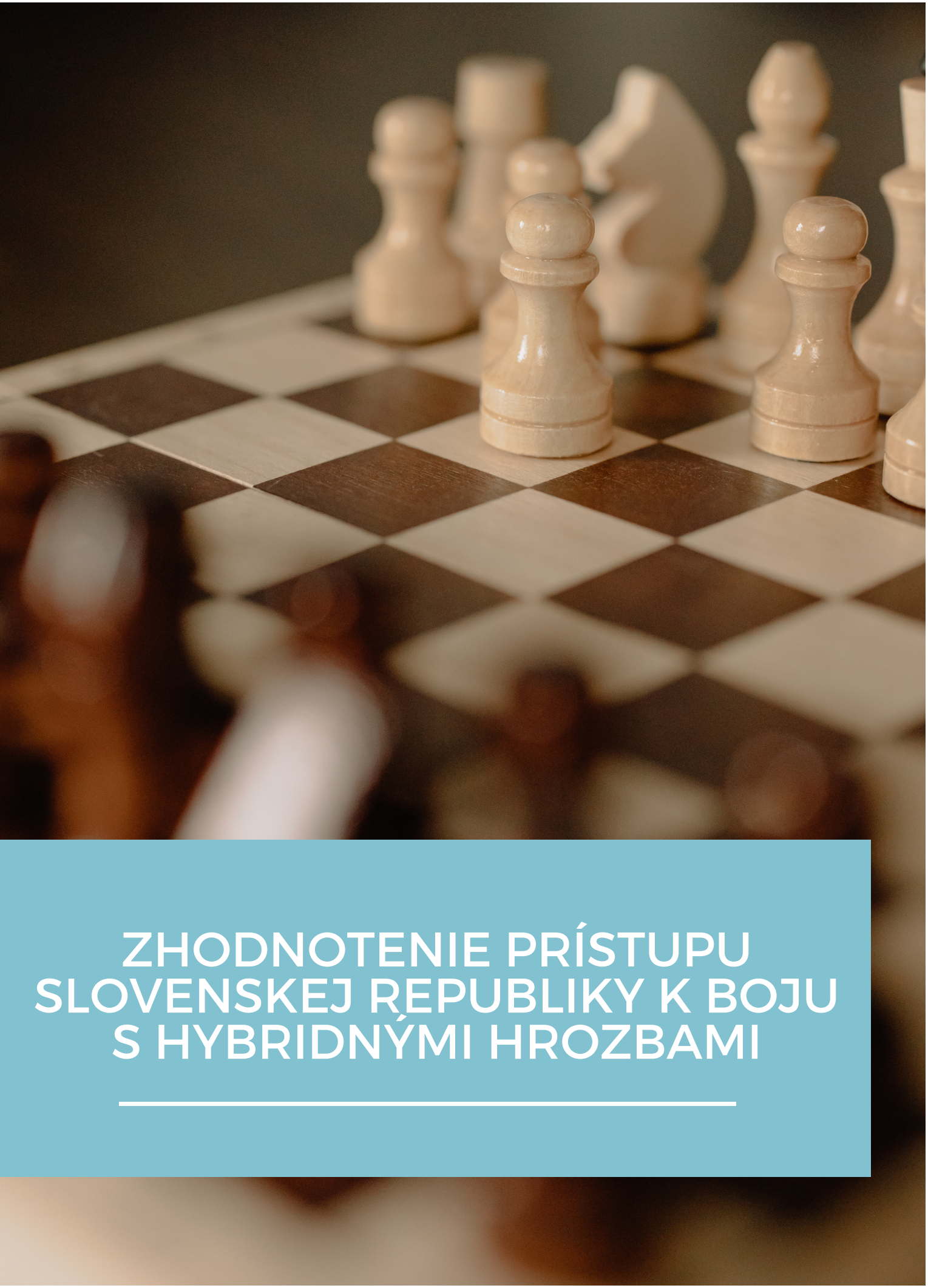


ZHODNOTENIE PRÍSTUPU SLOVENSKEJ REPUBLIKY K BOJU S HYBRIDNÝMI HROZBAMI

Autor:

Matej Kandrík, Stratpol - Strategic Policy Institute

Editori:

Peter Köles, Slovak Security Policy Institute

Kristína Urbanová, Stratpol - Strategic Policy Institute

Konzultácie:

Jakub Janda, European Values Center for Security Policy

Andrea Michalcová, European Values Center for Security Policy

Poďakovanie:

Úprimné poďakovanie patrí všetkým, ktorí sa do výskumu zapojili, ochotným respondentom, odborníkom a v neposlednom rade celému realizačnému tímu.

Výskum bol realizovaný v rámci projektu s finančnou podporou dotačných programov Ministerstva obrany Slovenskej republiky, Ambasády Spojených štátov amerických v Bratislave, NATO Public Diplomacy Division a Friedrich Naumann Stiftung.

OBSAH

KONTEXT

Prístup Slovenskej republiky (ďalej len „SR“) k boju proti hybridným hrozbám je dnes vo fáze formovania.

Primárnym dokumentom, ktorý definuje jeho základný inštitucionálny rámec je Koncepcia pre boj SR proti hybridným hrozbám (ďalej len „Koncepcia“) z roku 2018.

Záväzok intenzívne sa venovať hybridným hrozbám sformulovala nová vláda už v Programovom vyhlásení vlády SR na obdobie rokov 2020-2024 (ďalej len „PVV SR 2020-2024“).

Nová Bezpečnostná stratégia SR 2020 identifikuje pripravenosť štátu a spoločnosti efektívne a koordinovane reagovať na hybridné hrozby vrátane dezinformácií ako jednu zo strategických bezpečnostných priorít štátu.

Stratégia ďalej uvádza, že SR v rámci zvýšenia odolnosti štátu a spoločnosti voči hybridným hrozbám posilní kapacity a expertízu vo verejnej správe so zreteľom na celoštátnu koordináciu v oblasti plánovania, riadenia a tvorby politík.

Otázka hybridných hrozieb sa objavuje taktiež v Obrannej stratégii 2020. Tá odkazuje na odhodlanie SR reagovať na neželané hybridné pôsobenie proti jej zvrchovanosti, územnej celistvosti a nedotknuteľnosti hraníc, a to aj pod prahom zvyčajnej reakcie.

Ďalej pomenúva potrebu rozvinúť spôsobilosti spravodajských služieb, ústredných orgánov štátnej správy (ďalej len „ÚO ŠS“), systémovo usporiadať zdieľanie informácií, proces koordinovanej medzirezortnej analýzy a postupov predkladania informácií príslušným ústavným a štátnym orgánom na včasné rozhodovanie.

