli s formulovaním potreby reagovať na hybridné hrozby namierené voči Európskej únii v roku 2014 *(išlo napr. o politické*

---

[23]NATO, 2010. *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization.* [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, s. 10 – 13.

[24] NATO, 2023. *NATO´s Response to Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/cps/en/natohq/topics_156338.htm.

[25] NATO, 2022. *NATO 2022 Strategic Concept*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

[26] NATO, 2021. *The Secretary General´s Annual Report 2021*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=7.

[27] NATO, 2010. *BI-SC Input for a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

[28] RŮHLE, M., ROBERTS, C., 2021. *Enlarging NATO´s Toolbox to Counter Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

[29] NATO, 2021. *The Secretary General´s Annual Report 2021*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=7.

usmernenia predsedu Európskej komisie Jean-Claude Junckera z roku 2014, Závery Rady o spoločnej bezpečnostnej a obrannej politike z mája 2015, Závery Európskej rady z júna 2015).[30]

Z vykonanej analýzy právnych dokumentov európskeho práva verejného je zrejmé, že tejto problematike sa na pôde Európskej únie pod záštitou Európskej komisie a Rady Európskej únie venuje patričná pozornosť, ktorá poukazuje na závažnosť a aktuálnosť tohto problému.[31]

V praktickej rovine došlo v dôsledku nastavenia existujúceho legislatívneho rámca na regionálnej *(európskej)* úrovni k systémovej formácii koncepčného inštitucionálneho rámca pre kontrolu a elimináciu hybridných hrozieb, ktorý zastrešujú hlavne:

- ✓ Európske centrum výnimočnosti na boj proti hybridným hrozbám *(The European Centre of Excellence for Countering Hybrid Threats – ďalej len „Hybrid CoE")*,
- ✓ Integrovaná spravodajská jednotka zameraná proti hybridným hrozbám *(EU Hybrid Fusion Cell, ďalej len „HFC")*;
- ✓ Spravodajské a situačné centrum Európskej únie *(INTCEN)*.

Sme toho názoru, čo potvrdzujú aj výsledky obsahovej analýzy dokumentov dominantne riešiacich problematiku hybridných hrozieb a hybridného vojenstva *(aplikujúc metódu kauzálnej, komparatívnej a historickej analýzy)*, že ide o skutočne vážny globálny problém, ktorému je potrebné venovať pozornosť. V týchto intenciách považujeme za potrebné zdôrazniť, že túto skutočnosť si s plnou vážnosťou uvedomuje aj Slovenská republika, dôkazom čoho je celý rad krokov, iniciatív a opatrení prijatých na národnej úrovni.

2 Identifikácia hybridných hrozieb

2.1 Indikátory hybridných hrozieb – metodologické a metodické aspekty

Pojem *indikátor* má multidisciplinárny a multidimenzionálny charakter, čo sa v konečnom dôsledku prejavuje aj v možných prístupoch využiteľných pri jeho formulácii. Stretávame sa s ním v baníctve, chémii, matematike, elektrotechnike, biológii, atď. V snahe vystihnúť fundament problému, je viac než utilitárny pohľad prírodných vied. Práve z tohto uhla pohľadu vymedzuje slovník slovenského pravopisu indikátor ako *„ukazovateľ",* resp. *„látku, ktorá zmenou svojho zafarbenia alebo inej viditeľnej vlastnosti poukazuje na zmenu chemického zloženia danej látky",* prípadne ide o *„mechanizmus, látku, jav, ukazujúci stav alebo zmenu javov alebo veľkosť veličín"*. V prenesenom význame ide teda o *ukazovateľ momentálneho stavu reflektujúceho proces transformácie*. Aj v policajnej a bezpečnostnej

[30] Consilium 8971/15, EUCO 22/15 – pozn. autora.

[31] Bez nároku na úplnosť, k najvýznamnejším dokumentom na tomto úseku patria:

- ✓ *Európska stratégia energetickej bezpečnosti (2014),*
- ✓ *Za otvorené a bezpečné svetové oceány: prvky stratégie námornej bezpečnosti Európskej únie (2014),*
- ✓ *Európsky program v oblasti bezpečnosti (2015),*
- ✓ *Akčný plán v oblasti európskej obrany (2016),*
- ✓ *Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie (2016),*
- ✓ *Globálna stratégia pre zahraničnú a bezpečnostnú politiku Európskej únie (2016),*
- ✓ *Spoločné oznámenie o implementácii Spoločného rámca pre boj proti hybridným hrozbám – reakcia Európskej únie (2016),*
- ✓ *Spoločná deklarácia prezidenta Európskej rady, predsedu Európskej komisie a generálneho tajomníka NATO (podpísaná 8. 7. 2016 na samite EÚ-NATO vo Varšave),*
- ✓ *Vyhlásenie o implementácii Spoločnej deklarácie prezidenta Európskej rady, predsedu Európskej komisie a generálneho tajomníka NATO (6. 12. 2016),*
- ✓ *Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby (2018),*
- ✓ *Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde (2020),*
- ✓ *Strategický kompas pre silnejšiu bezpečnosť a obranu Európskej únie do roku 2030 (2022)*.

teórii je tento pojem už domestifikovaný, operujú s nim odborníci v oblasti kriminológie, kriminalistiky, vyšetrovania či odhaľovania a objasňovania trestných činov *(napr. I. Šimovček, M. Lisoň, J. Stieranka, P. Augustín, I. Látal, D. Bango, Š. Kočan, R. Rak, J. Meteňko, L. Hofreiter, A. Byrtusová, M. Hullová)*.

