Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **6**
Číslo/Number: **1**
Rok/Year: **2023**

Iniciatíva a opatrenia prijaté zo strany Slovenskej republiky na účely zabránenia šíreniu a negatívnym dôsledkom hybridných hrozieb

Initiatives and measures taken by the Slovak Republic to prevent the spread and negative consequences of hybrid threats

pplk. doc. JUDr. Monika Hullová, PhD.
Akadémia Policajného zboru v Bratislave, Katedra kriminálnej polície

Anotácia

Autorka v prehľadovej vedeckej štúdii analyzuje kroky, ktoré boli podniknuté zo strany SR na úseku zabránenia šíreniu a negatívnym dôsledkom hybridných hrozieb od roku 2016 po súčasnosť, resp. aj v kontexte budúcich trendov a vízií. Hybridné hrozby ako nový spôsob pôsobenia určitých subjektov sa stal problémom, ktorému musia čeliť všetky štáty sveta. Aj z toho dôvodu boli podniknuté viaceré kroky na medzinárodnej a národnej úrovni, ktorých cieľom je vytvoriť optimálny legislatívno-inštitucionálny rámec pre elimináciu tohto nežiadúceho bezpečnostného javu. Cieľom autorky bolo, na základe širokého spektra analytických metód, posúdiť postupnosť a koherenciu týchto krokov v kontexte identifikovaných potrieb spoločenskej praxe.

Annotation

The author analyses the steps taken by the Slovak Republic in the field of preventing the spread and negative consequences of hybrid threats from 2016 to the present, or even in the context of future trends and visions. Hybrid threats as a new way of action of certain entities has become a problem that all states of the world have to face. For this reason, too, several steps have been taken at the international and national level to create an optimal legislative and institutional framework for the elimination of this undesirable security phenomenon. The aim of the author was, on the basis of a wide range of analytical methods, to assess the sequence and coherence of these steps in the context of the identified needs of social practice.

Kľúčové slová

hybridná hrozba, koncepcia, stratégia, bezpečnostná stratégia, obranná stratégia, akčný plán, kybernetická bezpečnosť, bezpečnostné prostredie, bezpečnostný systém, riadenie rizík, krízová situácia

Keywords

hybrid threat, concept, strategy, security strategy, defence strategy, action plan, cyber security, security environment, security system, risk management, crisis situation

Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **6**
Číslo/Number: **1**
Rok/Year: **2023**

Úvod

Napriek tomu, že na *„hybridné hrozby“* sa spoločnosť často pozerá v kontexte prebiehajúceho vojenského konfliktu na Ukrajine, prípadne vo vzťahu k tzv. *„ISIL/Da'esh“* alebo Islamského štátu, tento novodobý negatívny jav je potrebné vnímať v širších (aj historických) súvislostiach.[1] Z toho najvšeobecnejšieho, filozofického pohľadu, možno povedať, že hybridné hrozby vo svojej podstate búrajú pomyselné hranice medzi vojnou a mierom, medzi bojujúcimi a nebojujúcimi (angl. *„combatants and non-combatants“*), medzi letálnymi a neletálnymi spôsobmi vedenia boja. Ide o metaforické pomenovanie, ktoré reflektuje na novodobé globálne zmeny v bezpečnostnom prostredí. Napriek tomu, že je ich pomerne náročné s určitosťou vymedziť, bezo sporu predstavujú enormné a dovolíme si povedať, že aj globálne bezpečnostné riziká. Mnoho odborníkov opodstatnene poukazuje na vágnosť ich pojmového vymedzenia, heterogénnosť, asymetrickosť či neregulárnosť a za určitých okolností aj nepredvídateľnosť z pohľadu ich štruktúry a obsahu (osobitne v tomto ohľade – ich motívov, cieľov, použitých nástrojov, aktérov, prejavov a dôsledkov). V posledných rokoch tu registrujeme permanentnú expanziu týchto rizík, ktorá sa prejavuje nielen v kvantitatívnom, ale predovšetkým kvalitatívnom význame (narastajúca rýchlosť, škála, intenzita pôsobenia hybridných hrozieb). Aj tieto skutočnosti opodstatnene vyvolávajú potrebu ich hlbšieho vedeckého skúmania a stali sa aj pre nás v určitom zmysle výzvou, výzvou ktorá plne inhibuje náš záujem a stala sa reálnym objektom a predmetom našej výskumnej činnosti.[2]

Na základe výstupov z rešerše odbornej literatúry sme dospeli k záveru, že v podmienkach SR sa s týmto pojmom po formálnej stránke prvýkrát stretávame v *„Bielej knihe o obrane SR“* (2016), ktorý sa následne premietol do *„Koncepcie pre boj SR proti hybridným hrozbám“* (2018), ***„Programového vyhlásenia vlády*** *SR pre roky 2021 – 2024“, „Koordinovaného mechanizmu odolnosti SR voči informačným operáciám“* (2020), *„Bezpečnostnej stratégie SR“* (2021), *„Obrannej stratégie SR“* (2021), *„Národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025“, „Akčného plánu realizácie: Národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025“, „Akčného plánu koordinácie boja proti hybridným hrozbám“* (2022 – 2024), *„Koncepcie bezpečnostného systému SR“* (2022) a *„Národnej stratégie riadenia rizík bezpečnostných hrozieb SR“* (2022 – 2032).

Na túto realitu sme sa rozhodli reagovať tak, že realizujeme účelovú analýzu týchto dokumentov. Naším cieľom v predkladanej prehľadovej vedeckej štúdii je komplexná analýza vynaloženej iniciatívy a opatrení prijatých zo strany SR na účely zabránenia a šíreniu hybridných hrozieb. Pri napĺňaní tejto ambície sme dominantne využili metódy obsahovej analýzy, historickej (retrospektívnej) analýzy, kauzálnej analýzy a tzv. problémovej analýzy.

Výsledky analýzy dokumentov reglementujúcich problematiku hybridných hrozieb v podmienkach SR

Biela kniha o obrane SR

Reagujúc na zhoršujúci sa stav v oblasti obrany štátu, vláda SR schválila v roku 2013 dokument s názvom *„Biela kniha o obrane Slovenskej republiky“.* Tento dokument definoval projekciu dlhodobého rozvoja garancie obrany štátu v časovom horizonte do roku 2024. Reflektujúc na zmeny v globálnej bezpečnostnej situácii, bolo nevyhnutné vykonať revíziu obrannej politiky štátu a jej ďalšie smerovanie

s výhľadom do roku 2030. Výsledkom tohto procesu bola revidovaná Biela kniha o obrane SR, ktorá bola schválená vládou SR uznesením č. 433 z 28. septembra 2016. V bode 55. tohto dokumentu sú medzi vážne bezpečnostné hrozby z hľadiska spôsobu vedenia konfliktov v meniacom sa bezpečnostnom prostredí subsumované *„… najmä propaganda na strategickej úrovni ako súčasť informačného a psychologického pôsobenia na vybrané cieľové skupiny spoločnosti v rámci tzv. informačnej vojny a špecifické operačné postupy, ktoré sú najlepšie charakterizované pojmom „hybridný spôsob vedenia bojových činností“. Propaganda na strategickej úrovni je jedným z pilierov konceptu tzv. permanentnej vojny.“*[3]

Koncepcia pre boj SR proti hybridným hrozbám

Podľa tohto strategického dokumentu (ďalej len *„koncepcia“*)[4] sú v bezpečnostnom prostredí SR evidované viaceré prejavy hrozieb, ktoré možno označiť prívlastkom hybridné. 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.“*[5]

Medzi tie najrelevantnejšie indikátory bezpečnostných hrozieb 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.[6]

Na margo uvedených indikátorov je potrebné uviesť niekoľko, aj kritických pripomienok. Uvedené spektrum prejavov nie je komplexné, chýbajú v ňom niektoré aspekty, napr. strategická korupcia, aktivity polovojenských a extrémistických skupín, ovplyvňovanie volebných procesov. Na druhej strane kvitujeme, že indikátory nie je možné vnímať izolovane, ale v kontexte s ostatnými prejavmi, ktoré je potrebné podrobiť dôkladnej korelačnej a kauzálnej analýze (príčina – následok javu).

V slovenských médiách a na sociálnych sieťach registrujeme rôzne propagandistické kampane šíriace dezinformácie o ekonomických a politických problémoch vyplývajúcich z členstva v NATO a EÚ (*napr.*

strata suverenity štátu v prospech nadnárodného celku, ktorá sa okrem iného prejavuje v tom, že nemáme možnosť rozhodovať o podstatných záležitostiach; ekonomické, vojenské a politické dôsledky takéhoto spojenectva, ktoré prinášajú skôr nevýhody a straty než benefity; zapájanie sa do vojnových konfliktov a vojnových operácií, v dôsledku čoho vystavujeme krajinu nebezpečenstvu a oslabujeme vlastnú obranyschopnosť prípadne sa dostávame do pozície, kedy dochádza k zneužitiu našej energetickej závislosti). Evidujeme propagandistické kampane šíriace dezinformácie o neschopnosti štátu (vlády) riešiť politické, ekonomické, kultúrne a sociálne problémy (*napr. energetickú krízu, utečeneckú a migračnú krízu, pandemickú situáciu*) a propagandistické kampane šíriace dezinformácie o polemickej ústavnosti, zákonnosti a demokratickosti štátu (*napr. spochybňovanie kredibility, dôveryhodnosti a objektivity štátnych orgánov a inštitúcií, ako aj verejných či štátnych predstaviteľov, poukazovaním na údajnú korupciu v politike a verejnej správe, na zasahovanie do nezávislosti a nestrannosti súdov, prokuratúry a polície; na zneužívanie právomocí verejných činiteľov, či na zasahovanie do volebných procesov*). Potenciál hybridnej hrozby nesú informácie prezentované v slovenských médiách a na sociálnych sieťach, ktorými sú propagované domáce radikálne organizácie *(napr. ktoré šíria rasovú, etnickú, náboženskú, kultúrnu, politickú a inú neznášanlivosť, netoleranciu, nacionalistické, ultranacionalistické, izolacionistické, anarchické, komunistické, destabilizačné myšlienky a ideový fanatizmus*), prípadne sú takéto hnutia rôznym spôsobom podporované. Podľa správy o bezpečnosti SR za rok 2021, na bezpečnostné prostredie nášho štátu mal vplyv kontinuálny nárast hybridných aktivít a vplyvových operácií, ktoré vykonávali subjekty tzv. *„antisystémového a antidemokratického spektra, štátne a neštátne subjekty naviazané na cudzích štátnych aktérov za využitia širokospektrálnej a podprahovej formy prostredníctvom rôznych komunikačných a informačných sietí“.*

Aj z týchto dôvodov bola, za účelom identifikácie hoaxov a eliminácie ich vplyvu v online priestore, zriadená špecializovaná oficiálna stránka Policajného zboru (ďalej len *„PZ“*) s názvom *„Hoaxy a podvody – Polícia SR“*. Súčasťou slovenskej bezpečnostnej scény sú však aj sabotáže a kybernetické útoky adresované na kľúčovú infraštruktúru štátu. Napr. podľa Národného centra kybernetickej bezpečnosti – *„SK-CERT počet detegovaných kybernetických útokov (pozorovaných jednotkami CSIRT a hlásených do SK-CERT) stúpa, pričom v roku 2021 ich bolo najviac zaznamenaných vo verejnej správe. Podľa správy o bezpečnosti SR za rok 2021 bolo v našom kybernetickom priestore nahlásených a detegovaných 42 085 540 incidentov a riešených bolo 3684 incidentov“*.[7]