Aktuálne je v procese prípravy tiež Akčný plán na koordináciu boja proti hybridným hrozbám a šíreniu dezinformácií (ďalej len „Akčný plán“).

S časťou problematiky hybridných hrozieb súvisí aj Koordinovaný mechanizmus odolnosti SR voči informačným operáciám, ktorý sa momentálne nachádza vo fáze zapracovania pripomienok z medzirezortného pripomienkového konania.

V roku 2019 sa SR stala členom Centra výnimočnosti strategickej komunikácie NATO v Rige (ďalej len „StratCom CoE“) a následne v roku 2020 aj členom Európskeho centra výnimočnosti pre boj s hybridnými hrozbami v Helsinkách (ďalej len „Hybrid CoE“).

Obmedzený inštitucionálny rozvoj je možné pozorovať taktiež na národnej úrovni.

V štruktúrach Ministerstva zahraničných vecí a európskych záležitostí SR vzniklo oddelenie pre hybridné hrozby a budovanie odolnosti vedené veľvyslancom s osobitým poslaním.

Dedikované pracovisko pre hybridné hrozby a dezinformácie bolo vybudované aj v štruktúre Národného bezpečnostného úradu.

K rozšíreniu či špecifikácii pôsobnosti do oblasti hybridných hrozieb došlo v prípade Národného bezpečnostného a analytického centra (ďalej len „NBAC“) a Situačného centra SR (ďalej len „SITCEN“).

V blízkej dobe možno očakávať sformovanie obdobných pracovísk aj na Ministerstve obrany a v rámci spravodajských služieb.

STRATEGICKÝ RÁMEC

Za ústredný strategický cieľ boja s hybridnými hrozbami možno v súlade s vymedzením obrany štátu označiť zachovanie nezávislosti, zvrchovanosti a schopnosti vlastného rozhodovania.

Pri ideálnom systémovom nastavení môže hybridné pôsobenie voči štátu naďalej prebiehať, ale je funkčne neutralizované a ostáva bez negatívnych dôsledkov.

Pre dosiahnutie takéhoto stavu a odstrašujúceho efektu na protivníka je potrebné komplexne rozvíjať a posilňovať odolnosť štátu a spoločnosti vo všetkých dotknutých sférach.

Prioritou musí byť tiež schopnosť prijímať vlastné reaktívne opatrenia či spolupodieľať sa na medzinárodných snahách o vyvodzovaní zodpovednosti voči pôvodcom hybridných hrozieb.

Obr. 1: Strategický rámec pre boj s hybridnými hrozbami
Zdroj: autor

OPATRENIA

Opatrenia voči pôsobeniu hybridných hrozieb možno rozdeliť do dvoch široko vymedzených skupín, ktoré môžu prebiehať rovnako na na národnej, ako aj na medzinárodnej úrovni:

PREEMPTÍVNE OPATRENIA (budovanie odolnosti)

REAKTÍVNE OPATRENIA (vyvodzovanie zodpovednosti)

V oboch prípadoch môže štát postupovať verejne, priamym pomenovaním situácie či dokonca konfrontáciou, alebo neverejnými kanálmi. Pre široké spektrum možných prejavov hybridných hrozieb a dostupných reakcií nie je možné rozvinúť univerzálnu stratégiu prijímania opatrení. Napokon, aj „nereakcia“ môže byť správnou reakciou.

PRINCÍPY

Celovládny prístup

Začína organizačnou kultúrou štátnej správy, ktorá aktívne podporuje transparentnosť, koordináciu, kooperáciu a strategické uvažovanie. Požaduje zdieľané povedomie o spoločnej zodpovednosti za dobrú správu vecí verejných a cielené budovanie odolnosti.

Stavia na funkčných komunikačných mechanizmoch na vnútrorezortnej úrovni, ktoré rozvíjajú mechanizmy medzirezortnej a nadrezortnej komunikácie. Tie sú predpokladom ďalšieho súčinného pôsobenia orgánov štátnej správy.

Cieľom celovládneho prístupu je predovšetkým prekonanie efektu silového rezortizmu.

Celospoločenský prístup

Základom budovania odolnosti štátu voči hybridnému pôsobeniu je silná občianska spoločnosť, súkromný sektor a akademická obec.

Títo aktéri nesú viacero kritických funkcií dobre fungujúceho štátu a zdravej, demokratickej spoločnosti.

Štát musí systematicky vytvárať priestor na participáciu, koordináciu a kooperáciu občianskej spoločnosti, súkromného sektora a akademickej obce na plánovaní, príprave, implementácii a vyhodnocovaní verejných politík (1).

Medzinárodný prístup

Je dôležité sledovať, diskutovať, aktívne sa zapájať do formulovania politík na úrovni EÚ a NATO a harmonizovať s nimi aktivity na národnej úrovni.

SR potrebuje efektívne využívať multiplikačný potenciál členstva pre zdieľanie informácií, výmenu poznatkov, preberanie skúseností a čo je najdôležitejšie, formovanie strategických politík tam, kde nedisponuje dostačujúcimi vlastnými kompetenciami a mocenskou váhou.

(1) V tomto ohľade je však namieste obozretnosť, keďže druhý a tretí sektor sa môže stať samotnou platformou pre hybridné pôsobenie nepriateľských aktérov.

BUDOVANIE ODOLNOSTI

Nevyhnutnou podmienkou odolného štátu a spoločnosti je dobrá správa vecí verejných. Tá sama o sebe znižuje mieru zraniteľnosti, napomáha spoločenskej kohézii a zvyšuje dôveru občanov v štát a jeho inštitúcie.

Na všeobecnej úrovni teda nie je budovanie odolnosti ničím iným, ako dobrým vládnutím so silným akcentom na celospoločenský prístup, transparentnosť a strategické formovanie verejných politík.

V užšom bezpečnostnom kontexte je debata o odolnosti voči hybridným hrozbách súčasťou širšej debaty o adaptácii bezpečnostného systému ako takého. Tá by mala byť realizovaná v súlade s princípmi celovládneho, celospoločenského a medzinárodného prístupu.

Žiadúcim počiatočným bodom systematického budovania odolnosti je vypracovanie ratingu zraniteľnosti všetkých identifikovaných domén hybridného pôsobenia. Túto úlohu by mal definovať pripravovaný Akčný plán v podobe metodickej, pravidelne opakovanej identifikácie a zhodnotenia zraniteľností a slabých miest u subjektov kritického významu, ktoré svojou pôsobnosťou spadajú do hybridných domén.

Prvé ratingy by mali taktiež zahŕňať právnu analýzu nástrojov a kompetencií zapojených orgánov štátnej správy.

Vhodná metodika ratingu musí byť spoločným produktom úsilia gestorov, spolugestorov a odborného zapojenia spravodajských služieb (2). Aplikácia metodiky a vykonanie ratingu by mali byť koordinované gestormi domén.