Vstupnou premisou pre uvažovanie podobného druhu je gnozeologická teória odrazu a jej pravidlo, že všetky predmety a javy materiálneho sveta možno poznávať prostredníctvom ich odrazu *(v podobe materiálnych a pamäťových stôp).* De facto ide o aplikáciu dialektického prístupu, podstatou ktorého je predpoklad, že veci a javy a priori predpokladajú existenciu vonkajších prejavov, a na druhej strane, vonkajšie prejavy indikujú, nasvedčujú existencii určitých vecí a javov. Dotiahnuc naše uvažovanie do dôsledkov, *indikátor predstavuje konkrétnu formu prejavu určitého javu navonok, ktorú môžeme vnímať, poznávať a hodnotiť, a tak sa zákonite o jave viac dozvedieť*. V týchto súvislostiach je indikátor *určitým symptómom (príznakom), charakteristickým vonkajším znakom, výraznou, typickou vlastnosťou niečoho.* Každý indikátor je zistiteľnou existenciou *(výskytom)* určitej veci alebo javu *(možno ho objektívne vnímať a pozorovať zmyslami, analyzovať a hodnotiť myšlienkovými procesmi)* a každý indikátor je vymedzený presne určenou skupinou znakov, funkcií a vlastností a je odlíšiteľný od inej skupiny znakov, funkcií a vlastností *(možno objektívne registrovať jeho rozlišovaciu črtu)*.

Problémom zostáva, že nie vždy sa nám podarí nájsť, resp. správne interpretovať vzťah *indikátor verzus predmet alebo jav*, aj vzhľadom na rôzne subjektívne determinanty *(napr. možnosti, schopnosti, vedomosti, skúsenosti, návyky, myšlienkové a kognitívne stereotypy, motiváciu pozorovateľa)* a objektívne determinanty *(napr. (ne)jednoznačnosť, (ne)prehľadnosť, (ne)heterogénnosť, (ne)čitateľnosť, (ne)predvídateľnosť, (ne)usporiadanosť, ne)systematickosť, zložitosť/jednoduchosť, náhodnosť/regulárnosť, prejavov konkrétneho javu)*.

V procese vnímania, poznávania a hodnotenia indikátor vystupuje ako *počiatočný poznatok o nejakej veci alebo jave, na základe ktorého začína proces jeho identifikácie a interpretácie*. Uvedené chápanie poukazuje na jeho informačnú funkciu *(význam)* indikátora. Každý indikátor je vo svojej podstate *komplexom informácií (inputom), ktorý vstupuje do informačného procesu a znižuje mieru entropie (neznalosti) o danom jave.* Výsledkom tohto tvorivého procesu *(zber, získavanie, triedenie, analýza, vyhodnotenie, využitie, distribúcia)* je interpretácia vzťahu indikátor verzus jav *(output – spracovaný údaj).* Indikátor možno vnímať aj z pohľadu jeho stimulačnej funkcie. V tomto prípade ide o *signál nasvedčujúci vzniku určitej udalosti, vyvolávajúci záujem alebo podozrenie zo strany pozorovateľa*. Korešponduje s tým aj asociácia zdôrazňujúca diferenciačnú funkciu indikátora. Podľa niektorých odborníkov sú indikátory *odchýlkou od normálnej situácie, ktorú dobre poznáme, a ktorá zodpovedá dodržiavaniu zákonov, nariadení a iných spoločenských noriem*. Pri takejto odchýlke je možné záujem pozorovateľa logicky predpokladať, *indikátor sa stáva inhibítorom (podnetom, stimulom, impulzom) záujmu o danú vec alebo jav, pretože nasvedčuje tomu, že „niečo nie je v poriadku“*.

Otázne je: *„Či indikátor sám o sebe predstavuje taký druh inhibítora, ktorý „nutne“ vyvoláva aktivitu na strane príjemcu?“* Na margo uvedeného možno uviesť, že tento potenciál indikátory určite majú, avšak v týchto intenciách nemožno hovoriť o jednoznačnom a generalizujúcom *(obligatórnom)* vzťahu, tzn. že použitie slovnej konštrukcie *„povinnosť konať“* namieste nie je. Na druhej strane, v praxi sú registrované situácie, keď sa od určitých subjektov aktivita žiada. Uvedené sa osobitne vzťahuje na činnosť orgánov presadzujúcich právo, podstatou ktorej je identifikácia a interpretácia indikátorov konaní majúcich protiprávny charakter *(napr. priestupky, správne delikty, trestné činy).* Tzn., že kritériom *(obligatórnym dôvodom)* pre začatie konania *(odhaľovania, objasňovania a dokazovania)* je samotná protiprávnosť javu *(jav ohrozuje alebo poškodzuje záujmy chránené spoločnosťou a vymedzené*

právom). Uvedené možno ilustrovať tým, že povinnosť odhaľovať, objasňovať a dokazovať protiprávne konania je jednou z kľúčových povinností určených orgánov bezpečnostného a justičného systému *(napr. polície, Finančnej správy, Zboru väzenskej a justičnej stráže, spravodajských služieb, prokuratúry, súdov)*. De facto ide o aplikačnú stránku zásad oficiality a legality *(etický, morálny, spoločenský a zákonný mandát)*.

Považujeme za dôležité na tomto mieste opätovne zdôrazniť, že identifikácia indikátora a interpretácia vzťahu indikátor verzus jav nebýva v praxi celkom jednoduchá, aj vzhľadom na vyššie zmienené determinanty objektívneho a subjektívneho charakteru. Pri hodnotení *nutnosti reakcie*, sú to práve také metriky, akými sú kvalita a kvantita objektívnych determinantov *(napr. intenzita indikátora, miera jeho čitateľnosti, vierohodnosti, obvyklosti, logickosti, konzistentnosti, úplnosti, pravdepodobnosti)* podstatným spôsobom ovplyvniť celý proces identifikácie a následnej interpretácie indikátora.