V týchto intenciách uvádzame, že Národné centrum kybernetickej bezpečnosti NCKB SK-CERT existuje od 1. septembra 2019. Jeho organizačno-inštitucionálnymi predchodcami boli *„SK CSIRC – Slovak Computer Security Incident Response Center“*, ktoré bolo zriadené v máji 2009 a Národná jednotka kybernetickej bezpečnosti SK-CERT alias *„Slovak Computer Emergency Response Team“,* ktorá bola kreovaná v januári 2016. Zriaďovateľom SK-CERT je Národný bezpečnostný úrad ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť. SK-CERT má od marca 2020 postavenie národnej jednotky CSIRT s pôsobnosťou pre SR (*pre doplnenie uvádzame, že na území Slovenska operuje viacero národných CSIRT jednotiek, pričom nie všetky sú medzinárodne akreditované či certifikované*).[8] Útvar zabezpečuje národné a strategické aktivity v oblasti riadenia kybernetickej bezpečnosti, analýz hrozieb, ale aj koordinácie riešenia kybernetických bezpečnostných incidentov na celonárodnej úrovni. Do jeho agendy spadá aj oblasť výuky, vzdelávania, tréningov, ako aj výskumu vo sfére kybernetickej bezpečnosti. Centrum spolupracuje na medzinárodnej úrovni napr. s The CERT Division v rámci

Software Engineering Institute, ENISA – The European Union Agency for Cybersecurity alias Európskou agentúrou pre bezpečnosť sietí a informácií, TF-CSIRT – Trusted Introducer, FIRST – The Forum of Incident Response and Security Teams.[9]

Aj v rámci organizačnej štruktúry PZ bolo na tieto účely zriadené špecializované pracovisko. Ide o odbor počítačovej kriminality Národnej centrály osobitných druhov kriminality Prezídia PZ, ktorého hlavnou náplňou práce je prevencia, odhaľovanie, objasňovanie a vyšetrovanie trestnej činnosti za využitia informačno-komunikačných technológií a trestnej činnosti, ktorej cieľom sú takéto technológie (napr. kybernetické útoky). Okrem toho, agenda kybernetickej bezpečnosti spadá pod oddelenie kybernetickej bezpečnosti v rámci Sekcie informatiky, telekomunikácií a bezpečnosti ministerstva.[10] Problematika hybridných hrozieb je súčasťou agendy Inštitútu správnych a bezpečnostných analýz Ministerstva vnútra SR. Ide o samostatný odborný útvar na úseku všeobecnej analytiky, procesno-organizačných auditov, procesnej architektúry verejnej správy, tvorby a vyhodnocovania politík, akcelerácie zavádzania inovácií, tvorby prognóz, stratégií a implementačných plánov a koordinácie činnosti na úseku boja proti hybridným hrozbám. Pre tento účel bolo kreované Centrum boja proti hybridným hrozbám ISBA-CBHH, ktoré je zodpovedné za identifikáciu hybridných hrozieb, spracovanie analytických, metodických, koncepčných a strategických materiálov, správ a prognóz, ako aj koordináciu aktivít v rámci rezortu. Analogický postup je v tomto smere aplikovaný aj u ostatných ústredných orgánov štátnej správy.[11]

Týmito skutočnosťami sme sa rozhodli zvýrazniť význam koordinácie pre účelovú realizáciu kontroly hybridných hrozieb, ktorá musí korešpondovať s prijatou koncepciou, v ktorej obsahu sú zakomponované legislatívne, organizačno-riadiace a strategicko-taktické opatrenia. Vzhľadom na vyššie uvedené riziká, ktoré plynú z hybridných hrozieb možno jednoznačne odôvodiť potrebu vytvorenia koncepcie, ktorá by komplexne reagovala na situáciu v bezpečnostnom prostredí SR. Sledovaným účelom koncepcie bolo – v prvom rade – zvýšiť povedomie spoločnosti o možnostiach výskytu prejavov hybridných hrozieb a vytvoriť tak predpoklady pre organizačno-inštitucionálny rámec riešenia tejto problematiky. V druhom rade – koncepcia vytvorila podmienky pre optimálne nastavenie mechanizmu výmeny informácií a kooperácie na úseku monitoringu hybridných hrozieb (identifikácia, analýza, vyhodnocovanie).

Koncepcia navrhuje rozčleniť národný inštitucionálny rámec pre riešenie problému hybridných hrozieb do 3 úrovní, a to:

1. národné kontaktné miesto pre hybridné hrozby,
2. národné kooperačné centrum pre hybridné hrozby,
3. štátne orgány.

Národným kontaktným miestom pre hybridné hrozby je podľa koncepcie **Situačné centrum SR** (ďalej len „SITCEN“). Jeho úlohy sú najmä:

1. prijímať a ďalej distribuovať na národnej úrovni produkty Hybrid Fusion Cell –Integrovanej spravodajskej jednotky zameranej proti hybridným hrozbám (ďalej len *„HFC“)*;
2. informovať a zdieľať informácie súvisiace s hybridnými hrozbami s HFC;

3. byť poradcom HFC pre hybridné hrozby, ktoré sa najviac dotýkajú SR;
4. asistovať HFC zabezpečovaním vypracúvania analýz bezpečnostnej situácie relevantnými orgánmi SR pri hodnotení a predpovediach vývoja;
5. aktualizovať svoje kontaktné údaje pre hladký tok informácií;
6. byť pripravený ku kontaktovaniu zo strany HFC v prípade krízovej situácie;
7. zúčastňovať sa stretnutí národných kontaktných bodov (ďalej len *„POCs“*) v Bruseli;
8. zabezpečovať kontaktovanie relevantných osôb v členskej krajine.[12]

Zámer zriadiť SITCEN odsúhlasila vláda SR ešte 4. 6. 2014. Zdôvodnila to tým, že na Slovensku sa nevykonáva komplexné a nepretržité vyhodnocovanie bezpečnostnej situácie na nadrezortnej úrovni. SITCEN ako vládne informačné analytické pracovisko s celoštátnou pôsobnosťou je súčasťou Kancelárie Bezpečnostnej rady SR (ďalej len *„KBR“*). Existuje od januára 2016, pričom k jeho zriadeniu došlo na základe zákona č. 346/2015 Z. z., ktorým sa dopĺňal **zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady SR v čase mieru** v znení zákona č. 319/2012 Z. z. Okrem samotnej KBR, je to práve Bezpečnostná rada SR (ďalej len *„BR SR“*), ktorej hlavnou úlohou je vyhodnocovať bezpečnostnú situáciu v SR a vo svete v čase mieru, a to s využitím informácií SITCEN. Na základe týchto informácií predkladá vláde návrhy opatrení na zníženie alebo odstránenie rizík ohrozenia bezpečnosti SR, ktoré môžu viesť k vzniku krízovej situácie. Pod záštitou BR SR pracujú aj výbory, ktoré sú jej stálymi pracovnými orgánmi. Takýmito výbormi sú napr. aj Výbor pre energetickú bezpečnosť, Výbor pre kybernetickú bezpečnosť, príp. Výbor pre koordináciu spravodajských služieb, ktoré analogicky ako SITCEN plnia úlohy na úseku boja proti hybridným hrozbám.[13] Pre názornejšiu predstavu náplne práce tohto pracoviska uvádzame informácie zo správy o bezpečnosti SR za rok 2021, z ktorých vyplýva, že *„SITCEN v spolupráci s PZ vykonávali monitoring a vyhodnocovanie škodlivých naratívov (v súvislosti s COVID-19) v online priestore a súvisiacich incidentov v reálnom svete v oblasti boja proti dezinformáciám. Okrem toho, SITCEN aj naďalej plnilo úlohy kontaktného bodu pre Európske centrum výnimočnosti na boj proti hybridným hrozbám (The European Centre of Excellence for Countering Hybrid Threats – ďalej len „Hybrid CoE“) a HFC.“*[14]

Na základe uvedeného možno vo všeobecnosti konštatovať, že podstata činnosti SITCEN spočíva v získavaní, vyhodnocovaní a analýze informácií o zmenách v bezpečnostnom prostredí (s dištinkciami v porovnaní so spravodajskými pracoviskami). Výstupným analytickým produktom tejto tvorivej činnosti sú najmä: pravidelná tematická mesačná správa ku konkrétnemu rizikovému javu alebo udalosti s prognózou ďalšieho vývoja, štvrťročná písomná správa o vývoji v identifikovanej krízovej oblasti sveta s tendenciami ďalšieho vývoja situácie, ročná správa o bezpečnosti SR s návrhom opatrení, mimoriadna správa podľa požiadavky vrcholných predstaviteľov štátu alebo pri náhlej zmene bezpečnostného prostredia SR. Na čele tohto národného informačného analytického pracoviska stojí riaditeľ, ktorý za výkon svojej funkcie zodpovedá riaditeľovi KBR. Súčasťami SITCENU sú jej organizačná a analytická časť. Vzhľadom na to, že podstatou tohto vládneho pracoviska je príprava analytických materiálov a ich predkladanie kompetentným adresátom pre ďalšie využitie, v tejto súvislosti je potrebné uviesť, že analytický produkt alebo výstup z analytického produktu nesmú tvoriť spravodajské

informácie získané činnosťou národného kooperačného centra.[15] Je zrejmé, že činnosť SITCENU je dôležitá pre voľbu strategických rozhodnutí v rámci smerovania bezpečnostnej politiky SR, príp. v neskorších etapách aj na operačno-taktickej úrovni. SITCEN sa medzičasom stal aj PoC pre Hybrid CoE a jedným z PoC pre EÚ Rapid Alert System. Z členstva čerpajú slovenskí experti v podobe webinárov, workshopov, vzdelávacích a tréningových aktivít a pod.