Výsledky prvých ratingov zraniteľnosti môžu gestorom domén poslúžiť ako analytický základ rozpracovania širokých doménových stratégií budovania odolnosti. Tie si následne spolugestori rozpracujú do vlastných tematicky špecifických akčných plánov budovania odolnosti.

Opakovanie ratingu v pravidelných dvoj- alebo trojročných intervaloch umožní hodnotiť efektívnosť implementácie opatrení a progres v budovaní odolnosti.

(2) Príprava metodiky pre realizáciu ratingu zraniteľnosti je úsilím, ktoré nájde svoje využitie aj pri zlepšovaní detekcie hybridných hrozieb. V prvom kroku bude potrebné za zapojenia celospoločenského rámca aktérov identifikovať slabé miesta a kritické zraniteľnosti pre každú doménu. V druhom kroku spravodajské služby a vybrané pracoviská bezpečnostných inštitúcií vypracujú analýzu predpokladaných cieľov, schopností a nástrojov protivníkov využívajúcich hybridné pôsobenie. V treťom roku je potrebné z prieniku zraniteľností a predpokladaného pôsobenia definovať set doménovo špecifických indikátorov hybridných hrozieb. Ich zjednodušením vznikne jednoduchá metodika detekcie pre potreby poverených pracovísk štátnej správy.

PRAHY REAKCIE

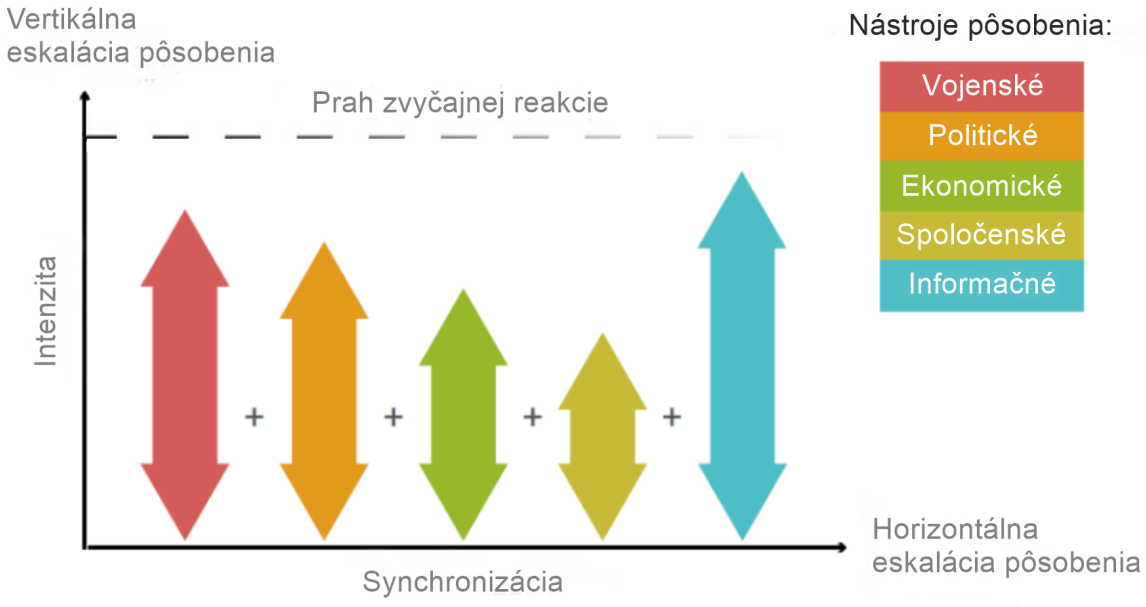
Hybridné hrozby sú často realizované tak, aby ich efekt zostával pod prahom zvyčajnej reakcie. To obmedzuje schopnosť cieleného aktéra včas a efektívne reagovať.

Daný stav vzniká z dôvodu náročnej detekcie a komplikovanej atribúcie hybridného pôsobenia. K zníženej schopnosti reagovať prispieva taktiež konvenčné zmýšľanie o bezpečnosti, ktoré kladie dôraz na vojenské hrozby.

Uvažovanie o nepriateľskom použití politických, ekonomických, spoločenských, informačných nástrojov a ich kombinácií nie je tak vžité. To v praxi často znamená, že pre nevojenské hrozby neexistujú zaužívané reakcie, čo, prirodzene, znemožňuje identifikáciu ich prahov.

Pre zefektívnenie reakčnej schopnosti na nepriateľské pôsobenie štát potrebuje sformulovať metodológiu na identifikáciu prahu reakcie na nevojenské nástroje a rozšíriť vlastnú senzitivitu voči formám vojenských nástrojov.

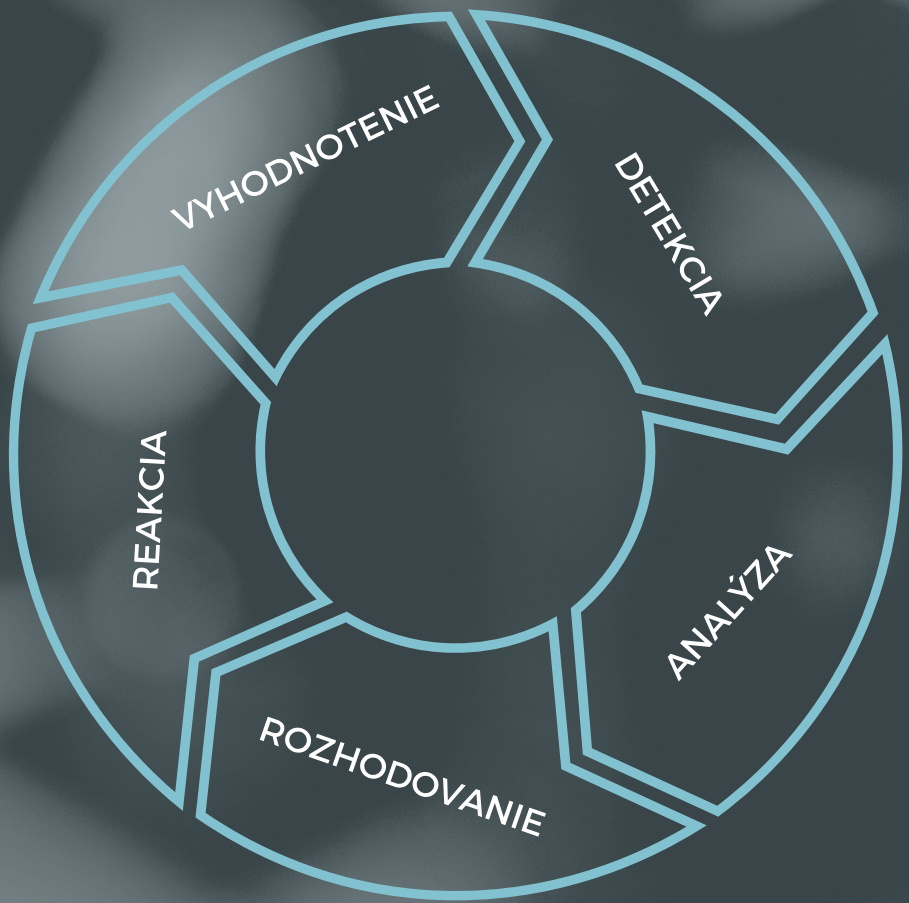
Pri identifikácii prahov je potrebné zohľadniť možné synergické efekty hybridného pôsobenia. Horizontálna eskalácia hybridného pôsobenia, a teda kombinácia rôznych nástrojov môže vytvoriť závažnú hrozbu tam, kde jej izolované prvky žiadnu hrozbu nepredstavujú.