Na druhej strane tu vzniká priestor pre úvahy: *„Či indikátor sám o sebe predstavuje taký druh inhibítora, ktorý je objektívne možné zachytiť, vnímať, poznávať a hodnotiť aj bez patričnej aktivity pozorovateľa?“*. Sme toho názoru, že určite áno *(v opačnom prípade by indikátor stratil niektoré z hlavných definičných čŕt – symptómovosť, príznakovosť, typickosť, zistiteľnosť a pod.)*. Samozrejme, často to závisí aj od intenzity samotného indikátora *(napr. jednoznačnosti, čitateľnosti, neobvyklosti, netradičnosti, novosti – objektívne determinanty).* Avšak aj tu existujú určité limity, pretože bez cieľavedome zameranej pozornosti *(intencionálnej aktivity)* pozorovateľa je pravdepodobnosť *úspešnej* identifikácie a interpretácie indikátora veľmi nízka, resp. podstatne sťažená. Indikátory môžu logicky nasvedčovať existencii pozitívnych aj negatívnych javov či konaní v spoločnosti. Nás, aj vzhľadom na riešený problém, budú zaujímať tie konania a javy, ktoré majú negatívny, protispoločenský charakter. Z pohľadu orgánov presadzujúcich právo sa v týchto intenciách žiada systematicky orientovať svoju pozornosť na vyhľadávanie možných indikátorov protiprávnych konaní, ich identifikáciu a interpretáciu. Práve týmto prístupom je možné dosiahnuť vyššiu mieru kontroly *(prevencie a represie)* nežiaducich javov a konaní v spoločnosti, t. j. stav, keď sú za daných okolnosti právo a poriadok rešpektované v čo najvyššej možnej miere *(bezpečnosť).* Z uvedeného vyplýva, že na subjekty, ktoré sú zodpovedné za identifikáciu a interpretáciu indikátorov protiprávnych konaní a javov, sú logicky kladené určité požiadavky v duchu hesla *smieť-vedieť-chcieť konať,* pretože v prípade, ak by ktorákoľvek z týchto zložiek absentovala alebo nebola adekvátna, úspešnosť celého procesu by bola skôr otázkou náhody, ba dovolíme si tvrdiť, že aj značne nereálna.

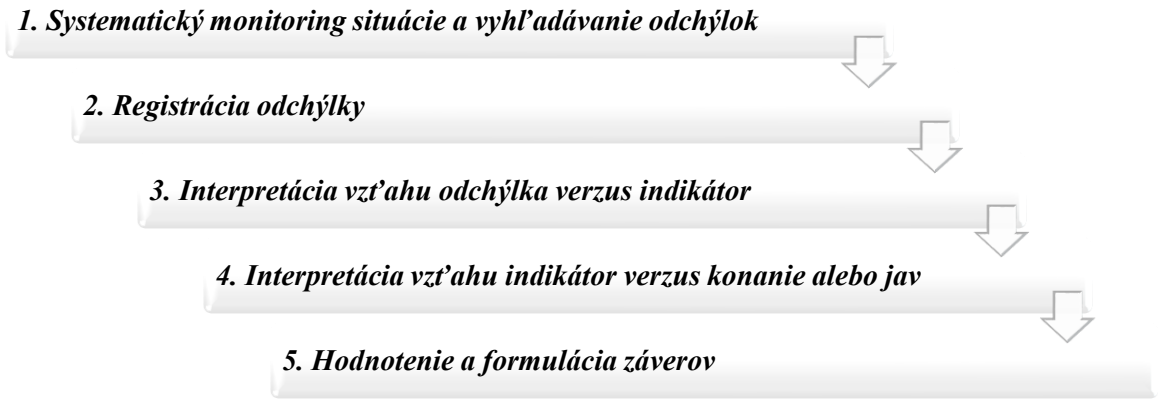
V kontexte uvedených tvrdení sa možno zamerať na hodnotenie dôkaznej funkcie *(významu)* indikátorov, hľadajúc odpoveď na otázku: *„Aký je vzťah medzi indikátorom a dôkazom v procese objasňovania trestných činov?“* Zastávame názor, že indikátory v žiadnom prípade nemožno považovať za hotové dôkazy, pretože stupeň ich právnej relevancie je pomerne nízky. Skôr má význam hovoriť o ich informačnej a kriminalistickej relevancii, aj keď ani tá nemusí byť a zvyčajne ani nebýva veľmi vysoká, pretože *indikátor obsahuje väčšinou druhotné, signálne informácie o určitých skutočnostiach, ktoré môžu (nemusia) mať vzťah ku kriminalisticky relevantnej udalosti.* V nadväznosti na uvedené sa vynára otázka: *„Aký je skutočný význam indikátorov, keď v porovnaní s oficiálnymi podnetmi majú toľko nedostatkov?“* Odpoveď možno hľadať v latencii, sofistikovanosti, organizovanosti protiprávnych konaní a problémoch spojených s ich identifikáciou, osobitne pri napĺňaní legitímnej ambície vyvodzovania trestnoprávnych a iných dôsledkov voči zodpovedným osobám *(subjektom porušujúcim a ohrozujúcim právo a poriadok).* Indikátory totižto v sebe nesú reálnu potenciu nepriaznivú bilanciu na úseku odhaľovania a objasňovania protiprávnych konaní vylepšovať, nakoľko ide *o komplex informácií nasvedčujúci tomu, že skutok, ktorého znaky sú uvedené v zákone (Trestnom zákone) sa stal, momentálne prebieha alebo ešte len prebehne*. Je potom úlohou orgánov presadzujúcich právo na základe práva a v jeho medziach

(zákonným spôsobom, za využitia zákonných prostriedkov) vyvodiť a preukázať zodpovednosť za protiprávne konanie konkrétnym osobám.