Národným kooperačným centrom pre hybridné hrozby je **Národné bezpečnostné analytické centrum** (ďalej len *„NBAC"*). Podľa koncepcie k jeho hlavným úlohám patrí najmä:

1. prijať informáciu ktorejkoľvek zložky štátneho orgánu alebo odôvodnený podnet fyzickej osoby alebo právnickej osoby s podozrením na hybridnú hrozbu a zaradiť ju do procesu vyhodnocovania vytvorením dokumentu NBAC;
2. po vyjadrení štátnych orgánov zastúpených v NBAC v spolupráci so SITCEN doplniť do príslušného dokumentu NBAC súvislosti z pohľadu bezpečnostných záujmov EÚ a NATO a rozhodnúť o potrebe spracovania výstupu pre príjemcov;
3. v spolupráci so SITCEN doplniť súvislosti z pohľadu bezpečnostných záujmov EÚ a NATO a rozhodnúť o potrebe spracovania výstupu pre príjemcov.[16]

NBAC vzniklo 1. 1. 2013 na základe projektu, ktorý schválila vláda SR uznesením č. 75 zo 7. 3. 2012. Iniciátorom projektu a zároveň jeho gestorom bola Slovenská informačná služba. NBAC predstavuje novú formu medzirezortnej organizačnej štruktúry. Je definované ako analytické, komunikačné a kooperačné stredisko Slovenskej informačnej služby s celoštátnou pôsobnosťou v oblasti bezpečnostných rizík (dominantne sa orientuje na identifikáciu hrozieb terorizmu). Hlavnou úlohou NBAC je príprava komplexných analytických hodnotení bezpečnostných incidentov na základe hlásení prijatých od štátnych orgánov SR, monitorovanie bezpečnostnej situácie v SR z odkrytých zdrojov a poskytovanie analytických produktov o bezpečnostných hrozbách určeným adresátom. Na jeho platforme spolupracujú vyslaní zástupcovia Slovenskej informačnej služby, Vojenského spravodajstva, PZ, Kriminálneho úradu Finančnej správy, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, Generálneho štábu Ozbrojených síl SR a Úradu vlády SR.[17] V tejto súvislosti považujeme za potrebné poznamenať, že na to, aby NBAC a SITCEN plnili svoje úlohy adekvátne ich poslaniu, je potrebné zabezpečiť nielen ich formálne postavenie, ale aj personálne a materiálne kapacity (*sme toho názoru, že v súčasnosti tomu tak nie je*).

Úlohy štátnych orgánov na úseku boja proti hybridným hrozbám sú podľa koncepcie nasledovné:

1. prvotne vyhodnocovať nahlásené incidenty vo svojej pôsobnosti vo vzťahu k hybridným hrozbám podľa indikátorov;
2. postupovať informáciu o incidente, ktorý spĺňa niektorý z indikátorov hybridnej hrozby na ďalšie spracovanie, posúdenie alebo vyhodnotenie NBAC;
3. poskytnúť v rámci svojej pôsobnosti NBAC doplňujúce informácie k nahlásenému incidentu, ktoré budú zo strany NBAC vyhodnotené ako hybridná hrozba.[18]

Dôvodom pre takýto postup je fakt, že agenda hybridných hrozieb nie je oficiálne (zákonnou cestou) zverená do výlučnej vecnej pôsobnosti žiadneho štátneho orgánu. V zákone č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení zákona č. 494/2022 Z. z. nie je vymedzená konkrétna zodpovednosť za boj proti hybridným hrozbám, napriek tomu, že vybrané bezpečnostné otázky sú v kompetencii viacerých orgánov štátnej správy, napr. Ministerstva vnútra SR (§ 11), Ministerstva obrany SR (§ 12), Ministerstva spravodlivosti SR (§ 13) a Národného bezpečnostného úradu (§ 34).

Ako sme už zdôraznili vyššie, v rámci hybridných hrozieb, ktoré sú spôsobilé ohroziť základné fungovanie štátnych procesov, oslabiť dôveru občanov v štát alebo narušiť verejný poriadok, je to aj kybernetický priestor, ktorý sa hlavne v posledných desaťročiach stáva ich doménou. Vo vzťahu k tzv. *„kybernetickej bezpečnosti“* možno uviesť, že podľa § 35, ods. 3 tohto zákona, ministerstvá a ostatné ústredné orgány štátnej správy v rozsahu vymedzenej pôsobnosti zodpovedajú za úlohy obrany, kybernetickú bezpečnosť a vytváranie podmienok na realizáciu požiadaviek zabezpečovania príprav na obranu, ochranu kybernetického priestoru.[19] Orgány verejnej moci vykonávajúce svoju pôsobnosť v oblasti kybernetickej bezpečnosti vymedzuje aj zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 231/2022 Z. z., ktorým sa transponovala smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v únii. V zmysle § 4 tohto zákona sú nimi Národný bezpečnostný úrad, jednotlivé ministerstvá, Generálna prokuratúra SR, Najvyšší kontrolný úrad SR, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov SR, Úrad pre reguláciu sieťových odvetví a iné orgány štátnej správy.

Východiskovým, strategickým dokumentom, ktorý komplexne určuje strategický prístup SR k zabezpečeniu kybernetickej bezpečnosti je **Národná stratégia kybernetickej bezpečnosti na roky 2021 – 2025**.[20] Súčasťou národnej stratégie kybernetickej bezpečnosti je **Akčný plán realizácie: Národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025**, v zmysle ktorého sú definované úlohy, určené zodpovedné subjekty[21] a takisto aj časové horizonty pre jednotlivé úlohy. Špecifické postavenie medzi týmito subjektmi má Národný bezpečnostný úrad, ktorý riadi strategické, koncepčné a normotvorné činnosti, je kontaktným bodom pre zahraničie, vrátane medzinárodných organizácií, vedie register základných služieb, register prevádzkovateľov základných služieb, register poskytovateľov digitálnych služieb a vykonáva ďalšie dôležité činnosti a aktivity v oblasti kybernetickej bezpečnosti na národnej úrovni. Okrem toho, na účely monitorovania implementácie akčného plánu je zriadený stály monitorovací výbor.[22] Zo *Správy o kybernetickej bezpečnosti v SR v roku 2021* vyplýva, že tento rok *„… v globálnom kybernetickom priestore znamenal rýchly vývoj možností a spôsobov útokov. Tento trend je pozorovaný kontinuálne už niekoľko rokov a je spôsobený nielen rýchlym vývojom informačných technológií, ale najmä neustále sa zvyšujúcou závislosťou spoločnosti od technológií a služieb v kybernetickom priestore. Útočníci veľmi rýchlo reagujú na zmeny a prispôsobujú sa globálnym trendom, pričom neustále hľadajú nové spôsoby, ako sa dostať k citlivým dátam, finančným prostriedkom alebo ku kontrole nad systémami a službami.“* Z pohľadu globálnych trendov, najzávažnejšou hrozbou bolo šírenie ransomwéru,[23] ale aj expanzia nových foriem phishingu a smishingu.[24] Aj tieto skutočnosti jednoznačne poukazujú na nové hrozby, ktorým musí spoločnosť čeliť na takmer dennej báze. Je

zrejmé, že si to vyžaduje komplexný prístup, ktorého súčasťou je vybudovanie kvalifikovanej infraštruktúry.

Tak ako sme sa to snažili interpretovať vyššie, úlohy na úseku boja proti hybridným hrozbám, kybernetickej kriminalite a kybernetickým útokom musia byť rozdelené medzi celé spektrum subjektov v rámci verejnej (štátnej) správy. Napriek tomu je potrebné uviesť, že koncepcia si nestanovila za cieľ vytvoriť novú inštitúciu, ktorá by komplexne mapovala všetky prejavy hybridných hrozieb (vrátane kybernetických incidentov), nakoľko by to, vzhľadom na ich variabilitu, nebolo ani reálne.

V súlade s koncepciou dotvára organizačno-inštitucionálny rámec riešenia tejto problematiky aj možnosť spolupráce na nadnárodnej úrovni v už spomínanom Hybrid CoE. Pre doplnenie uvádzame, že centrum výnimočnosti zriadilo Fínsko v Helsinkách v apríli 2017 na základe výzvy EÚ adresovanej jej členským štátom. V súčasnosti na tomto projekte spolupracuje 33 členských štátov, EÚ a NATO, vrátane Slovenska, ktoré je jeho členom od augusta 2020. Centrum má 3 základné siete záujmových komunít (tzv. *„The Community of Interest“*), a to: 1. Hybridný vplyv, 2. Zraniteľnosť a odolnosť, 3. Stratégia a obrana. Tieto komunity reprezentujú odborníci z členských krajín, EÚ a NATO. Ich úlohou je multinacionálna a multidisciplinárna výmena osvedčených postupov, skúseností a odborných poznatkov, ako aj vytváranie priestoru pre koordinačné aktivity. Centrum zriadilo aj ďalšie organizačno-štrukturálne jednotky, ktoré plnia parciálne ciele na úseku boja proti hybridným hrozbám. Samotný akademický výskum a odbornú diskusiu na relevantné témy zabezpečuje špecifický výskumný a analytický tím (*The Research and Analysis team*). Okrem toho, úsek vzdelávania a prípravy na prácu s rôznymi scenármi hybridných hrozieb zastrešuje špecializovaný tím (*The Training and Exercises team*).[25]

Programové vyhlásenie vlády SR pre roky 2021 – 2024

Programové vyhlásenie vlády SR na obdobie rokov 2021 – 2024 bolo predložené Národnej rade SR so žiadosťou o vyslovenie dôvery dňa 28. 4. 2021. Vláda sa v tomto deklaratórnom dokumente o. i. zaviazala, že preskúma zvýšenie ochrany záujmov SR prostredníctvom noriem trestného práva pred rizikom hybridných hrozieb, týkajúcich sa najmä šírenia propagandy a dezinformácií, podpory extrémistických zoskupení a kybernetických útokov.

V kontexte meniaceho sa bezpečnostného prostredia, v ktorom vystupujú do popredia silnejúce kybernetické hrozby, hybridné hrozby a dezinformácie, determinované úrovňou technologického rozvoja vrátane umelej inteligencie, bude osobitný dôraz kladený na rozvoj spôsobilostí rezortu ministerstva obrany.

Súčasťou vládnej stratégie boja proti silnejúcim hybridným hrozbám je okrem posilnenia kapacít na celoštátnej úrovni aj aktívna účasť SR na medzinárodnom úsilí pri odvracaní týchto hrozieb, aj vzhľadom na deklarovanú potrebu upevňovania transatlantickej väzby (členstvo v NATO).

Popri tom, vláda vidí priority v príprave akčného plánu na koordináciu boja proti hybridným hrozbám a šíreniu dezinformácií a vo vybudovaní adekvátnych centrálnych kapacít pre jeho realizáciu rešpektujúc pritom premisu: *„Boj proti hybridným hrozbám nesmie nikdy oslabiť podstatu slobody slova ako východiskového princípu demokracie.“* Vláda sa v tomto smere zaviazala, že schváli zákon o dátach, ktorý by komplexne riešil problematiku v tzv. *„oblasti OpenData“* (otvorené údaje – dáta, centrálne

registre). Jeho cieľom je identifikovať dôležité štátne informačné systémy a dáta v nich a zároveň dosiahnuť ich sprístupnenie cez koncept *„Open API“*.[26] Dôvodom pre takýto postup je skutočnosť, že napriek podniknutým legislatívnym a metodickým krokom (existencia zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov, tzv. zákona o slobode informácií v znení zákona č. 428/2022 Z. z.) je prax v ich poskytovaní zo strany štátnych a samosprávnych orgánov neuspokojivá. V tejto súvislosti je potrebné uviesť, že zákon o dátach s navrhovanou účinnosťou v máji 2021 doteraz schválený nebol, hoci momentálne prebieha vyhodnocovanie medzirezortného pripomienkového konania.[27] Na druhej strane, vláde sa v tomto ohľade podarilo schváliť Akčný plán koordinácie boja proti hybridným hrozbám na roky 2022 – 2024.