Obr. 2: Synchronizácia horizontálneho a vertikálneho pôsobenia typického pre hybridné hrozby. Modifikované autorom. Originál prebraný z MCDC Countering Hybrid Warfare Project

CYKLUS DARAV

Základné úlohy pre ústredné orgány štátnej správy pre boj s hybridnými hrozbami tak, ako ich formuluje Koncepcia, sú náplňou **detekcie – analýzy – rozhodovania – akcie – vyhodnocovania**. Tieto funkcie prepojené do procesného cyklu tvoria základ schopnosti štátu reagovať na hybridné hrozby.



Detekcia:

Detekcia by mala prebiehať v rovine monitoringu indikátorov a v rovine rozpoznávania anomálií.

V prípade hybridných hrozieb je žiadúce rozšírenie tradičných indikátorov sledovaných spravodajskými službami a ďalšími analytickými centrami o set špecifických indikátorov hybridného pôsobenia pre jednotlivé domény.

Rozpoznávanie anomálií je výzvou odhaľovať nepredvídateľné fenomény, tzv. unknown unknowns.

Dnes systematická detekcia hybridného pôsobenia spadá primárne do kompetencií spravodajských služieb. Pri úvahách o zlepšení funkcie detekcie a schopnosti identifikovať hybridné pôsobenie možno postupovať dvoma smermi:

- **Rozšírenie aktérov detekcie** (zapojenie identifikovaných a ďalším zadaním poverených útvarov ÚO SŠ, krajov a obcí);

- **Rozšírenie poľa detekcie** (rozpracovanie a implementácia špecifických indikátorov pre potreby spravodajských služieb)

Analýza

V kontexte hybridných hrozieb je pre analýzu kľúčová schopnosť zlučovať rôznorodé vstupy do kontextualizovaných produktov schopných odhaliť synchronizáciu či prepojenia rozličných prejavov horizontálneho hybridného pôsobenia.

Primárnym nositeľom funkcie analýzy je NBAC ako analytické, komunikačné a kooperačné medzirezortné pracovisko Slovenskej informačnej služby (ďalej len „SIS“) celoštátnej pôsobnosti, ktoré je pre analýzu najviac povolaným.

Do jeho činnosti medzi inými prispieva aj SITCEN, a to sprostredkovaním produktov únijného Hybrid Fusion Cell a ďalších vstupov z úrovne EÚ a NATO.

Rozhodovanie

Rozhodovanie prebieha v rovine zhodnotenia, či bol dosiahnutý prah reakcie, a teda či štát bude alebo nebude reagovať.

V prípade rozhodnutia, že sa reagovať bude, je ďalším krokom rozhodnutie o špecifikácii reakcie.

Rozhodovanie o „nereakcii", reakcii a špecifikácii reakcie by malo byť vždy realizované s ohľadom na základný strategický rámec boja s hybridnými hrozbami.

V prípade zásadnej eskalácie a dosiahnutia zodpovedajúceho prahu reakcie bude rozhodovaciu funkciu plniť vláda SR ako kolektívny orgán.

V prípade obmedzenej eskalácie či nízkej úrovne hrozby je predstaviteľné, že by rozhodovaciu funkciu plnili gestori domén v koordinácii s dotknutými štatutármi ÚO ŠS.

Akcia

Do množiny akcie spadajú súhrnne všetky opatrenia a kroky podniknuté ako výsledok rozhodovacieho procesu v reakcii na prítomnosť hybridnej hrozby.

Môže sa jednať o akcie smerom do vnútra, typicky posilňovanie odolnosti, akcie cielené na pôvodcu hybridnej hrozby či akcie na medzinárodné spoločenstvo.

V závislosti od konkrétnych opatrení a krokov funkciu akcie môže plniť definované orgány štátnej správy.

Vyhodnotenie

Záverečné vyhodnotenie je prvkom spätnej väzby pre priebeh predchádzajúcich funkcií cyklu.

Nemožno univerzálne špecifikovať aktérov zodpovedných za vyhodnotenie. Schopnosť spätného vyhodnotenia a spracovania tzv. lessons learned by mala byť dobrou praxou organizačnej kultúry všetkých zapojených aktérov.

SWOT ANALÝZA

Analýza silných stránok, slabých stránok, príležitostí a hrozieb je základom efektívneho strategického plánovania. Integruje a vyhodnocuje získané poznatky, ktoré ďalej slúžia pre formuláciu dlhodobých plánov vývoja.

VNÚTORNÉ PROSTREDIE

Silné stránky

- Obnova zahranično-politického konsenzu na úrovni ústavných činiteľov.
- Sformulovanie istého politického záväzku a záujmu zaoberať sa hybridnými hrozbami v programovom vyhlásení vlády.
- Zdieľané povedomie o problematike hybridných hrozieb u tzv. hybridnej leading group (3).
- Zárodky dedikovaných pracovných štruktúr u tzv. hybridnej leading group.
- Osvedčenie sa NBAC ako medzirezortného analytického, komunikačného a koordinačného pracoviska operačnej úrovne, majúceho potenciál plniť funkciu národného fusion cell pre hybridné hrozby.

Slabé stránky

- Roztrieštenosť bezpečnostného systému a dvojkoľajnosť jeho procesov.
- Absencia lídra v agende hybridných hrozieb na politickej i operačnej úrovni.
- Absencia konsenzu v prístupe k hybridným hrozbám u tzv. hybridnej leading group a absencia zapojenia Ministerstva vnútra SR.
- Kritický nedostatok personálno-odborného a materiálno-technického zabezpečenia naprieč ÚO ŠS.
- Politickým nezáujmom izolovaná a marginalizovaná Kancelária bezpečnostnej rady a SITCEN.
- Slabá až absentujúca diskusia o strategickom plánovaní, tvorbe politík budovania odolnosti či strategickej komunikácii.