Indikátory protiprávnych konaní a negatívnych spoločenských javov možno klasifikovať z rôznych hľadísk, pričom samotné členenie indikátorov na jednotlivé subkategórie či triedy nepriamo vypovedá o ich charaktere *(najmä o ich hybridnosti)*. Z tohto uhla pohľadu možno bez nároku na úplnosť hovoriť o nasledovných klasifikačných kritériách a subkategóriách indikátorov:

- ✓ miera všeobecnosti *(všeobecné a špeciálne)*,
- ✓ časové hľadisko *(pred vznikom javu/ spáchaním skutku, v priebehu existencie javu/ v priebehu páchania skutku, po zániku existencie javu/ po spáchaní skutku)*,
- ✓ priestorové/ teritoriálne hľadisko *(domáce, zahraničné, zmiešané)*,
- ✓ kvantitatívne hľadisko *(časté, menej časté, zriedkavé)*,
- ✓ kvalitatívne hľadisko *(kvalita informácií, kvalita informačného zdroja – pravdivé/ nepravdivé, dôveryhodné/ nedôveryhodné, zjavné/ latentné, a pod.)*,
- ✓ subjektové hľadisko *(vec, jav, osoba, jednotlivec/ skupina osôb, verejný/ neverejný alias súkromný sektor, mocenská/ nemocenská pozícia, vzdelanie a pod.)*,
- ✓ objektové hľadisko *(legitímne/ nelegitímne, morálne/ nemorálne, profitujúce/ neprofitujúce a pod.)*.

Práca s indikátormi má jednoznačne procesuálny charakter, tzn., že ju tvorí sled viacerých, kontinuálne na seba nadväzujúcich činností *(postupov, operácií a úkonov)*, vzájomne prepojených *(ktorých integrujúcim činiteľom je spoločný cieľ, úloha, funkcia)*, logicky a časovo ohraničených *(majú svoj začiatok, priebeh a koniec)*. Pravdepodobne netreba pripomínať, že takýto prístup je účelový a umožňuje nám jednak pochopiť jadro problému a druhej strane poznávať, ako sa náš zvolený objekt skúmania *(model)* správa a aké má vlastnosti. V idealizovanej podobe je model práce s indikátormi možné rozčleniť do nasledovných etáp:[32]



Obrázok 1. Model práce s indikátormi – zdroj: vlastná tvorba

Proces začína relatívne samostatnou etapou, a to *systematickým monitoringom situácie so zameraním na vyhľadávanie (rozpoznávanie) odchýlok.* Pre väčšinu zainteresovaných vzniká problém s definovaním *„normálnej situácie“*, pretože neexistuje jej univerzálne vymedzenie. V praxi to znamená, že to, čo určitá skupina obyvateľstva vníma ako žiaduce, je pre iného iba akceptovateľné a pre niekoho dokonca neakceptovateľné alebo vyslovene

[32] HULLOVÁ, M., 2012. *Indikátory odhaľovania a objasňovania korupcie*, s. 54.

nežiaduce. S ohľadom na variabilnosť možných prístupov je takúto situáciu možné chápať ako *„oscilujúcu okolo určitej hodnoty, ktorú všeobecne považujeme za prijateľnú.“*[33] Rešpektovanie tolerovateľnej miery odchýlok poskytuje šancu, že sa na vymedzení takejto situácie zhodne majorita spoločnosti. Podstatou *systematického* monitoringu situácie je jej vnímanie, skúmanie a hodnotenie v priebehu vývoja. Je preto logické, že k objektívnym výsledkom nemožno dôjsť v prípade, ak sa monitoring vykonáva len jednorazovo, krátkodobo, nepravidelne, či stochasticky *(výsledok by mohol byť značne skreslený, ovplyvnený momentálnym vývojom situácie, ktorý nemusí nutne vypovedať o vývoji situácie v globále).* Faktom zostáva, že celý proces vyhľadávania a rozpoznávania odchýlok jednoznačne vyžaduje intencionalitu v konaní jeho realizátorov *(cieľavedomosť, účelovosť, plánovitosť, systematickosť, aktívnosť, intenzívnosť a pod.).*

Ak sa bližšie pozrieme na podstatu procesu vyhľadávania a rozpoznávania odchýlok, je zrejmé, že vychádza z princípov *komparatívnej analýzy,* tzn., že na to, aby sme dva objekty mohli porovnať, musíme ich v prvom rade adekvátne poznať. Poznať predpokladá – cielene ich pozorovať, skúmať, analyzovať a hodnotiť podľa vopred zvolených kritérií. Až následne je možné oba objekty, podľa premyslenej schémy postupu, komparovať *(t. j. hľadať spoločné – príbuzné a rozdielne – nepríbuzné znaky a črty).* Z metodického hľadiska prichádza do úvahy paralelné poznávanie a porovnávanie objektov *(oba objekty súčasne)* alebo kontinuálne poznávanie a porovnávanie *(najprv jeden a až potom druhý objekt).* Osobitne v tomto prípade, keď porovnávame situáciu vo vývoji, má svoje opodstatnenie kontinuálne poznávanie a porovnávanie.