V každom prípade, vzhľadom na súčasnú politickú situáciu (pád vlády a stanovenie termínu predčasných volieb na september 2023), je otázne, ktoré kroky sa vláde podarí na tomto úseku ešte podniknúť.

Koordinovaný mechanizmus odolnosti SR voči informačným operáciám

V novembri 2020 prešiel medzirezortným pripomienkovým konaním materiál zameraný na budovanie odolnosti Slovenska voči informačným operáciám. Tento materiál reagoval na potrebu deklarovanú v *„Akčnom pláne Európskej únie boja proti dezinformáciám“ (2018), Akčnom plán pre európsku demokraciu (2019 – 2024), Európskom akte o slobode médií (2022), Kódexe postupov Európskej únie proti šíreniu dezinformácií (2018),* atď. Korešpondoval aj so závermi z prieskumu Eurobarometra orientovaného na média a správy z roku 2022, ktorý poukazoval na závažnosť tohto problému (*až 83 % opýtaných si myslí, že dezinformácie ohrozujú demokraciu a až 51 % Európanov sa domnieva, že boli vystavení dezinformáciám na internete*).[28]

Aj na podklade týchto skutočností bol vytvorený nelegislatívny materiál, ktorý pojednáva o novodobom spoločenskom fenoméne, tzv. *„informačných operáciách“* (ďalej len *„IO“)* a ochrane pred týmito operáciami v civilnej oblasti. Samotné IO vymedzuje v súlade s prezentovaným poznaním nepolitickej mimovládnej organizácie – GLOBSEC ako *„široké spektrum aktivít a spôsobov, ktoré slúžia na zber a šírenie potenciálne škodlivých informácií“.* Patria tu napr. dezinformácie, využívanie falošných identít a manipulatívnych techník na internete či zneužívanie technológií, prostredníctvom ktorých môže dôjsť až k zámernému zasahovaniu do vnútorných záležitostí štátu s cieľom oslabiť spoločnosť. Zároveň vymedzuje prvky IO (ďalej len *„PIO“*), medzi ktoré radí napr. *„falošné správy, hoaxy, propagandu, konšpiračné teórie, paródiu a satiru, dezinformáciu a malinformáciu“*.[29]

Národný inštitucionálny rámec budovania odolnosti voči PIO tvoria predovšetkým SITCEN, NBAC, orgány činné v trestnom konaní, orgány verejnej moci, mimovládne organizácie. Vo vzťahu k zahraničiu tento rámec dotvára spolupráca s Hybrid CoE v Helsinkách a StratCom CoE v Rige (*NATO Strategic Communication Centre of Excellence – Centrum výnimočnosti strategickej komunikácie).*[30]

Súčasťou koordinovaného mechanizmu je problematika vyhľadávania a identifikácie PIO, ich analýza, posúdenie vplyvu a rozhodovanie o reakcii (*ponúka rôzne scenáre reakcií v závislosti od stupňa vplyvu – nepatrný, znepokojujúci, vysoký, kritický*). [31]

Na druhej strane, vo vzťahu k prezentovaným informáciám, sa považujeme za potrebné zmieniť aj o existencii silného oportunistického názorového prúdu, ktorý ostro kritizuje akékoľvek zásahy, obmedzovania, manipulácie, či cenzúru štátu, ktorá je v príkrom rozpore so základnými ústavnými právami – slobodou slova a prejavu, ochranou osobnosti, nedotknuteľnosti súkromia a osobných údajov, zhromaždovacieho práva a pod. Samozrejme, aj tieto idey majú svoje racionálne jadro a je potrebné ich vziať do úvahy pri posudzovaní potenciálneho hybridného pôsobenia, rešpektujúc pritom zásadu *„secundum et intra legem“*.[32] Aj tieto skutočnosti viedli v konečnom dôsledku k tomu, že predkladaný materiál nebol schválený a doposiaľ sa podľa neho nepostupuje. Momentálne je rozpracovaná aktualizovaná verzia pod názvom *„Systém reakcie SR na informačné operácie“*.

Bezpečnostná stratégia SR a Obranná stratégia SR

V januári 2021 Národná rada SR po 16 rokoch schválila novú bezpečnostnú a novú obrannú stratégiu SR, napriek tomu že v roku 2017 boli obe stratégie schválené vládnym kabinetom, k ich predloženiu a následnému schváleniu zastupiteľským zborom nedošlo (*posledné parlamentom schválené stratégie pochádzajú z roku 2005*). Bezpečnostná a obranná stratégia sú vo svojej podstate koncepčnými (strategickými) dokumentmi, ktorých cieľom je zabezpečiť optimálne nastavenie a fungovanie bezpečnostného a obranného systému nášho štátu. V zásade platí pravidlo, že tieto stratégie by sa mali aktualizovať približne každých 5 – 7 rokov, prípadne skôr, ak dôjde k zásadným zmenám bezpečnostného prostredia. Práve v kontexte posledného zmieneného dôvodu, oba dokumenty zhodne konštatujú, že globálna bezpečnosť sa vo viacerých ohľadoch zhoršila, čo má priamy dopad na bezpečnosť a odolnosť SR. Hrozby a výzvy, ktorým čelíme, sú podľa nich *„čoraz zložitejšie, previazanejšie, bezprostrednejšie a majú väčšie dôsledky na našu bezpečnosť.“*

Pripravenosť štátu a spoločnosti efektívne a koordinovane reagovať na hybridné hrozby, vrátane dezinformácií bola zaradená medzi strategické bezpečnostné záujmy SR v najbližšom období. Bezpečnostná stratégia konštatuje, že *„… najvýraznejšie sa hybridné pôsobenie prejavuje cieleným šírením propagandy a dezinformácií proti demokratickému zriadeniu a ukotveniu SR v NATO a EÚ. Okrem dezinformačného pôsobenia sa hybridné hrozby na našom území prejavujú aj snahou o vytváranie potenciálne zneužiteľných závislostí v ekonomike, energetike či v kritickej infraštruktúre. Taktiež sú spojené aj so zahraničnou podporou miestnych extrémistických skupín a so snahami o zneužívanie a manipuláciu národnostných a iných menšín na politické účely.“*[33]

Na zvýšenie odolnosti štátu a spoločnosti voči hybridným hrozbám sa SR zaviazala, že na národnej úrovni posilní štrukturálne a personálne kapacity a expertízu vo verejnej správe. Zároveň deklarovala, že sa zameria na zefektívnenie koordinácie aktivít zainteresovaných subjektov, predovšetkým v oblasti plánovania, riadenia a tvorby politík na vládnej a rezortnej úrovni (v oblasti infraštruktúry, kybernetickej bezpečnosti, hospodárstva, ozbrojených síl, kultúry, spoločnosti, verejnej správy, politickej sféry, legislatívy, diplomacie, spravodajských služieb a informačného priestoru). Okrem toho bude, na medzinárodnej úrovni, vo vzájomnej koherencii so zahranično-politickým smerovaním SR, aktívne spolupracovať s NATO a EÚ, ako aj ďalšími medzinárodnými organizáciami a príslušnými medzinárodnými centrami výnimočnosti v oblasti boja proti hybridným hrozbám.[34]

V súlade s obrannou stratégiou SR, je prioritným cieľom zabezpečenie včasnej identifikácie a analýzy hrozieb a rizík. Nástrojom saturácie týchto cieľov sú aktivity orientované na rozvíjanie spôsobilosti

spravodajských služieb (osobitne v tomto ohľade – vojenského spravodajstva), ústredných orgánov štátnej správy a odborných prvkov, ktoré plnia úlohy v tejto oblasti. Zmyslom takého postupu je systémové usporiadanie vzájomného zdieľania informácií, procesu koordinovanej medzirezortnej analýzy a postupu predkladania informácií príslušným ústredným orgánom štátnej správy. Okrem rozvíjania spôsobilostí spravodajských služieb je pozornosť zameraná aj na rozvíjanie špecifickej spôsobilosti ozbrojených síl proti hybridnému pôsobeniu. Súčasťou obrannej stratégie SR je zabezpečenie včasného rozhodovania ústavných a štátnych orgánov o opatreniach na úseku obrany štátu v prepojení s rozhodovaním medzinárodných organizácií, a to aj v podmienkach hybridného pôsobenia.[35]

Akčný plán koordinácie boja proti hybridným hrozbám

Podľa expertov na bezpečnostné prostredie sa *„hybridné pôsobenie proti záujmom SR za posledných niekoľko rokov presunulo z periférie do hlavného prúdu na takmer všetky úrovne spoločnosti.“* Práve toto zistenie, spojené s odhodlaním spoločnosti efektívne zmierňovať rozvratné pôsobenie hybridných aktérov, bolo dôvodom pre spracovanie nového strategicko-taktického dokumentu na roky 2022 – 2024 pod gesciou Ministerstva obrany SR. Ďalšími nemenej dôležitými argumentmi podporujúcimi potrebu spracovania akčného plánu, bola globálna zmena bezpečnostného prostredia, rešpektovanie aliančných záväzkov nášho štátu voči EÚ a NATO, ako aj absencia stratégie pre boj SR s hybridnými hrozbami. Okrem toho, akčný plán dopĺňa systém organizačno-inštitucionálneho zabezpečenia o tzv. Výbor pre hybridné hrozby BR SR, ktorý bude koordinačným uzlom pre tvorbu bezpečnostných politík. V tejto súvislosti je potrebné uviesť, že výbor nebol do dnešného dňa vytvorený, napriek tomu, že podľa TASR, pripravovaná novela zákona o fungovaní Bezpečnostnej rady v čase mieru, ktorú vo februári 2023 posunuli poslanci Národnej rady SR do druhého čítania, s týmto výborom počíta. Nová legislatíva by mala byť účinná od mája 2023.[36] Z uvedeného vyplýva, že BR SR v súčasnosti nedisponuje stálym pracovným orgánom zameraným výhradne na problematiku hybridných hrozieb. Agenda zasahuje do pracovnej náplne iných, už existujúcich výborov, ktoré sme uvádzali vyššie. Podľa Ministerstva obrany SR, ktoré návrh predložilo: *„Hlavným poslaním nového výboru BR SR bude podieľať sa na koordinácii činností zameraných na vyhodnocovanie bezpečnostnej situácie doma i v zahraničí, prijímanie opatrení na riešenie hybridného pôsobenia proti záujmom SR a tvorbu relevantných politík v oblasti boja proti hybridným hrozbám.“*[37]

Akčný plán koordinácie boja proti hybridným hrozbám je nelegislatívnym rámcovým, strategickým dokumentom. Ambíciou materiálu je vymedziť adekvátny okruh krokov (úloh a aktivít postavených na inštitucionálnom rámci), ktoré je potrebné na tomto úseku podniknúť za účelom zlepšenia schopnosti štátu a spoločnosti reagovať na hybridné hrozby. Návrh plánu bol predložený na medzirezortné pripomienkové konanie v novembri 2021. V decembri 2021 bolo ukončené medzirezortné pripomienkové konanie a materiál bol predložený BR SR a vláde SR na schválenie. K jeho formálnemu schváleniu došlo v marci 2022 na základe uznesenia vlády SR č. 235.

