

**KONCEPCIA PRE BOJ SLOVENSKEJ REPUBLIKY PROTI  
HYBRIDNÝM HROZBÁM**

## ÚVOD

Bezpečnostné prostredie v Európe prešlo za posledných niekoľko rokov zásadnými zmenami a ich výsledkom je zmena už známych konvenčných hrozieb, ktoré získali v dôsledku rozvoja technológií úplne novú dimenziu a zvýšila sa ich intenzita.

Konvenčný vojenský konflikt má v súčasnosti podstatne vyššie politické, finančné, ľudské a morálne náklady a preto sa čoraz viac štátnych a neštátnych aktérov spolieha na nevojenské prostriedky tak, aby nemuseli formálne vyhlásiť vojnu. Paralelným použitím nátlakových a podvratných činností, konvenčných a nekonvenčných metód (napr. nepriateľská propaganda, podpora extrémizmu, využívanie národnostných alebo náboženských komunít nespokojných s ich postavením v spoločnosti, podpora kriminálnych aktivít, útoky na kritickú infraštruktúru) môžu destabilizovať spoločnosť cieľových štátov a oslabiť ich tak, aby boli ľahšie ovplyvniteľné alebo v krajnom prípade aj menej odolné voči použitiu konvenčnej vojenskej sily.

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

V medzinárodnom meradle môžu byť zamerané na narušenie súdržnosti medzinárodných zoskupení, ktorých členom je Slovenská republika (ďalej len „SR“), najmä Európskej únie (ďalej len „EÚ“) a Severoatlantickej aliancie (ďalej len „NATO“) a oslabovanie vzájomnej solidarity medzi ich členmi. Boj proti tomuto typu hrozieb preto vyžaduje aj intenzívnu medzinárodnú spoluprácu a koordináciu na nadnárodnej úrovni.

EÚ vo svojej globálnej stratégii definovala hybridnú hrozbu ako jednu z najväznejších bezpečnostných výziev EÚ a smerom k jej obyvateľom a v tejto súvislosti boj proti hybridným hrozbám by mal vychádzať z odporúčaní definovaných už z prijatých dokumentov EÚ<sup>1)</sup> a dohôd o spolupráci EÚ a NATO<sup>2)</sup> s cieľom zabezpečiť čo najvyššiu efektivitu prijímaných opatrení.

SR je súčasťou celkového bezpečnostného prostredia, čelí rovnakým typom hrozieb ako iné členské štáty EÚ a NATO v rôznej intenzite, a preto tento typ hrozieb nemôže ignorovať. Hybridné stratégie sú založené na vysokej adaptabilite a iniciátori útokov prispôbujú výber použitých prostriedkov slabým miestam konkrétneho cieľového štátu. Hlavnú zodpovednosť za identifikáciu týchto slabých miest, ktoré by útočník mohol využiť, nesie konkrétny štát.

---

<sup>1)</sup> Ide najmä o: „Spoločný rámec pre boj proti hybridným hrozbám - reakcia EÚ“ (JOIN(2016) 18 final) zo 6. 4. 2016 a „Spoločné oznámenie o implementácii Spoločného rámca pre boj proti hybridným hrozbám – reakcia EÚ“ (JOIN(2017) 30 final) z 19. 7. 2017.

<sup>2)</sup> „Spoločná deklarácia prezidenta Európskej rady, predsedu Európskej komisie a generálneho tajomníka NATO“ podpísaná 8. 7. 2016 na samite EÚ-NATO vo Varšave a „Vyhlásenie o implementácii Spoločnej deklarácie prezidenta Európskej rady, predsedu Európskej komisie a generálneho tajomníka NATO“ zo 6. 12. 2016.

## **I. Aktuálny stav a cieľ koncepcie boja proti hybridným hrozbám**

Súčasne pôsobiace aktivity, ktoré ohrozujú základné atribúty štátu alebo ich funkčnosť, sa označujú ako hybridné hrozby. Hybridná hrozba je definovaná ako súbor nátlakových a podvratných činností, konvenčných a nekonvenčných, vojenských a nevojenských metód, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať na dosiahnutie konkrétnych cieľov bez formálneho vyhlásenia vojny a pod prahom zvyčajnej reakcie. Sú realizované aktivitami charakterizovanými centrálnou riadeným spravodajským a informačným pôsobením, pôsobením neštátnych aktérov, vrátane polovojenských skupín, či nasadením ozbrojených síl štátneho aktéra bez označenia. Takéto aktivity sa môžu začať skôr, než dôjde k otvorene deklarovaným vojenským operáciám. Polarizujú spoločnosť, vnášajú neistotu, a tým podkopávajú legitimitu, dôveryhodnosť, akcieschopnosť štátnych inštitúcií a demokratický ústavný poriadok a majú tak negatívny vplyv na realizáciu bezpečnostných záujmov štátov, ktoré sú im vystavené.