Na konečný výsledok tohto procesu výrazne vplývajú subjektívne determinanty, osobitne úroveň percepčných, rozumových a analytických schopností, ako aj *znalosť situácie v bežných podmienkach,* t. j. znalosť právneho systému, operatívnej situácie, modusu operandi protiprávnych konaní, osobná a miestna znalosť a pod Mnohí odborníci odporúčajú zamerať svoj *focus* na tie identifikačné objekty *(osoby, veci, miesta, urbanistické objekty, situácie a pod.)*, ktoré sú *rizikové, citlivé.* Napr. pri kontrole kriminality môže ísť o tzv. *záujmové osoby, veci, miesta, objekty a situácie, ktoré majú súvis s pripravovanou, páchanou alebo spáchanou trestnou činnosťou, prípadne iným negatívnym spoločenským javom.* Niektorí odborníci odporúčajú orientáciu na *situácie*, pretože tie vo svojej podstate inkorporujú všetky ostatné parametre *(osoby, veci, objekty, miesta).*[34]My sa viac prikláňame k názoru, že takýto prístup, napriek jeho všestrannosti, môže v praxi spôsobovať nemalé problémy, hoci z dlhodobého a koncepčného hľadiska je určite namieste *(napr. zbytočný široký záber identifikačných objektov sa v konečnom dôsledku môže premietnuť do spochybnenej efektívnosti a účelnosti celého procesu, a práve preto je potrebné rešpektovať konkrétne požiadavky adresátov týchto procesov).* Napriek uvedenému budeme v kontexte riešeného problému, najmä zo simplifikačného hľadiska, používať termín *situácia*, bez ohľadu na to, ktoré konkrétne parametre boli/sú/budú naším primárnym identifikačným objektom.

Ďalšou etapou je *registrácia odchýlky* podmienená analýzou vstupných údajov získaných z realizácie prvej etapy. Laicky povedané, odchýlka predstavuje rozdiel medzi tým, čo je a čo by malo byť. Na to, aby sme mohli vysloviť vierohodný záver o existencii určitej odchýlky, je potrebná dôkladná príznaková analýza vstupných údajov *(primárnych a sekundárnych dát, t. j. aktuálnych a historických dát).* Z lingvistického hľadiska sa analýza často zamieňa s pojmami analytická činnosť, analytická práca, avšak obsah týchto pojmov nie je, napriek ich príbuznosti, identický. Podstatu problému tvorí fakt, že analýza označuje proces *(analytickú činnosť)* a zároveň aj jeho výsledok *(analytický dokument).* Významový rozdiel sa často dá zistiť až v kontexte čítanej vety. Ani pojmy *analýza* a *analytická činnosť* nie sú totožné, ak si uvedomíme, že analýza vyjadruje len určitú analyticko-syntetickú metódu v rámci

[33] LÁTAL, I., 1996. *Příznaková analýza a možnosti jejího užití v policejní praxi*, s. 74.
[34] BUDKA, I., 2002. *Vybrané kapitoly služby kriminální policie a vyšetřování*, s. 235.

analytickej činnosti. V spoločenských vedách ide *„o dôsledné poznávanie a hodnotenie spoločenskej skutočnosti, t. j. objektov, javov, procesov a ich vzájomných vzťahov, súvislostí medzi nimi a hľadania príčin. Tým, že zobrazuje skúmaný objekt, v čo najväčšej šírke jeho vlastností a vzťahov, umožňuje skúmajúcemu preniknúť do podstaty javov a objasniť skryté súvislosti problémov.“*[35]

Prívlastok *príznaková* vypovedá o zameraní takejto činnosti, pretože analýza nám môže pomôcť nájsť odpovede na okruhy problémov ozrejmujúce charakter príznakov javu. Prednostne rieši nasledovné otázky: *„Čo sa stalo? Ako sa to stalo“ Prečo sa to stalo? Kde sa to stalo? Kedy sa to stalo? Aká veľká je odchýlka (kvantitatívny a kvalitatívny rozsah zmien)? Ktoré subjekty (príp. ich počet) zaznamenalo odchýlku?“* V tejto súvislosti je potrebné vziať do úvahy aj skutočnosť, že v procese registrácie odchýlky môže dochádzať k určitým chybám, skresleniam či nepresnostiam vznikajúcich napr. v dôsledku subjektivizmu pri vnímaní a hodnotení reality alebo informačných šumov. Práve preto je potrebné spektrum poznatkov o odchýlke čo najviac upresňovať, dopĺňať ďalšími informáciami, a dosiahnuť tak logické vysvetlenie toho, čo bolo i nebolo porovnávané a zistené. [36]

Podstatou tretej etapy je *interpretácia vzťahu odchýlka verzus indikátor.* V týchto intenciách je potrebné uviesť, že nie každá odchýlka od normálnej situácie musí byť nutne vnímaná ako indikátor určitého konania alebo javu, pretože nemá dostatočnú kvalitatívnu alebo kvantitatívnu intenzitu či relevanciu *(napr. absentuje prítomnosť príznakovej črty).* Okrem toho, ak by sme túto odchýlku vnímali izolovane, pravdepodobnosť správnej interpretácie by bola zrejme veľmi nízka, a práve z tohto dôvodu si táto etapa vyžaduje opätovné vyhľadávanie ďalších odchýlok, prípadne hľadanie väzieb medzi týmito odchýlkami. S narastajúcim počtom odchýlok *(dve a viac)* sa lineárne zvyšuje aj úspešnosť interpretácie vzťahu odchýlka verzus indikátor resp. určenia pravdivostnej alebo pravdepodobnostnej hodnoty záveru *(registrovaná odchýlka určite/pravdepodobne je/nie je indikátorom konkrétneho konania alebo javu)*. Pri mnohých, najmä protiprávnych konaniach a javoch, u ktorých dominuje ich latentný charakter, je vyhľadávanie odchýlok veľmi náročný proces spadajúci do kompetencií operatívnych a spravodajských zložiek štátu.