Strategickými cieľmi akčného plánu sú:

- posilnenie odolnosti štátu a spoločnosti voči hybridným hrozbám,
- posilnenie medzirezortnej spolupráce a koordinácie s cieľom včasnej detekcie, analýzy,

- atribúcia a reakcia na hybridné aktivity voči SR,
- zvyšovanie povedomia spoločnosti o rizikách hybridného pôsobenia a potrebe zvyšovania celospoločenskej odolnosti voči nim,
- vybudovanie systému strategickej komunikácie na celovládnej a rezortnej úrovni,
- posilnenie aktívneho pôsobenia SR pri rozvoji spolupráce v rámci EÚ a NATO v oblasti boja s hybridnými hrozbami a posilňovania medzinárodnej spolupráce.[38]

Podľa akčného plánu je kľúčovým predpokladom efektívnej reakcie štátu celospoločenský prístup (tzv. *„whole-of-society approach“*), čo vyžaduje zapojenie a koordináciu inštitúcií štátnej správy, ekonomického a akademického sektora. Okrem toho sa počíta s vytvorením nových, resp. posilnením už existujúcich útvarov na Úrade vlády SR, Ministerstve obrany SR, Ministerstve vnútra SR a Ministerstve zahraničných vecí a európskych záležitostí SR.

Akčný plán je podľa druhu zavedených opatrení rozdelený do šiestich segmentov, pričom medzi základné úlohy, bez nároku na úplnosť, na tomto úseku patria:

1. Všeobecné úlohy,
2. Systémové opatrenia,
3. Strategická komunikácia a dezinformácie,
4. Budovanie odolnosti obyvateľstva,
5. Ochrana volebných procesov,
6. Cudzí vplyv.[39]

Úlohy, ktoré vyplývajú z akčného plánu sa priebežne plnia. Napr. na Úrade vlády bol zriadený odbor pre strategickú komunikáciu, ktorý spolu so SITCEN patria pod KBR, sekcie prevencie korupcie a krízového manažmentu. KBR plní úlohy súvisiace s činnosťou BR SR a bola zriadená na základe ústavného **zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu**. Odbor pre strategickú komunikáciu vytvára a realizuje komunikačné opatrenia určené na posilňovanie odolnosti štátu a občanov voči hybridným hrozbám; realizuje komunikáciu s verejnosťou v oblasti boja proti hybridným hrozbám na webovej stránke úradu vlády a separátnych účtoch na sociálnych sieťach; navrhuje a vytvára komunikačné výstupy; spolupracuje s ďalšími útvarmi strategickej komunikácie na príslušných rezortoch; vytvára a podieľa sa na medzinárodnej spolupráci v oblasti strategickej komunikácie; na požiadanie pripravuje podkladové materiály pre komunikačné výstupy k problematike hybridných hrozieb a boja proti nim; úzko spolupracuje so SITCEN a s Tlačovým a informačným odborom; vypracúva návrhy vnútorných predpisov vo svojej pôsobnosti; pomáha koordinovať strategickú komunikáciu naprieč ústrednými orgánmi štátnej správy.[40] Problematiku riešenia krízových situácií mimo iné reglementuje aj **zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení zákona č. 9/2021 Z. z.**, ktorý na tomto úseku dáva status orgánov krízového riadenia vláde, BR SR, ministerstvám a ostatným ústredným orgánom štátnej správy, Národnej bane Slovenska, bezpečnostnej rade kraja, okresu, obciam, vyšším územným

celkom a obvodným úradom. Zákon o lobingu doteraz schválený nebol, hoci sa na Slovensku s takýmito legislatívnymi pokusmi stretávame približne od roku 2001. Posledný návrh bol predložený v novembri 2021, pripomienkové konanie bolo plánované na január 2022, čím sa podarilo zavŕšiť predprípravnú fázu, avšak ku finálnemu schváleniu zákona nedošlo.[41] V týchto intenciách musíme s ľútosťou konštatovať, že zákon o lobingu nebol zaradený ani do *„Plánu legislatívnych úloh vlády SR na rok 2022“* a dokonca ani *„Plánu legislatívnych úloh vlády SR na rok 2023“*. Zákon o volebnej kampani bol naposledy novelizovaný v októbri 2022, a to zákonom č. 264/2022 o mediálnych službách a o zmene a doplnení niektorých zákonov v znení zákona č. 351/2022 Z. z. Zmeny sa okrem iného týkali aj problematiky politickej propagácie, jej povinného evidovania a financovania volebnej kampane. Čo sa týka zavedenia povinnosti registrácie povinných subjektov v *„Registri partnerov verejného sektora“,* túto problematiku reglementuje zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov. Tento zákon bol naposledy novelizovaný v novembri 2019 (zákonom č. 241/2019 Z. z.), pričom zmeny sa okrem iného týkali identifikácie a verifikácie konečného užívateľa výhod. Ďalšie legislatívne zmeny, v kontexte nami riešeného problému, sú naviazané na pripravovaný dokument – nariadenie vlády SR, ktorým sa ustanovujú kritické zahraničné investície s plánovanou účinnosťou od marca 2023. Momentálne je v štádiu vyhodnocovania medzirezortného pripomienkového konania.[42] Vo vzťahu k právnej úprave povinného zverejňovania zmlúv v registri zmlúv, túto problematiku rieši zákon o slobodnom prístupe k informáciám. Napriek tomu, že tento zákon bol naposledy novelizovaný v januári 2023 (zákonom č. 428/2022 Z. z.), v nami riešenej oblasti (systém vynucovania a sankcionovania za porušenie tejto povinnosti) nedošlo k výraznejším zmenám. Na margo trestnoprávneho postihu konania, ktoré môže mať charakter hybridného pôsobenia uvádzame, že Trestný zákon bližšie špecifikuje pojmy *„cudzia moc“* a *„cudzí činiteľ“* [43]. De iure ide o základné alebo kvalifikované skutkové podstaty trestných činov vyzvedačstva, vlastizrady (úkladov proti SR, teroru, záškodníctva, sabotáže) a ohrozenia mieru, kde je tento prvok ich explicitnou súčasťou (zákonným znakom trestného činu). Okrem toho, môže byť takéto konanie postihnuté aj v rámci iných skutkových podstát trestných činov a kvalifikované ako tzv. priťažujúca okolnosť – tak ako o tom hovorí ustanovenie § 37 písm. l) – *„v spojení s cudzou mocou alebo cudzím činiteľom“,* teda okolnosť, na ktorú súd prihliada v procese rozhodovania o vine a treste.[44] Z tohto neukončeného výpočtu trestných činov je zrejmé, že okruh konaní postihnuteľných trestným právom, ktoré môžu mať hybridný charakter je veľmi široký. Napriek tomu možno konštatovať, že k legislatívnym zmenám v intenciách návrhov akčného plánu v trestnoprávnej oblasti doposiaľ nedošlo.

Zastávame názor (zo syntézy uvedeného je to zrejmé), že nie je možné detailne analyzovať všetky aktivity a úlohy z pohľadu odpočtu ich plnenia aj vzhľadom na širokospektrálnosť akčného plánu. Pokúsili sme sa len poukázať na určité, z nášho uhla pohľadu vnímané, najvýznamnejšie aspekty. V každom prípade, akčný plán je dlhodobý plánovací dokument a rada aktivít a úloh stojí ešte pred nami.

Koncepcia bezpečnostného systému SR

Z uznesenia vlády SR č. 485 zo 17. októbra 2018 vyplynula povinnosť spracovať materiál – Koncepciu bezpečnostného systému SR (ďalej len *„koncepcia“*). Návrh koncepcie bol spracovaný v gescii Ministerstva vnútra SR a predložený na medzirezortné pripomienkové konanie v októbri 2022.

Momentálne prebieha jeho vyhodnotenie.[45] Uvedený nelegislatívny materiál je tematicky, podľa priorít, rozdelený do dvoch častí. Prvou prioritou je medzirezortné krízové riadenie a koordinácia a druhou prioritou sú funkcie bezpečnostného systému (plánovanie, prevencia, reakcia, obnova). Nová koncepcia nahrádza Koncepciu bezpečnostného systému SR, ktorá bola schválená uznesením vlády SR č. 1098 z októbra 2002.

Primárnym dôvodom pre spracovanie novej koncepcie je zistenie, že *„súčasný bezpečnostný systém SR neodráža prelínanie vojenských a nevojenských hrozieb, jeho možnosti reagovania na súčasné vnútorné a vonkajšie bezpečnostné hrozby sú limitované a hlavný dôraz a funkcionalita spočíva v riešení krízových situácií ex post.“* Okrem toho, *„v súčasnom systéme absentuje orgán, ktorý by koordinoval, monitoroval, viedol a zhodnocoval všetky relevantné akcie a činnosti v oblasti bezpečnosti a krízového riadenia vo vzťahu k bezpečnostnej situácii na národnej aj medzinárodnej úrovni.“* Koncepcia preto navrhuje upraviť kompetencie KBR a urobiť zásadné zmeny v organizácii a fungovaní bezpečnostného systému SR ako celku.

Práve na základe týchto skutočností bolo navrhnuté nové inštitucionálne nastavenie bezpečnostného systému SR (2 modely), ktorý reprezentujú nasledovné súčasti:

- Národná rada SR, vláda SR (výkonný orgán), prezident SR, ministerstvá a ostatné ústredné orgány štátnej správy,
- BR SR (výbory BR SR), odborná pracovná skupina, BR kraja, BR okresu,
- KBR (riaditeľ, analytický odbor),
- NBAC (riaditeľ je zároveň predsedom nového výboru BR SR pre hybridné hrozby),
- Ústredný krízový štáb (riadiaca skupina, operačná skupina, implementačná skupina, informačný manažment); rezortný krízový štáb; krízový štáb vyšších územných celkov a územnej samosprávy.

Pôsobnosť parlamentu, vlády, prezidenta, ministerstiev a ostatných ústredných orgánov štátnej správy počas krízovej situácie vyplýva z **Ústavy Slovenskej republiky č. 460/1992 Zb., v znení ústavného zákona č. 24/2023 Z. z.**, ale aj ďalších zákonov (*napr. zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení zákona č. 9/2021 Z. z., ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení ústavného zákona č. 414/2020 Z. z., zákona č. 319/2002 Z. z. o obrane SR v znení zákona č. 306/2019 Z. z.*).

Podľa koncepcie, je úlohou BR SR na tomto úseku schvaľovať plány odolnosti štátu ako preventívny nástroj pre jednotlivé bezpečnostné hrozby. Vzhľadom na to, že ústredné orgány štátnej správy majú povinnosť vypracovať tzv. *„situačné plány“* v rozsahu svojich pôsobností, je žiadúce, aby už existujúce situačné plány boli opätovne aktualizované tak, aby odrážali reálne bezpečnostné hrozby a určovali hlavné úlohy pre zainteresované orgány štátnej správy. Situačné plány prezentujú zoznam bezpečnostných hrozieb, scenáre možného vývoja bezpečnostných hrozieb, opatrenia na predchádzanie krízovým situáciám a ich riešenie. Tieto plánovacie dokumenty umožňujú efektívne anticipovať a modifikovať vývoj bezpečnostnej situácie podľa potrieb spoločnosti. Koncepcia v súlade

s akčným plánom, ako sme už avizovali vyššie, odporúča zriadiť stály výbor rady pre hybridné hrozby a zároveň navrhuje udeliť BR SR výkonné právomoci v čase krízovej situácie (*momentálne tomu tak nie je*). Aj týmito krokmi možno zvýšiť účinnosť a efektivitu prijímaných opatrení v situáciách, kedy štát čelí akútnemu bezpečnostnému riziku.