(3) Ministerstvo obrany SR, Ministerstvo zahraničných vecí a európskych záležitostí SR, Národný bezpečnostný úrad, SIS, Vojenské spravodajstvo, Kancelária bezpečnostnej rady, SITCEN.

VONKAJŠIE PROSTREDIE

Príležitosti

- Iniciatívne formovanie prebiehajúcej debaty o regulácii sociálnych sietí a boji proti dezinformáciám na úrovni EÚ skrz silné národné stanoviská k Digital Services Act (DSA) a European Democracy Action Plan (EDAP).

- Nízkonákladové zintenzívnenie komunikačnej prítomnosti štátu v online priestore a na sociálnych sieťach.

- Fond obnovy ako zdroj finančných prostriedkov pre adaptáciu štátnej správy v zmysle potrieb boja s hybridnými hrozbami.

- Trend rozvíjania celospoločenského prístupu skrz širokú, intenzívnu a systematickú spoluprácu štátu so súkromným sektorom, občianskou spoločnosťou a akademickou obcou.

- Prístup k zdieľaniu informácií o hybridných hrozbách a možnosti čerpať zo zahraničnej expertízy skrz platformy a mechanizmy na úrovni EÚ a NATO.

Hrozby

- Preukázateľná existencia štátnych i neštátnych aktérov, ktorí vnímajú NATO a EÚ ako oponentov a využívajú hybridné nástroje na presadzovanie vplyvu.

- Cielené využívanie slabých miest inherentne vlastných otvoreným, demokratickým spoločnostiam zo strany hybridne pôsobiacich aktérov.

- Rýchle tempo technologického progresu kontinuálne vytvárajúce nové zraniteľnosti naprieč doménami hybridného pôsobenia.

- Neochota technologických gigantov seriózne sa zaoberať šírením dezinformácií na ich platformách.

ZHODNOTENIE

Aktuálny stav prístupu SR s hybridnými hrozbami možno charakterizovať ako spejúci k záveru svojej formatívnej fázy.

Základné povedomie o problematike umožňuje diskusiu sústredenú na otázky identifikácie inštitucionálnych aktérov, ich úloh, nastavenia procesov a informačných tokov.

Tento základ vymedzila Koncepcia, ktorá pomerne uspokojivo zadefinovala základný inštitucionálny rámec a vstupnú sadu úloh. V obmedzenej miere a nie príliš konkrétne sa Koncepcia vyjadruje taktiež k možnostiam zvyšovania odolnosti voči hybridným hrozbám.

Koncepcia neidentifikovala koordinačného gestora ďalšieho rozvoja boja s hybridnými hrozbami – ide o stále otvorenú otázku a bez jej vyriešenia nebude možné uspokojivo uzavrieť formatívnu fázu prístupu SR k boju s hybridnými hrozbami.

K uspokojivému plneniu úloh zadaných koncepciou dochádza na úrovni SITCEN a NBAC. Pre sfunkčnenie plnenia úloh ostatných štátnych orgánov sa začal zadaním PVV SR 2020-2024 v priebežnej koordinačnej gescii Ministerstva obrany SR pripravovať Akčný plán.

Ten by mal určiť koordinačného gestora, ideálne s pôsobnosťou na nadrezortnej úrovni tak, aby boli v maximálnej miere využití už existujúci aktéri a prvky bezpečnostného systému a nedochádzalo k jeho ďalšiemu trieštеniu.

Ďalšou identifikovanou potrebou je zásadné zlepšenie v oblasti detekcie hybridného pôsobenia, k čomu je potrebné pristúpiť v dvoch rovinách.

Prvou je prehĺbenie spôsobilostí spravodajských služieb, ktoré dnes plnia primárne úlohy detekcie. V druhej rovine ide o rozšírene aktérov zapojených do detekcie o ďalšie príslušné útvary ÚO ŠS, krajov a obcí.

To dnes naráža na prekážky ako chýbajúce povedomie o problematike mimo hybridnú leading group, absencia funkčnej metodiky detekcie, chýbajúce organizačné štruktúry u zainteresovaných inštitúcií či nedostatok technicko-materiálneho a personálne-odborného zabezpečenia.

Bez posilnenia personálnych a finančných kapacít, zavedenia systematického vzdelávania a osvety v štátnej správe a vypracovania metodických materiálov detekcie nebude v tejto oblasti možný ďalší progres.

Ďalší rozvoj prístupu SR v boji proti hybridným hrozbám by mal byť určený výstupmi ratingu zraniteľnosti jednotlivých domén (4).

Ratingy pomôžu identifikovať medzery v kompetenciách či dostatočnosti právnych nástrojov a následne určiť priority stratégií a akčných plánov budovania odolnosti voči hybridnému pôsobeniu.

Napokon, viac ako cenným zdrojom informácií a skúseností by pre SR malo byť členstvo v Hybrid CoE a StratCom CoE, z ktorých by mal štát čerpať v maximálnej miere.

Vhodným rozšírením by bolo aj zapojenie SR do štruktúr Osobitnej skupiny pre strategickú komunikáciu pre východ, ktorá je súčasťou Európskej služby pre vonkajšiu činnosť. Ide o hlavné operatívne nástroje EÚ pre analýzu dezinformácií.

Slovenský zástupca či zástupkyňa v Osobitnej skupine by mohol byť zdrojom odborných znalostí v oblasti boja s dezinformáciami z najvyšších úrovní únijnej politiky.

(4) Ratingy zraniteľnosti môžu do určitej miery nahradiť vykonanie auditu bezpečnostného systému a tým prispieť k adresnejšiemu formulovaniu požiadaviek na jeho adaptáciu.

ODPORÚČANIA A NÁVRH MODELU

Na základe zistení realizovaného výskumu v tejto kapitole bola sformulovaná sada odporúčaní a návrh inštitucionálneho modelu pre boj SR s hybridnými hrozbami.

Cieľom je pomenovať optimálny stav, navrhnúť sadu konkrétnych opatrení a časového rámca pre dosiahnutie toho, čo môže byť vnímané ako ideálny prístup SR k boju s hybridnými hrozbami.

Odporúčania sú rozdelené do troch kategórií podľa logickej súslednosti odporúčaní a potreby rozfázovania ich implementácie: **okamžité odporúčania, odporúčania pre Akčný plán a strategické odporúčania.**

OKAMŽITÉ ODPORÚČANIA

1 Organizačné preradenie Kancelárie bezpečnostnej rady (ďalej len „KBR“) zo Sekcie prevencie korupcie a krízového manažmentu priamo pod Kanceláriu predsedu vlády SR.