Po vyvodení záveru, že zaznamenaná odchýlka je alebo s najväčšou pravdepodobnosťou môže byť indikátorom protiprávneho konania alebo javu, nasleduje ďalšia etapa, ktorá spočíva v *interpretácii vzťahu indikátor verzus konanie alebo jav.* Z logiky veci vyplýva, že každý indikátor nasvedčuje existencii určitého konania alebo javu, otázne je: *„Či sa nám podarí tento vzťah racionálne interpretovať a nájsť správnu kombináciu indikátora a konania alebo javu?“* Situáciu komplikuje aj skutočnosť, že rôzne konania a javy môžu mať rovnaké alebo veľmi príbuzné indikátory, ktoré vedú k ich zámene a k vytvoreniu mylných súdov. Práve z tohto dôvodu je ešte pred samotným formulovaním záveru potrebné vykonať opätovnú analýzu, pretože každá analýza umožňuje rozčleniť informácie na pravdivé a nepravdivé, relevantné a irelevantné, nutné a náhodné atď. V tomto prípade sa osobitne odporúča použiť kauzálnu a systémovú analýzu. Kauzálna analýza nám umožní pochopiť väzby medzi príčinou a následkom *(jav, konanie – indikátor)* a systémová analýza väzby medzi jednotlivými prvkami vo vnútri systému a viacerými systémami navonok *(medzi indikátormi jedného javu alebo konania navzájom, medzi jedným javom a konaním a iným javom a konaním).* Konečným produktom tohto myšlienkového procesu je opätovne vyslovenie záveru o pravdivostnej alebo pravdepodobnostnej hodnote indikátora určitého konania alebo javu *(indikátor určite/pravdepodobne je/nie je prejavom existencie konkrétneho konania alebo javu).*

---

[35] KULÍŠEK, M., 1997. *Analytická činnosť v rezorte MV SR*, s. 4-7.
[36] LÁTAL, I., 1996. *Příznaková analýza a možnosti jejího užití v policejní praxi*, s. 75.

Záverečnou etapou práce s indikátormi je *zhodnotenie celého procesu* z hľadiska jeho efektívnosti, účelnosti, zákonnosti, objektívnosti a relevancie a *formulácia záverov a odporúčaní*, predovšetkým zodpovedaním nasledovných otázok:

- ✓ *Čo sa nám podarilo urobiť a zistiť?*
- ✓ *Čo sa nám nepodarilo urobiť a zistiť?*
- ✓ *Prečo sa nám to nepodarilo urobiť a zistiť?*
- ✓ *Ako to môžeme momentálne prípadne do budúcna napraviť?*
- ✓ *Ako to, čo sa nám podarilo urobiť alebo zistiť, môžeme ďalej využiť?*

Hlavne posledná zmienená otázka vypovedá o ďalšom možnom využití poznania, ktoré sme nadobudli pri práci s indikátormi. Ak na tento proces nazeráme v kontexte identifikácie a kontroly *(prevencie a represie)* nežiadúcich konaní alebo javov v spoločnosti, dominantne prostredníctvom operatívno-pátracej, spravodajskej činnosti, vyšetrovania a dokazovania trestných činov, naším cieľom je formulácia záveru o opodstatnenosti začatia trestného stíhania resp. vyvodenia trestnoprávnej zodpovednosti voči konkrétnej osobe/osobám/skupinám osôb. De facto ide o transformačný proces, kde je typický informačný reťazec pri práci s indikátormi reprezentovaný *nespracovaným údajom – analytickou informáciou – operatívnou informáciou – dôkaznou informáciou* a spadá do vecnej pôsobnosti operatívnych a spravodajských zložiek štátu, ako aj orgánov činných v trestnom konaní a súdov.

2.2 Indikátory hybridných hrozieb – praktické aspekty

Komplexné vymedzenie spektra indikátorov hybridných hrozieb, ktoré registrujeme v spoločnosti, predstavuje skutočne náročnú *(praktickú, teoretickú, aj výskumnú)* úlohu. Vzhľadom na zložitosť a hybridnosť tohto javu, si dokonca, s určitou mierou skepsy, dovolíme tvrdiť, že ide o úlohu nesplniteľnú v plnom rozsahu. Napriek tomu tu takéto počiny registrujeme a vnímame ich jednoznačne pozitívne. Problematike indikátorov hybridných hrozieb je venovaná osobitná pozornosť v Koncepcii pre boj Slovenskej republiky proti hybridným hrozbám z roku 2018. Medzi tie najrelevantnejšie indikátory hybridných útokov v SR podľa bezpečnostných analytikov patria:

- ✓ externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ✓ ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- ✓ rozsiahle sabotáže proti kľúčovej infraštruktúre;
- ✓ kybernetické útoky s potenciálom spôsobiť škody veľkého rozsahu;
- ✓ informačné a propagandistické operácie s cieľom podkopať dôveru v štátne inštitúcie, vyvolať spoločenské nepokoje a vážne destabilizovať politickú a bezpečnostnú situáciu;
- ✓ ovplyvňovanie etnických, náboženských a kultúrnych menšín a ich manipulácia na politické účely;
- ✓ hrozba použitia vojenskej sily.[37]

Z uvedeného je zrejmé, že podstata indikátorov hybridných hrozieb spočíva v intencionálnom a komisívnom konaní, ktoré môže mať militantný *(násilný)* aj nemilitantný *(nenásilný)* charakter. Zastávame názor, že prezentované spektrum indikátorov nie je uzavretým systémom *(chýbajú v ňom niektoré aspekty, napr. strategická korupcia, aktivity polovojenských a extrémistických skupín, ovplyvňovanie volebných procesov)* a ani statickým