Čo sa týka KBR, aj v tomto prípade koncepcia navrhuje posilniť výkonné právomoci tohto orgánu, a to najmä vo vzťahu k výborom rady (*riaditeľ kancelárie získa oprávnenie priamo ukladať úlohy predsedom výborov BR SR*). Okrem toho je žiadúce zefektívniť spoluprácu medzi kanceláriou a NBAC a analytickými útvarmi z relevantných rezortov, napr. Ministerstva vnútra SR, Ministerstva obrany SR, Ministerstva zahraničných vecí a európskych záležitostí SR a pod. (*na zabezpečenie vysokej kvality predkladaných materiálov do BR SR bude riaditeľ KBR oprávnený využívať analytické spôsobilosti týchto útvarov*). Zároveň je cieľom posilniť prepojenie medzi KBR a BR SR (*riaditeľ KBR, ktorý je súčasne aj tajomníkom BR SR, bude mať bezprostredný vplyv na plánovanie tematiky rokovaní rady; jemu podriadená analytická jednotka bude vykonávať analytickú činnosť v oblasti bezpečnostných hrozieb a k nim prislúchajúcich plánov zvyšovania odolnosti štátu*). Je zrejmé, že týmito organizačnými a kompetenčnými zmenami sa postavenie KBR výrazne posilní, čo bude mať priamy vplyv na účinnosť a efektivitu boja proti hybridným hrozbám. Systematickosť a koordinovanosť aktivít jednotlivých zainteresovaných subjektov je nesporne tým nástrojom, ktorý môže aktívne prispieť k naplneniu týchto cieľov.

Okrem toho, podľa koncepcie je potrebné zriadiť *„stálu odbornú pracovnú skupinu“*, vo variabilnom zložení z vecne kompetentných zástupcov príslušných ústredných orgánov štátnej správy podľa riešených tém, na základe ich vyžiadania riaditeľom KBR a nominácie vedúcim (štatutárom) ústredného orgánu štátnej správy. Sme toho názoru, že zložitosť a heterogénnosť hybridných hrozieb si jednoznačne vyžaduje erudovaný a variabilný (operatívny) prístup.

Z tohto uhla pohľadu si je potrebné uvedomiť rýchlu a neustále sa meniacu dynamiku vývoja hybridných hrozieb, a práve táto skutočnosť kladie požiadavky na permanentné rozvíjanie odborných kapacít. Vzhľadom na to, že KBR je súčasne kontaktným bodom SR v Hybrid CoE a bude mať aj priame prepojenie na novovytvorený výbor pre hybridné hrozby, vytvárajú sa predpoklady na oboznamovanie sa s aktuálnymi trendami a nastavenie optimálneho rámca na ich potláčanie.

Ako sme už uviedli vyššie, riaditeľ NBAC bude súčasne predsedom výboru pre hybridné hrozby a v rámci činnosti BR SR spolupracuje s riaditeľom KBR. Aj táto skutočnosť poukazuje na posilnenie väzieb medzi jednotlivými subjektmi.

Koncepcia venuje osobitnú pozornosť krízovému riadeniu a jeho koordinácii. Práve v týchto intenciách má nosné postavenie tzv. *„Ústredný krízový štáb“* (ďalej len *„ÚKŠ“*), ktorý je poradným orgánom vlády v čase krízovej situácie. Aj v tomto prípade je vhodné aplikovať variabilný (operatívny) prístup, osobitne pri kreovaní tohto orgánu. Zloženie ÚKŠ bude variovať v závislosti od typu hrozby. Činnosť štábu bude riadiť predseda, t. j. vrcholový predstaviteľ rezortu zodpovedný za prípravu situačného plánu podľa špecifického druhu hrozby. Pri voľbe členov (expertov na riešenie situácií, ktoré vznikli resp. môžu vzniknúť počas krízy) sa bude reflektovať najmä na potrebu ich odbornosti podľa druhu krízy. O aktivácii ÚKŠ rozhodne predseda BR SR. Návrh na aktiváciu môže podať ktorýkoľvek stály člen BR SR alebo riaditeľ KBR. Predseda ÚKŠ bude zároveň zodpovedný za predkladanie návrhov na prijatie opatrení pre rozhodnutie vlády SR. Na lokálnej a rezortnej úrovni budú v súlade s vyššie uvedenými zákonmi pre

oblasť krízového riadenia a zákonom č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení zákona č. 146/2023 Z. z. operovať rezortné krízové štáby, krízové štáby územnej samosprávy (*vyšších územných celkov, obcí, primátori/ starostovia obcí*). Analogické funkcie počas krízovej situácie budú plniť aj orgány miestnej štátnej správy (*BR kraja a BR okresu, okresný úrad v sídle kraja/ okresný úrad, prednostovia okresných úradov v sídle kraja/ okresných úradov*).

Druhá časť koncepcie, ako sme už naznačili vyššie, pojednáva o základných funkciách bezpečnostného systému (*plánovanie, prevencia, reakcia, obnova*), ktoré je potrebné systematicky napĺňať. Aj z týchto dôvodov koncepcia poukazuje na potrebu rešpektovania princípov európskej bezpečnostnej a obrannej politiky, systému reakcie NATO na krízové situácie – NCRS a ďalších odporúčaní medzinárodných organizácií podporených príslušnými dohovormi, ktorými je SR viazaná. Zároveň zdôrazňuje potrebu využívania nových poznatkov, ktoré pre tieto účely vypracoval *„CEPC NATO – Výbor pre civilné núdzové plánovanie“* (*napr. „Základné požiadavky, usmernenia na dosiahnutie odolnosti a hodnotiace kritériá“ – „Baseline Requirements, Resilience Guidelines and Evaluation Criteria“*). Koncepcia navrhuje vypracovať jednotnú *„Metodiku civilného núdzového plánovania“*, pričom tým nie je dotknuté plánovanie obrany štátu podľa zákona č. 319/2002 Z. z. o obrane SR a Smernice vlády SR o plánovaní obrany štátu.[46]

Z doteraz uvedeného vyplýva, že nová koncepcia bezpečnostného systému SR vychádza z identifikovaných potrieb spoločenskej praxe (nedostatočná efektívnosť, koordinovanosť, komplexnosť, erudovanosť systému v oblasti krízového riadenia), ktoré sa prostredníctvom systému návrhov a odporúčaní snaží riešiť.

Národná stratégia riadenia rizík bezpečnostných hrozieb SR

„Národná stratégia riadenia rizík bezpečnostných hrozieb SR (ďalej len „stratégia“) navrhuje systémové opatrenia ohľadom prevencie, pripravenosti a reakcie na bezpečnostné hrozby, a pomenováva nástroje na zvyšovanie spoločenskej, ekonomickej a individuálnej (občianskej) odolnosti formou integrovaného riadenia rizík na nadrezortnej úrovni.“ Tento strategický dokument v oblasti efektívneho riadenia rizík plánuje aktivity na obdobie najmenej 10 rokov, počínajúc rokom 2022 (začiatok prípravy stratégie), až do roku 2032 (termín uzavretia čerpania finančných prostriedkov z nového plánovacieho obdobia komunitárnych a štrukturálnych fondov). Konkrétne úlohy a opatrenia, ktoré vyplývajú zo stratégie budú, spolu s ich časovým plnením, zahrnuté v akčnom pláne, ktorý bude pravidelne aktualizovaný každé tri roky. Stratégia bola koncipovaná a predložená na skrátené medzirezortné konanie ešte v roku 2021 a k jej schváleniu došlo v januári 2022,[47] pričom prvý plán bol predložený na rokovanie vlády už koncom júna 2022.

Stratégia v súlade s bezpečnostnou analýzou potrieb definuje dva základné strategické ciele SR v oblasti efektívneho manažmentu rizík:

1. Predchádzať stratám a vzniku škôd v súvislosti s mimoriadnymi udalosťami, zoceliť krajiny voči rizikám a integrovať mitigačné opatrenia do všetkých rozvojových aktivít SR;
2. Modernizovať krízovú komunikáciu a formovať situačné povedomie zabezpečením participácie aktérov a skvalitnením inštitucionálnej a technologickej základne riadenia rizík.

Stratégia napĺňa multilaterálne rámce, ktoré sa SR zaviazala implementovať do svojich strategických dokumentov, rešpektujúc pritom postavenie člena v OSN, EÚ, NATO a iných medzinárodných organizáciách a inštitúciách. Výsledkom tohto neukončeného procesu je existujúci legislatívny rámec pre oblasť manažmentu rizík bezpečnostných hrozieb.[48]

Súčasťou stratégie je aj národný register hrozieb, zoznam kľúčových rizík z dlhodobého hľadiska (25 – 30 rokov), kľúčových rizík s cezhraničným účinkom, kľúčových rizík v dôsledku multiplikačného efektu zmeny klímy, zoznam gestorov a iných aktérov angažovaných v procese riadenia rizík, vymedzenie prioritných oblastí strategických cieľov, implementačného postupu a podmienok financovania.

Záver

Hybridné hrozby vo svojej podstate prinášajú konflikt individuálnych a verejných záujmov. Na jednej strane tu máme slobodu slova, prejavu a právo na informácie ako základné piliere demokracie a na druhej strane tu máme autonómnosť, celistvosť, ústavnosť, zákonnosť a obranyschopnosť štátu. Pri strete a realizácií oboch princípov – musí zákonite dôjsť k obmedzeniu jedného v prospech zachovania druhého, polemická je miera zásahov do práv a slobôd občanov v záujme zachovania spoločenskej rovnováhy.

Sme toho názoru, že aj posledný analyzovaný strategický dokument, v úzkej časovej, obsahovej a formálnej previazanosti na jeho *„predchodcov“,* jednoznačne poukazuje na to, že bezpečnostné prostredie sa v posledných rokoch vážne zmenilo v dôsledku existencie nových foriem hrozieb, ktorým musí SR a aj celé medzinárodné spoločenstvo čeliť. Z tohto uhla pohľadu možno iniciatívu a aktivity SR na úseku zabránenia šíreniu a negatívnym dôsledkom hybridných hrozieb v rozmedzí rokov 2016 – 2023 hodnotiť pozitívne. Osobitne k uvedenému, stroho vyslovenému hodnotiacemu záveru uvádzame, že pri ich spracovaní a následnej realizácii je rešpektovaná identita konkrétnej potreby a koncepcia postupov pri zabezpečovaní kontroly hybridných hrozieb (prevencia, represia). V priebehu tohto pomerne krátkeho obdobia, keď sa hybridné hrozby dostali do povedomia širšej odbornej verejnosti a kompetentných štátnych orgánov a inštitúcií, bol podniknutý celý rad krokov koncepčného a strategického charakteru. Výsledkom tohto neukončeného procesu je, podľa nášho názoru, vcelku dobre nastavený základný legislatívno-inštitucionálny rámec ich intencionálneho potláčania. V tejto súvislosti považujeme za potrebné podotknúť, že v súčasnosti sa pripravuje nová Koncepcia strategickej komunikácie SR a nová Stratégia boja proti hybridným hrozbám, ktoré budú zohľadňovať dynamickosť a variabilitu bezpečnostného prostredia.