2 Špecifikácia a urýchlené naplnenie personálnych a technicko-materiálnych potrieb KBR a SITCEN tak, aby obe entity mohli plniť svoje aktuálne a nové úlohy v plnom rozsahu. Obsadenie pozície riaditeľa KBR apolitickou, odborne nespochybniteľnou autoritou, a to v čo najkratšom čase.

3 Rozšírenie pôsobnosti SITCEN o pracovisko alebo tím sústredený na strategické výhľady, analýzu trendov a dlhodobý vývoj. Adresátmi ich produktov by mal byť čo najširší okruh aktérov participujúcich na bezpečnostnom systéme, minimálne ale členovia Bezpečnostnej rady, gestori hybridných domén a NBAC.

4 Zavedenie pravidelného neutajovaného analytického monitoringu v gestorstve KBR za plného zapojenia SITCEN. Výstupy budú ponúkať prehľad trendov v oblasti hybridných hrozieb a dezinformácií v minimálnej cirkulácii pre gestorov a spolugestorov hybridných domén. Účelom je budovanie zdieľaného informačného základu a povedomia o hybridných hrozbách v štátnej správe.

5 Zintenzívnené zapojenie Ministerstva vnútra SR do prípravy a plánovania boja s hybridnými hrozbami, ktoré je prirodzeným držiteľom širokej agendy a kompetencií zasahujúcich do viacerých hybridných domén. Ministerstvo si musí určiť alebo ideálne vytvoriť novú štruktúru, ktorá bude interne koordinovať boj s hybridnými hrozbami a zastupovať rezort v tejto oblasti navonok.

6 Bližšie preskúmanie možnosti čerpania finančných prostriedkov z Fondu obnovy EÚ za účelom adaptácie bezpečnostného systému SR a štátnej správy ako takej k budovaniu odolnosti a celospoločenského prístupu k správe vecí verejných.

7 Aktívna verejná komunikácia pre budovanie spoločenskej dôvery v štátne inštitúcie. SIS a Vojenské spravodajstvo by mali rozšíriť verejné časti svojich výročných správ a nevyhýbať sa iným formám verejnej komunikácie. Zriadenie profilov na sociálnych sieťach či mediálne vystúpenia riaditeľa SIS sú kroky správnym smerom.

ODPORÚČANIA PRE AKČNÝ PLÁN

1 Určenie KBR ako vedúceho koordinačného gestora Akčného plánu a ďalšieho boja s hybridnými hrozbami vo všeobecnosti. Špecifickou úlohou je súbežné kompetečné posilnenie KBR a štatútu SITCEN pre plnenie úloh vyplývajúcich z koordinačného gestorstva boja proti hybridným hrozbám v plnom rozsahu.

2 Zriadenie Centra strategickej komunikácie na Úrade vlády SR (ďalej len „ÚV SR“) ako samostatného pracoviska či rozšírenie pôsobnosti tlačového a informačného odboru ÚV SR s adekvátnym posilnením personálneho a technicko-materiálneho zabezpečenia. Prvou úlohou Centra by mala byť príprava koncepcia strategickej komunikácie, ktorá by zadefinovala východiskový rámec, zapojených aktérov, ich úlohy a ciele strategickej komunikácie SR.

3 Realizácia dôkladného mappingu relevantných aktérov a subjektov s pôsobnosťou v ich doméne. Mapping by mal zahŕňať subjekty verejnej správy, súkromného sektora, akademickej obce či občianskej spoločnosti. Na úrovni verejnej správy by mal tento mapping identifikovať a priamo určiť špecifické útvary a pracoviská s konkrétnymi zadaniami v boji s hybridnými hrozbami, na úrovni súkromného sektora, akademickej obce a občianskej spoločnosti identifikovať partnerov pre ďalší rozvoj spolupráce.

4 Vypracovanie metodiky ratingu odolnosti hybridných domén ich gestormi. Na základe vypracovanej metodiky je potrebné realizovať rating odolnosti pre jednotlivé domény a podľa jeho záverov sformulovať široké doménové stratégie budovania odolnosti. Ďalšou úlohou pre všetkých gestorov a spolugestorov by malo byť rozpracovanie špecifických akčných plánov budovania odolnosti pre konkrétne inštitúcie či oblasti.

5 Vypracovanie základnej, jednoduchej metodiky detekcie hybridného pôsobenia pre potreby poverených pracovísk štátnej správy jednotlivými gestormi a spolugestormi domén.

6 Vypracovanie a implementácia plánu budovania povedomia, spoločných cvičení, systematického vzdelávania a osvety o hybridných hrozbách pre štátnu správu jednotlivými gestormi a spolugestormi domén.

STRATEGICKÉ ODPORÚČANIA

1 Vytvorenie pozície podpredsedu vlády pre bezpečnostné otázky. Z dlhodobého hľadiska bude potreba silného nadrezortného zastrešenia bezpečnostnej problematiky len rásť. Idúc nad rámec problematiky hybridných hrozieb by účelom tejto funkcie mala byť konsolidácia bezpečnostného systému ako takého skrz efektívnu koordináciu súčinnosti a pripravenosti jeho častí.