[37] NBÚ, 2018. Koncepcia boja proti hybridným hrozbám. [online]. [cit. 2023-1-26]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

systémom *(systém sa mení, vyvíja, je mnohostranný a heterogénny),* a práve preto ho je potrebné permanentne skúmať, analyzovať, hodnotiť a dopĺňať. Pokiaľ sa na problém pozeráme optikou cez národnú úroveň, táto úloha spočíva na pleciach spoločnosti a štátu. V konkrétnych reáliách ide najmä o štátne orgány a orgány štátnej správy, napr. o Ministerstvo vnútra Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo spravodlivosti Slovenskej republiky, Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky, Národný bezpečnostný úrad *(de facto ide o široké spektrum štátnych subjektov, okrem iného inkorporujúcich bezpečnostné, vojenské, operatívne, spravodajské zložky)*. Úlohou týchto subjektov je získavať informácie o incidentoch vo vzťahu k hybridným hrozbám podľa indikátorov, analyzovať, hodnotiť a nahlasovať ich kompetentným adresátom *(najmä Národnému bezpečnostnému analytickému centru – NBAC, Situačnému centru Slovenskej republiky – SITCEN)*, ktorí ich majú následne spracovať, posúdiť alebo vyhodnotiť a spracované poznanie postupovať či predkladať konečným adresátom *(Kancelária Bezpečnostnej rady Slovenskej republiky, Bezpečnostná rada Slovenskej republiky, vláda, parlament, prezidentka Slovenskej republiky, a pod.)*. Určité druhy indikátorov *(za podmienky, že napĺňajú znaky skutkovej podstaty niektorého z trestných činov uvedených osobitnej časti Trestného zákona)* sú tieto subjekty povinné oznamovať orgánom činným v trestnom konaní.

Pri hodnotení bezpečnostných hrozieb platí premisa, že prejav hrozby nemožno vnímať izolovane, nezávisle od iných prejavov. *„Podstatnou črtou hybridného spôsobu boja je súčinnosť a prepojenie rôznych prvkov hybridnej hrozby a ich paralelné nasadenie tak, aby vytvorili kvalitatívne vyššiu a zložitejšiu viacdimenzionálnu hrozbu. Hybridnou hrozbou sa rozumie až kombinované použitie niekoľkých, najmenej troch indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.“*[38]

Z uvedeného vyplýva, že pri práci s indikátormi hybridných hrozieb sa zohľadňuje nielen ich kvalitatívne, ale aj kvantitatívne hľadisko *(požiadavka minimálneho počtu registrovaných indikátorov).* Týmto prístupom je možné zabezpečiť vyššiu reliabilitu a validitu dosiahnutých záverov.

V podmienkach rezortu vnútra je potreba koordinácie zberu, vyhodnocovania a zdieľania informácií majúcich charakter hybridnej hrozby *(indikátorov hybridných hrozieb)* zakomponovaná v Pláne hlavných úloh Ministerstva vnútra Slovenskej republiky na rok 2022. Konkrétny postup po získaní informácie majúcej charakter hybridnej hrozby v hrubých rysoch upravuje nariadenie Ministerstva vnútra Slovenskej republiky č. 51/2017 o poskytovaní informácií NBAC. V súlade s týmto interným aktom riadenia je gestorom pre komunikáciu s NBAC v pôsobnosti ministerstva – národná protiteroristická jednotka národnej kriminálnej agentúry Prezídia Policajného zboru *(PTC NAKA)*. Na druhej strane, NBAC vystupuje, v zmysle uznesenia vlády Slovenskej republiky č. 229/2016 z 8. 6. 2016, ktorým bol schválený nový štatút NBAC ako analytické, komunikačné a kooperačné stredisko Slovenskej informačnej služby s pôsobnosťou na celom území Slovenskej republiky pre oblasť bezpečnostných hrozieb. Špecifické postavenie v systéme inštitucionálneho zabezpečenia kontroly hybridných hrozieb v tomto rezorte prináleží Centru boja proti hybridným hrozbám *(CBHH)* v rámci Inštitútu správnych a bezpečnostných analýz *(ISBA)*.

Samotný model postupu vyplýva z Akčného plánu koordinácie boja proti hybridným hrozbám na roky 2022 – 2024 *(APHH)* a metodického zámeru zberu indikátorov hybridných hrozieb v rámci Ministerstva vnútra Slovenskej republiky. Podstata tohto modelu spočíva v tom, že určené útvary Ministerstva vnútra Slovenskej republiky zašlú informácie majúce charakter indikátorov hybridných hrozieb *(manuálne prostredníctvom formulára alebo sprístupnením databázy)* – CBHH, ktoré ich vyhodnotí, zanalyzuje a následne zašle

[38] NBÚ, 2018. Koncepcia boja proti hybridným hrozbám. [online]. [cit. 2023-1-26]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

v stanovenom formáte PTC NAKA, ktoré komunikuje s NBAC. Analogický model je aplikovaný aj u ostatných štátnych orgánov, ktorým táto povinnosť vyplýva z APHH.

Záver

Hybridné hrozby predstavujú pre štáty a spoločenstvá enormné riziko, ktorému je potrebné venovať pozornosť v každom smere. Sme toho názoru, že súčasná bezpečnostná situácia vyžaduje systematický monitoring situácie, vyhľadávanie odchýlok, ktoré majú potenciál indikátora hybridných hrozieb, pretože práve týmto prístupom je možné pozitívne situáciu ovplyvniť, prípadne sa pripraviť na ďalší *(aj rizikový)* vývoj bezpečnostnej situácie. Indikátory hybridných hrozieb ako prejavy hybridného pôsobenia či hybridného spôsobu vedenia boja predstavujú značne diferencovaný systém, ktorý je často veľmi náročné dekódovať. Napriek tomu, že situáciu nám do istej miery komplikujú rôzne objektívne aj subjektívne determinanty, vyjadrujeme presvedčenie, že dôkladná a systematická operatívna a spravodajská činnosť v prepojení s komplexnou analytickou prácou sú osvedčenými piliermi efektívnej identifikácie a eliminácie *(minimalizácie)* hybridných hrozieb.

Literatúra

Printové dokumenty

BUDKA, I., 2002. *Vybrané kapitoly služby kriminální policie a vyšetřování*. Praha: Policajní Akademie České republiky, 2002. 266 s.