Sme si vedomí aj toho, že hybridné hrozby sa vyznačujú značnou diverzitou a podprahovosťou, čo značne komplikuje ich identifikáciu a následnú elimináciu. Z uvedeného vyplýva predpoklad, ktorý si dovolíme formulovať na záver tohto príspevku: *„Najväčší problém v kontexte eliminácie hybridných hrozieb bude spočívať práve v operačno-taktickej rovine – detekcia, interpretácia hybridnej hrozby a vyvodenie patričnej zodpovednosti“.*

Použité informačné zdroje

Bezpečnostná stratégia SR. [online]. [2023-1-30]. Dostupné online: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

Účinnejší Kódex postupov EÚ proti šíreniu dezinformácií. [online]. [2023-1-30]. Dostupné online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_sk.

Hybrid CoE. What is Hybrid CoE? [online]. [2023-2-1]. Dostupné online: https://www.hybridcoe.fi/.

Kolektív autorov. 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.

LP/2021/799 Národná stratégia riadenia rizík bezpečnostných hrozieb SR. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2021/799.

LP-2022-636 Návrh Koncepcie bezpečnostného systému SR. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/636.

LP/2022/636 Koncepcia bezpečnostného systému SR. [online]. [2023-1-30]. Dostupné online:https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/636.

LP/2020/507 Koordinovaný mechanizmus odolnosti SR voči informačným operáciám. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2020/507.

LP/2021/55 Zákon o údajoch. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2021/55.

MO SR. Akčný plán koordinácie boja proti hybridným hrozbám. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf.

MO SR. Biela kniha o obrane SR. [online]. [2023-1-30]. Dostupné online: https://www.mod.gov.sk/data/BKO2016_LQ.pdf.

NBÚ. Akčný plán kybernetickej bezpečnosti. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf.

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

NBÚ. Národná stratégia kybernetickej bezpečnosti. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf

NBÚ. SK-CERT. [online]. [2023-1-30]. Dostupné online: https://www.sk-cert.sk/sk/o-nas/index.html.

NBÚ. Správa o kybernetickej bezpečnosti v SR v roku 2021. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf.

Obranná stratégia SR. [online]. [2023-1-30]. Dostupné online: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf.

PI/2022/308 Návrh nariadenia vlády SR, ktorým sa ustanovujú kritické zahraničné investície. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2022/308.

PI/2022/176 Návrh zákona, ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady SR v čase mieru v znení neskorších predpisov. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2022/176.

PI/2021/264 Návrh zákona o lobingu. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2021/264.

Pokyn Inštitútu správnych a bezpečnostných analýz MV SR o organizačnom poriadku Inštitútu správnych a bezpečnostných analýz MV SR č. 1/2022 z 1. 3. 2022.

O nás: Národné bezpečnostné analytické centrum (NBAC): [online]. [2023-2-1]. Dostupné online: https://www.sis.gov.sk/o-nas/nbac.html.

Správa o činnosti SIS za rok 2021. [online]. [2023-1-26]. Dostupné online: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby.

sk. [online]. [2023-1-26]. Dostupné online: www.slovnik.aktuality.sk.

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v únii.

Správa o bezpečnosti SR za rok 2021. [online]. [2023-1-30]. Dostupné online: https://www.vlada.gov.sk/share/uvsr/br-sr/sprava_o_bezpecnosti_sr_2021.pdf?csrt=9218400007279347994.

sk. Bezpečnostná rada SR by mohla mať nový výbor pre hybridné hrozby. [online]. [2023-1-30]. Dostupné online: https://www.teraz.sk/slovensko/bezpecnostna-rada-sr-by-mohla-mat-nov/691544-clanok.html.

TF-CSIRT. Team Database. [online]. [2023-1-30]. Dostupné online: https://www.trusted-introducer.org/directory/country_LICSA.html.

ÚV SR. Organizačný poriadok. [online]. [2023-1-30]. Dostupné online: https://www.vlada.gov.sk/share/uvsr/dokumenty_uvsr/organizacny-poriadok/op_uvsr_1122.pdf?csrt=9218400007279347994.

ÚV SR. Štatút Situačného centra SR. [online]. [2023-2-5]. Dostupné online:https://www.vlada.gov.sk/data/files/8042_statut-situacneho-centra-sr.pdf?csrt=9218400007279347994.

Vojenské spravodajstvo. Správa o činnosti vojenského spravodajstva za rok 2021. [online]. [2023-1-26]. Dostupné online: **http://mepoforum.sk/wp-content/uploads/2022/06/VS-Sprava-o-Cinnosti-2021.pdf**.

Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení ústavného zákona č. 414/2020 Z. z..

Ústava Slovenskej republiky č. 460/1992 Zb., v znení ústavného zákona č. 24/2023 Z. z.

Zákon č. 346/2015 Z. z., ktorým sa dopĺňal zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady SR v čase mieru v znení zákona č. 319/2012 Z. z.

Zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení v znení zákona č. 146/2023 Z. z.

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení zákona č. 325/2022 Z. z.

Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady SR v čase mieru v znení zákona č. 97/2023 Z. z.

Zákon č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení zákona č. 92/2022 Z. z.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 351/2022 Z. z.

Zákon č. 129/2002 Z. z. o integrovanom záchrannom systéme v znení zákona č. 351/2022 Z. z.

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení zákona č. 497/2022 Z. z.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 231/2022 Z. z.

Zákon č. 264/2022 o mediálnych službách a o zmene a doplnení niektorých zákonov v znení zákona č. 351/2022 Z. z.

Zákon č. 319/2002 Z. z. o obrane SR v znení zákona č. 306/2019 Z. z.

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 92/2022 Z. z.

Zákon č. 128/2015 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v znení zákona č. 91/2016 Z. z.

Zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení zákona č. 241/2019 Z. z.

Zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo čase vojny a vojnového stavu v znení zákona č. 9/2021 Z. z.

Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (tzv. zákon o slobode informácií) v znení zákona č. 428/2022 Z. z.

Zákon č. 300/2005 Z. z. Trestný zákon v znení zákona č. 117/2023 Z. z.

Poznámky pod čiarou

[1] Zo správy o činnosti SIS za rok 2021 vyplýva, že SIS v priebehu tohto roka zaznamenala zintenzívnenie hybridného pôsobenia zo strany Ruskej Federácie, a to v informačnej, spravodajskej, spoločenskej a kultúrnej sfére. Okrem toho pokračovalo hybridné a vplyvové pôsobenie Číny na SR, aj keď viditeľnosť a intenzita informačných aktivít vo verejnom priestore sa v porovnaní s rokom 2020 znížila. In SIS. Správa o činnosti SIS za rok 2021. [online]. [2023-1-26]. Dostupné online: https://www.sis.gov.sk/pre-vas/sprava-o-cinnosti.html#hrozby. Podľa správy o činnosti Vojenského spravodajstva (ďalej len „VS“) za rok 2021 vyplýva, že zdrojom priamej hybridnej hrozby pre EÚ a SR vo forme organizovania a podpory nelegálnej migrácie do členských štátov bola v roku 2021 Bieloruská republika. Zároveň je dlhodobo zaznamenaný trend nárastu hybridných aktivít Ruskej Federácie na území SR prostredníctvom diplomacie, pôsobenia cudzích spravodajských služieb, strategickej propagandy. In VS. Správa o činnosti VS za rok 2021. [online]. [2023-1-26]. Dostupné online: http://mepoforum.sk/wp-content/uploads/2022/06/VS-Sprava-o-Cinnosti-2021.pdf.

[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.

[3] MO SR. Biela kniha o obrane SR. [online]. [2023-1-30]. Dostupné online: https://www.mod.gov.sk/data/BKO2016_LQ.pdf.

[4] Koncepcia sa chápe ako významový útvar (sústava názorov, spôsob nazerania ma niečo, spôsob ponímania niečoho), osnova, rozvrh, plán, hlavný zámer alebo konštrukčný princíp. Naproti tomu stratégia (z gréckeho „strategos“ – generál alebo „stratos“ – vojsko, výprava + „agein“ – viesť) je teória alebo prax o vedení boja; náuka o príprave a vedení bojovej operácie; umenie viesť kolektív s cieľom dosiahnuť veľké spoločné ciele; dlhodobý zámer na dosiahnutie určitého cieľa, napr. vojenská stratégia. In Slovnik.sk. [online]. [2023-1-26]. Dostupné online: www.slovnik.aktuality.sk.

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

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

[7] Správa o bezpečnosti SR za rok 2021. [online]. [2023-1-30]. Dostupné online: https://www.vlada.gov.sk/share/uvsr/br-sr/sprava_o_bezpecnosti_sr_2021.pdf?csrt=9218400007279347994.

[8] TF-CSIRT. Team Database. [online]. [2023-1-30]. Dostupné online: https://www.trusted-introducer.org/directory/country_LICSA.html.

[9]NBÚ. SK-CERT. [online]. [2023-1-30]. Dostupné online: https://www.sk-cert.sk/sk/o-nas/index.html.

[10] Za účelom zefektívnenia nahlasovania a riešenia kybernetických incidentov bola dokonca zriadená vyhradená emailová adresa a telefonický kontakt (incident@minv.sk a tlf. kontakt 09610 56 789).

[11] Pokyn Inštitútu správnych a bezpečnostných analýz MV SR o organizačnom poriadku Inštitútu správnych a bezpečnostných analýz MV SR, č. 1/2022 z 1. 3. 2022.

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

[13] Bezpečnostná rada SR (BR SR) vznikla na základe ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu. BR SR sa ako poradný orgán podieľa na vytváraní a realizácii bezpečnostného systému SR, plnení medzinárodných záväzkov v oblasti bezpečnosti, vyhodnocuje bezpečnostnú situáciu v SR a vo svete; pripravuje pre vládu návrhy opatrení na zachovávanie bezpečnosti SR, na predchádzanie krízovým situáciám, ako aj návrhy na riešenie vzniknutej krízovej situácie. Podrobnosti jej fungovania v čase mieru ustanovuje osobitný zákon, a to zákon č. 110/2004 Z. z. v znení zákona č. 97/2023 Z. z. Ak je v čase vojny, vojnového stavu alebo výnimočného stavu znemožnená činnosť vlády, vykonáva jej ústavné právomoci až do obnovenia činnosti BR SR s výnimkou rozhodovania o programe vlády a jeho plnení, o požiadaní o vyslovenie dôvery a o udelení amnestie vo veciach priestupkov. BR SR má 6 stálych výborov, a to: výbor pre zahraničnú politiku, výbor pre obranné plánovanie, výbor pre civilné núdzové plánovanie, výbor pre koordináciu spravodajských služieb, výbor pre energetickú bezpečnosť, výbor pre kybernetickú bezpečnosť. BR SR má 9 členov. Na čele rady stojí predseda (predseda vlády), v jeho neprítomnosti ho zastupuje podpredseda (podpredseda vlády). Radu tvoria aj jej ďalší členovia (ministri obrany, vnútra, financií, zahraničných vecí a európskych záležitostí; ostatných vymenúva Prezident SR), ktorí majú právo predkladať návrhy, informácie, materiály, vyjadrovať stanoviská a rozhodovať formou hlasovania. BR SR rozhoduje v zbore; na prijatie uznesenia je potrebný súhlas nadpolovičnej väčšiny. Podľa územného a správneho usporiadania SR sa zriaďujú BR kraja a okresu. Predsedom BR kraja/ okresu je prednosta okresného úradu v sídle kraja/ prednosta okresného úradu. Ďalšími členmi BR kraja/ okresu sú zástupca ozbrojených síl určený Ministerstvom obrany SR, zástupca PZ, zástupca Hasičského a záchranného zboru a predseda vyššieho územného celku.