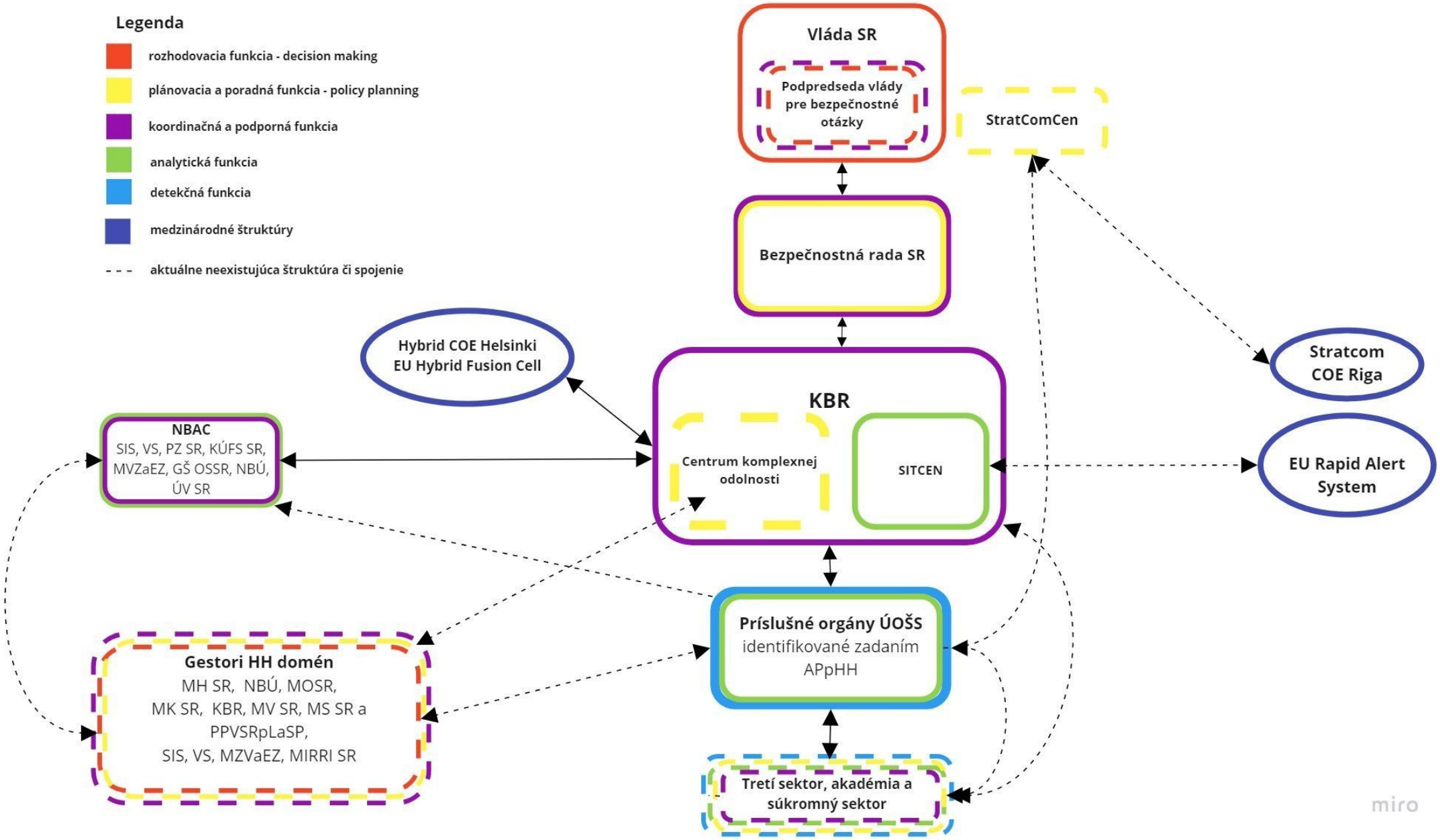
2 Zásadné investície do ľudských zdrojov, bez ktorých sa nezaobíde rozvoj kapacít pre boj s hybridnými hrozbami. Je potrebné vytvoriť záväzný systematický plán rastu tabuľkových miest a personálnych kapacít naprieč štátnou správou pre potreby boja SR s hybridnými hrozbami.

3 Vznik Centra komplexnej odolnosti ako nového dedikovaného pracoviska KBR. Centrum by bolo zásadným rozšírením odborných, poradných a konzultačných kapacít KBR pre nadrezortné plánovanie a prípravu politík a koordináciu ich implementácie. Personálne by malo byť zložené z detašovaných pracovníkov gestorov hybridných domén a kmeňových pracovníkov KBR a SITCEN.

4 Budovanie partnerstiev štátnych inštitúcií v oblasti obrany a bezpečnosti s vysokými školami. Štát by mal prinášať do výuky prvky praxe a aktívne sa spolupodieľať na odbornom formovaní svojich potenciálnych budúcich pracovníkov. Zlepšiť je potrebné aj kontakt so slovenskými študentmi a študentkami v zahraničí. Podpornú úlohu v rozvoji ďalšieho odborného vzdelávania by mali zohrávať aj mimovládne organizácie.

5 Realizácia pravidelných hĺbkových sociologických výskumov v spolupráci so Slovenskou akadémiou vied, univerzitami a odborníkmi z tretieho sektora. Účelom je monitorovanie posunu dôvery v inštitúcie, podpory verejných politík či verejnej mienky ohľadom dezinformačných naratívov a adresnejšie cielenie strategickej komunikácie a informačných kampaní štátu. Do obdobných výskumov by sa SR mala čo najaktívnejšie zapájať aj na medzinárodnej úrovni.

6 Zmena inštitucionálnej kultúry ako zásadný predpoklad pre posun ku komplexnému integrovanému bezpečnostnému systému. SR musí aktívne a systematicky podporovať strategické uvažovanie, zdôrazňovať horizontálnu koordináciu a kooperáciu v rámci štátnej správy prostredníctvom spoločných cvičení či intenzívneho využívania nadrezortných pracovných skupín.



Obr. 3: Posledná fáza návrhu inštitucionálneho modelu boja proti hybridným hrozbám v jeho ideálnej podobe
Zdroj: autor

INŠTITUCIONÁLNY MODEL

Najsilnejším novým prvkom je pozícia podpredsedu vlády pre bezpečnostné otázky. V tejto pozícii je možné vidieť zavŕšenie potreby silnej nadrezortnej koordinácie bezpečnostného systému ako celku.

V užšom kontexte boja proti hybridným hrozbám predstavuje politickú nadstavbu pre odborne-pracovnej úrovni pôsobenia KBR.

KBR sa javí ako entita v ideálnej pozícii prepojiť koordinačnú, odborne-analytickú a konzultačne-poradnú funkciu v jednej štruktúre.

Významnou devízou KBR je taktiež jej nadrezortné postavenie a úzke napojenie na Bezpečnostnú radu SR, ktorá je najvyšším iniciatívnym, poradným a konzultačným orgánom vlády v oblasti bezpečnosti.

Rozvinutie plného potenciálu KBR môže prebiehať v niekoľkých krokoch. V prvej fáze je potrebný presun KBR v organizačnej štruktúre ÚV SR priamo do Kancelárie predsedu vlády.

Rovnako dôležité je obsadenie pozície riaditeľa KBR silnou odbornou autoritou a adekvátne posilnenie celého pracoviska po personálnej aj technicko-materiálnej stránke.

Súčasťou by malo byť aj vytvorenie nového pracovného tímu SITCEN pre strategické výhľady, analýzu trendov a dlhodobého vývoja.

Cieľom druhej fázy je príprava KBR na plné prebratie koordinačného gestorstva pre boj s hybridnými hrozbami. Potrebné bude preskúmať a v prípade potreby adekvátne posilniť kompetencie KBR a štatút SITCEN.

V štruktúre KBR je možné pokračovať rozšírením pracovného tímu pre strategické výhľady na Centrum komplexnej odolnosti. To by popri strategických výhľadoch bolo pracoviskom pre plánovanie, odborný rozvoj a koordináciu politík posilňujúcich odolnosť štátu.