HULLOVÁ, M., 2012. *Indikátory odhaľovania a objasňovania korupcie*. Bratislava: Akadémia Policajného zboru v Bratislave, 2012. 116 s. ISBN 978-80-8054-551-2.

KULÍŠEK, M., 1997. *Analytická činnosť v rezorte MV SR*. Bratislava: Akadémia Policajného zboru v Bratislave, 1997. 111 s. ISBN 80-8054-028-4.

LÁTAL, I., 1996. Příznaková analýza a možnosti jejího užití v policejní praxi. In *Kriminalistika*, 1996, roč. XXIX, č. 1, s. 73-75.

LISOŇ, M., 2012. *Teória operatívneho policajného poznania*. Bratislava: Akadémia Policajného zboru v Bratislave, 2012. 213 s. ISBN 978-80-8054-540-6.

MO SR, *Akčný plán koordinácie boja proti hybridným hrozbám 2022 – 2024.*

MV SR, *Nariadenie Ministerstva vnútra Slovenskej republiky č. 51/2017 o poskytovaní informácií Národnému bezpečnostnému analytickému centru.*

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

Elektronické dokumenty

HAVLÍK, M., 2021. *Koncepty hybridního válčení a Armáda České republiky*. In *Vojenské rozhledy,* 2021, 30 (1), 038-051. ISSN 1210-3292 (print), 2336-2995 (on-line). [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/koncepty-hybridniho-valceni#_ftn18.

HOFFMAN, F. G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online]. [cit. 2023-1-19]. Dostupné na internete:

https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

HUBER, T. M. et al., 2002. *Compound Warfare: The Fatal Knot*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf, s. 13-14.

Informačné centrum o NATO. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy: Výzkumně prezentační projekt Jagello 2000 realizovaný ve spolupráci s Fakultou sociálních studií Masarykovy univerzity v Brně a se Zastoupením Evropské komise v České republice.* [online]. [cit. 2023-1-19]. Dostupné na internete: http://data.idnes.cz/soubory/na_knihovna/A161212_M02_021_HH16_PP-V1.PDF.

JANOŠEC, J., 2010. *Hrozba a riziko v bezpečnostní terminologii*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://dk.upce.cz/bitstream/handle/10195/37995/Jano%C5%A1ecJ_HrozbaARiziko_2010.pdf.

KŘÍŽ, Z. – SHEVCHUK, Z. – ŠTEVKOV, P., 2016. *Hybridní válka jako nový fenomén v bezpečnostním prostředí Evropy*. [online]. [cit. 2023-1-19]. Dostupné na internete: http://data.idnes.cz/soubory/na_knihovna/A161212_M02_021_HH16_PP-V1.PDF.

McCUEN, J., J., 2008. *Hybrid Wars*. [online]. [2023-1-24]. Dostupné na internete: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf.

NATO, 2010. *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

NATO, 2021. *Glossary of Terms and Definitions (English and French): AAP-06: Edition 2021*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600.

NATO, 2023. *NATO´s Response to Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/cps/en/natohq/topics_156338.htm.

NATO, 2022. *NATO 2022 Strategic Concept*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

NATO, 2010. *Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization.* [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

NATO, 2021. *The Secretary General´s Annual Report 2021*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf#page=7.

NBÚ, 2018. *Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám.* [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nbu.gov.sk/wp-content/uploads/PHHD/Koncepcia-boja-SR-proti-hybridnym-hrozbam.pdf.

PAWLAK, P., 2015. *Understanding hybrid threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://epthinktank.eu/2015/06/24/understanding-hybrid-threats/.

RŮHLE, M., ROBERTS, C., 2021. *Enlarging NATO´s Toolbox to Counter Hybrid Threats*. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

Slovník cudzích slov, 2023. [online]. [cit. 2023-1-19]. Dostupné na internete: http://slovnikcudzichslov.sk/slovo/hybrid.

Wikipedia. *Sun-c'*, 2022. [online]. [cit. 2023-1-19]. Dostupné na internete: https://sk.wikipedia.org/wiki/Sun-c%E2%80%99.

ZŮNA, P., 2010. *Kritický pohled na koncept hybridních válek*. In *Vojenské rozhledy*, 2010, roč. 19 (51), č. 3, s. 33-45, ISSN 1210-3292. [online]. [cit. 2023-1-19]. Dostupné na internete: https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/kriticky-pohled-na-koncept-hybridnich-valek.

Keywords: hybrid threat, hybrid war, classical (total) war, hybrid conflict, risk, threat, security situation, identification, indicator, analysis, analytical activity

Summary

Hybrid threats represent modern security risks that all states, societies, and nations are currently facing in varying degrees of intensity. A new conceptual way of promoting one's own interests and power, at the expense of the sovereignty, democracy, constitutionality and legality of the other, is thus becoming an immanent part of a broader military strategy. Hybrid threats are characterized by heterogeneity, latency, sophistication, planning, purposefulness, and systematicity. These features to a certain extent predict the complexity of their identification as a key factor in eliminating and minimizing their harmful consequences. These facts have also become the leitmotif of this paper. In the present scientific study, the author focuses on the methodological, methodological and practical aspects of identifying hybrid threats. Hybrid threats thus automatically become a real object of identification. Identification as a process of cognition, investigation, evaluation and explanation of social reality is, in the context of the formulated scientific problem, defined by means of hybrid threat indicators. Indicators as certain signals, symptoms, or initial knowledge of an action or phenomenon, have the potential to eliminate or minimize the risks arising from hybrid threats.

pplk. doc. JUDr. Monika Hullová, PhD.
Akadémia Policajného zboru v Bratislave
Katedra kriminálnej polície
e-mail: monika.hullova@akademiapz.sk

Recenzenti: doc. Ing. Michal Orinčák, PhD., JUDr. Juraj Drugda, PhD.