[14] Správa o bezpečnosti SR za rok 2021. [online]. [2023-2-1]. Dostupné online: https://www.vlada.gov.sk/share/uvsr/br-sr/sprava_o_bezpecnosti_sr_2021.pdf?csrt=9218400007279347994.

[15] ÚV SR. Štatút Situačného centra SR. [online]. [2023-2-5]. Dostupné online:https://www.vlada.gov.sk/data/files/8042_statut-situacneho-centra-sr.pdf?csrt=9218400007279347994.

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

[17] SIS. O nás: Národné bezpečnostné analytické centrum (NBAC): [online]. [2023-2-1]. Dostupné online: https://www.sis.gov.sk/o-nas/nbac.html.

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

[19] Pojmom kybernetický priestor sa pôvodne metaforicky označovalo prostredie, v ktorom prebieha prenos a spracovanie digitálne zaznamenanej informácie. V súčasnosti označuje informačnú a komunikačnú infraštruktúru organizácie, štátu, alebo globálnu informačnú a komunikačnú infraštruktúru.

[20] NBÚ. Národná stratégia kybernetickej bezpečnosti. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf.

[21] Medzi tieto zodpovedné subjekty akčný plán radí: Centrum vedecko-technických informácií, Generálnu prokuratúru SR, Informačné a komunikačné technológie, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, konzorcium, ktoré vznikne na základe úlohy G.5, Medzinárodnú agentúru pre atómovú energiu, všetky ministerstvá, Národnú banku Slovenska, Národný bezpečnostný úrad, NCKB SK-CERT, Národnú expertnú skupinu, poskytovateľov digitálnych služieb, prevádzkovateľov základných služieb, Slovenskú akadémiu vied, Slovenskú informačnú službu, Slovenskú národnú akreditačnú službu, Štátny inštitút odborného vzdelávania, štátnu správu, Republikovú úniu zamestnávateľov, Úrad jadrového dozoru SR, Úrad na ochranu osobných údajov SR, Úrad pre normalizáciu, metrológiu a skúšobníctvo, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Vojenské spravodajstvo a Združenie miest a obcí Slovenska.

[22] NBÚ. Akčný plán kybernetickej bezpečnosti. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf.

[23] Na úseku pomoci obetiam ransomweru (slovo zložené z anglických slov „ransom“ – výkupné a „software“ – ide o typ škodlivého kódu, ktorý môžu útočníci využiť na uzamknutie zariadenia alebo zašifrovanie jeho obsahu s cieľom vymôcť od majiteľa daného zariadenia peniaze) sa poškodeným odporúča navštíviť portál www.nomoreransom.org. Ide o iniciatívu, ktorá bola spustená v júli 2016 národnou jednotkou holandskej polície pre boj proti kriminalite páchanej prostredníctvom vyspelých technológií. Do projektu bola zapojená aj SR a stránka bola lokalizovaná do slovenského jazyka. Okrem toho, oznamovanie a následné riešenie takýchto incidentov v trestnoprávnej rovine je možné aj prostredníctvom e-mailovej adresy v rámci PZ: pckrimi@minv.sk.

[24] NBÚ. Správa o kybernetickej bezpečnosti v SR v roku 2021. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf.

[25] Hybrid CoE. What is Hybrid CoE? [online]. [2023-2-1]. Dostupné online: https://www.hybridcoe.fi/.

[26] Otvorené aplikačné programovacie rozhranie (otvorené API) je všeobecne definované ako API, ktoré používa spoločný alebo univerzálny jazyk alebo štruktúru na podporu univerzálnejšieho prístupu.

De facto ide o rozhranie, ktoré je zdieľané a otvorené pre verejné použitie. V dôvodovej správe k návrhu zákona sa uvádza, že účelom predkladaného zákona (tzv. zákonníka údajov) je o. i. zadefinovať verejný záujem a významný verejný záujem v oblasti údajov a zároveň právne vymedziť práva (oprávnenia) a povinnosti analytických jednotiek, dátového kurátora a povinných subjektov. Zámerom návrhu zákona je zabezpečiť primeranú úroveň pri manipulácii s tzv. „mojimi údajmi". Problematiku ochrany osobných údajov však upravuje aj zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 92/2022 Z. z., pričom dátovú legislatívu zastrešujú aj ďalšie právne predpisy, napr. zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení zákona č. 325/2022 Z. z., zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 351/2022 Z. z.

[27] LP/2021/55 Zákon o údajoch. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2021/55.

[28] EK. Účinnejší Kódex postupov EÚ proti šíreniu dezinformácií. [online]. [2023-1-30]. Dostupné online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan/strengthened-eu-code-practice-disinformation_sk.

[29] Dezinformácia je nepravdivá alebo zmanipulovaná informácia, ktorá je šírená zámerne s cieľom zavádzať a uškodiť, malinformácia je informácia, ktorá je založená na realite, šírená zámerne s cieľom spôsobiť ujmu a misinformácia je mylná alebo nepravdivá informácia, ktorá sa na rozdiel od dezinformácií, šíri nevedome a bez úmyslu poškodiť (teda nejde o PIO).

[30] StratCom CoE vzniklo v roku 2014. Tvoria ho experti 12 štátov vrátane Slovenska, ktoré je jeho členom od roku 2019 – pozn. autorky.

[31] LP/2020/507 Koordinovaný mechanizmus odolnosti SR voči informačným operáciám. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2020/507.

[32] Uvedená zásada reprezentuje „konanie na základe zákona a v medziach zákona" (činnosť presne podľa zákona resp. činnosť v súlade so zákonom) – limituje činnosť orgánov verejnej moci pri výkone svojich právomocí a plnení svojich povinností.

[33] Bezpečnostná stratégia SR. [online]. [2023-1-30]. Dostupné online: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

[34] Bezpečnostná stratégia SR. [online]. [2023-1-30]. Dostupné online: https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf.

[35] Obranná stratégia SR. [online]. [2023-1-30]. Dostupné online: https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf.

[36] PI/2022/176 Návrh zákona, ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady SR v čase mieru v znení neskorších predpisov. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2022/176.

[37] Teraz.sk. Bezpečnostná rada SR by mohla mať nový výbor pre hybridné hrozby. [online]. [2023-1-30]. Dostupné online: https://www.teraz.sk/slovensko/bezpecnostna-rada-sr-by-mohla-mat-nov/691544-clanok.html.

[38] MO SR. Akčný plán koordinácie boja proti hybridným hrozbám. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf.

[39] MO SR. Akčný plán koordinácie boja proti hybridným hrozbám. [online]. [2023-1-30]. Dostupné online: https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM.pdf.

[40] ÚV SR. Organizačný poriadok. [online]. [2023-1-30]. Dostupné online: https://www.vlada.gov.sk/share/uvsr/dokumenty_uvsr/organizacny-poriadok/op_uvsr_1122.pdf?csrt=9218400007279347994.

[41] PI/2021/264 Návrh zákona o lobingu. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2021/264.

[42] PI/2022/308 Návrh nariadenia vlády SR, ktorým sa ustanovujú kritické zahraničné investície. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/PI/2022/308.

[43] V zmysle § 133, ods. 1 a 2 zákona č. 300/2005 Z. z. Trestného zákona v znení zákona č. 117/2023 Z. z. sa cudzou mocou rozumejú cudzie štáty a ich vojenské alebo iné zoskupenia predstavované ich organizáciami a orgánmi, akými sú najmä osoby vykonávajúce spravodajskú činnosť, vojenskí funkcionári, diplomati a iní štátni úradníci. Cudzím činiteľom sa rozumie fyzická osoba alebo právnická osoba, ktorá síce nie je orgánom alebo zástupcom cudzieho štátu, ale vzhľadom na svoje politické, hospodárske alebo spoločenské postavenie má významný vplyv vo svojom štáte alebo v medzinárodných vzťahoch.

[44] Napr. pri trestnom čine ohrozovania utajovanej skutočnosti, útoku na orgán verejnej moci, útoku na verejného činiteľa, zneužívanie právomoci verejného činiteľa, ohýbania práva, korupcie, podnecovania, schvaľovania trestného činu, zasahovania do nezávislosti súdu, marenia spravodlivosti, marenia prípravy a priebehu volieb a referenda, ohrozenia dôvernej skutočnosti a vyhradenej skutočnosti, násilného prekročenia štátnej hranice, nedovoleného prekročenia štátnej hranice, šírenia poplašnej správy, ohovárania, spolupráce s nepriateľom, vojnovej zrady, služby v cudzom vojsku, teroristického útoku, účasti na bojovej činnosti organizovanej bojovej skupiny na území iného štátu, niektorých foriem účasti na terorizme, financovania terorizmu, cestovania na účel terorizmu, nedobrovoľného zmiznutia, založenia, podpory a propagácie hnutia smerujúceho k potlačeniu základných ľudských práv a slobôd, prejavu sympatie k hnutiu smerujúcemu k potlačeniu základných ľudských práv a slobôd, výroby, rozširovania a prechovávania extrémistického materiálu, hanobenia národa, rasy a presvedčenia, podnecovania k národnostnej, rasovej a etnickej nenávisti.

[45] LP/2022/636 Koncepcia bezpečnostného systému SR. [online]. [2023-1-30]. Dostupné online:https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/636.

[46] LP-2022-636 Návrh Koncepcie bezpečnostného systému SR. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2022/636.

[47] LP/2021/799 Národná stratégia riadenia rizík bezpečnostných hrozieb SR. [online]. [2023-1-30]. Dostupné online: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2021/799.

[48] Medzi hlavné (národné) legislatívne východiská, na ktorých je stratégia postavená, patria nasledovné právne predpisy: zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení zákona č. 146/2023 Z. z., zákon č. 128/2015 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení zákona č. 91/2016 Z. z., zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení zákona č. 497/2022 Z. z., zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo čase vojny a vojnového stavu v znení zákona č. 9/2021 Z. z., zákon č. 129/2002 Z. z. o integrovanom záchrannom systéme v znení zákona č. 351/2022 Z. z., ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení ústavného zákona č. 414/2020 Z. z., zákon č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení zákona č. 92/2022 Z. z.