Špecifikom centra by malo byť jeho personálne obsadenie, kde by pracovníkov KBR a SITCEN dopĺňali detašovaní pracovníci zo štruktúr gestorov hybridných domén. Tak je možné zabezpečiť silný medzirezortný charakter Centra pri zachovaní väzby a kontaktu na materský rezort.

Takéto nastavenie sa javí ako ideálne pre vytvorenie dedikovaného stáleho pracoviska, ktoré systematicky operuje s kombinovanými vstupmi od orgánov štátnej správy.

Ďalším novým prvkom je Centrum strategickej komunikácie, ktoré by malo vzniknúť buď rozšírením pôsobnosti Tlačového a informačného odboru ÚV SR alebo ako nová organizačná štruktúra Kancelárie predsedu vlády.

Úlohou centra by malo byť vypracovanie národnej koncepcie strategickej komunikácie, nastavovanie východiskových komunikačných rámcov a naratívov, koordinácia a podpora nadrezortných komunikačných kampaní či vyhodnocovanie implementácie úloh vyplývajúcich z koncepcie strategickej komunikácie a jej variantov na rezortnej úrovni.

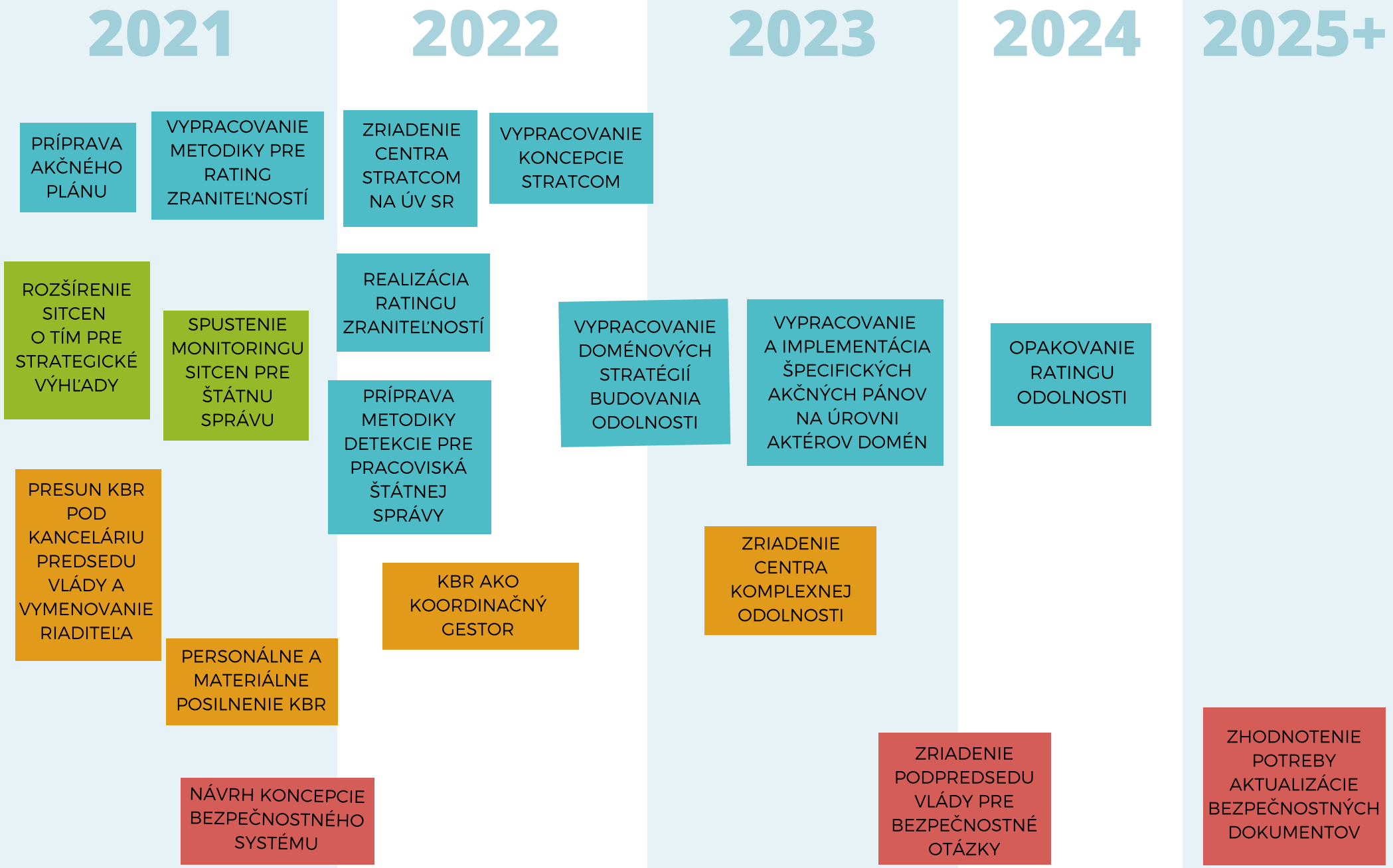
Je taktiež potrebné zmieniť gestorov hybridných domén, ktorých identifikáciu predpokladá Akčný plán.

Tento dokument by mal presne zadefinovať, aké orgány štátnej správy budú plniť gestorskú funkciu, ale aj rozsah stanovených úloh a termíny ich plnenia.

Gestori by mali ďalej dohliadať a asistovať pri plnení úloh, realizovať mapping aktérov a rating odolnosti v rámci vlastných domén.

Staronovým prvkom je tretí sektor, akadémia a súkromný sektor, ktorého zapojeniu do boja s hybridnými hrozbami je potrebné prisúdiť väčšiu váhu a dôraz.

Okrem prirodzenej participácie na budovaní odolnosti sa priestor na zapojenie javí v jednotlivých dázach DARAV cyklu, kde však bude žiadúci silne individuálny a špecifický prístup.



Obr. 3: Navrhovaná časová os prijatých opatrení
Zdroj: autor

ZDROJE

LP/2018/133 Koncepcia pre boj Slovenskej republiky proti hybridným hrozbám. https://www.slov-lex.sk/legislativne-procesy/SK/LP/2018/133

LP/2020/507 Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám. https://www.slov-lex.sk/legislativne-procesy/SK/LP/2020/507

LP/2020/590 Návrh Bezpečnostnej stratégie Slovenskej republiky. https://www.slov-lex.sk/legislativne-procesy/SK/LP/2020/590

LP/2020/592 Návrh Obrannej stratégie Slovenskej republiky. https://www.slov-lex.sk/legislativne-procesy/SK/LP/2020/592

MCDC Countering Hybrid Warfare Project. Countering Hybrid Warfare. 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Programové vyhlásenie vlády Slovenskej republiky na obdobie rokov 2020-2024. https://www.mpsr.sk/download.php?fID=18769