V zákone č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov nie je žiadnemu štátnemu orgánu SR vymedzená zodpovednosť za boj proti hybridným hrozbám a z toho dôvodu v SR v súčasnosti žiadnemu zo štátnych orgánov nie je zverená vecná pôsobnosť problematika hybridných hrozieb, preto táto koncepcia navrhuje inštitucionálny rámec pre riešenie problematiky hybridných hrozieb. V pôsobnosti jednotlivých orgánov je v uvedenom zákone stanovený rozsah ich činností v oblasti bezpečnosti.

Žiaden z rezortov tiež nedisponuje materiálnymi, technickými a ľudskými zdrojmi pre komplexné pokrytie tejto problematiky. Hybridné hrozby teda majú prierezový, medziinštitucionálny charakter a spadajú do kompetencie viacerých štátnych orgánov. Je preto mimoriadne potrebné, aby všetky štátne orgány dôsledne uplatňovali právomoci v rámci kompetencií, ktoré im boli zverené. Nebolo by účelné, a pravdepodobne ani možné, zveriť zodpovednosť za boj proti hybridným hrozbám a za plnenie všetkých súvisiacich úloh do výlučnej pôsobnosti jediného rezortu.

Účelom koncepcie je nastavenie mechanizmu výmeny informácií a kooperácie pri ich vyhodnocovaní. Cieľom koncepcie nie je vytvorenie novej inštitúcie, ktorá by mapovala všetky prejavy hybridných hrozieb, pretože ich variabilita je neobmedzená. Stanovenie rozsahu pôsobnosti takejto inštitúcie ohraničeným rámcom by tiež nebolo adekvátne.

## **II. Východiská pre vypracovanie koncepcie hybridných hrozieb**

Aj na území SR prebieha propagandistická kampaň šíriaca dezinformácie o údajných politických a ekonomických problémoch vyplývajúcich z členstva v EÚ a NATO vytváraním falošného obrazu o nevýhodách obmedzenia suverenity národných štátov v prospech európskeho integračného projektu, vstupu do schengenského priestoru a prijatia spoločnej európskej meny. Propaganda populisticky ponúka zjednodušené videnie reality a simplifikácia je tiež charakteristickým znakom ňou predkladaných riešení. Často spochybňuje samotný demokratický spôsob vlády ako údajne neschopný reagovať na aktuálne politické, ekonomické, sociálne a bezpečnostné výzvy, akými sú napr. finančná kríza alebo utečenecká a migračná kríza.

To sa môže odraziť v spoločnosti vo zvýšenej nedôvere v zastupiteľskú demokraciu, znížení záujmu o účasť vo voľbách do národných parlamentov alebo Európskeho parlamentu a tým k oslabeniu legitimity zvolených politických reprezentácií. Konečným cieľom takýchto kampaní je oslabiť samotné štáty a ich politiky, oslabiť EÚ zvnútra alebo dokonca vyvolať odchod jej členov a poškodiť tak jej geopolitické postavenie.

Do propagandistických a vplyvových aktivít sú často zapojené aj štátne orgány cudzích

mocností, najmä spravodajské služby. Tieto sa cielene snažia osloviť osoby s politickým, ekonomickým alebo spoločenským vplyvom s úmyslom ovplyvňovať ich rozhodnutia alebo získať ich pre vedomú alebo nevedomú spoluprácu pri získavaní informácií, šírení propagandy v prospech cudzej moci.

Potenciálnou hybridnou hrozbou voči bezpečnosti SR môže byť aj podpora domácich radikálnych organizácií presadzujúcich ciele totožné s cieľmi aktérov hybridných hrozieb. Radikálne subjekty môžu mať politickú a finančnú podporu zo zahraničia s cieľom propagácie nacionalistických a izolacionistických tendencií, šírenia národnostnej alebo náboženskej nenávisťi a destabilizácie spoločnosti. Podobne zneužiteľné môžu byť aj marginalizované skupiny a menšiny nespokojné so svojou situáciou a postavením v spoločnosti, ktorých negatívny postoj voči majoritnej spoločnosti môže byť využitý na vyvolávanie nepokojov. Vývoj na východe Ukrajiny a na Kryme, ale aj v konfliktových zónach na Blízkom východe a v severnej Afrike ukazuje aj na zvýšené riziko podpory poskytovanej radikálnym ozbrojeným skupinám alebo jednotlivcom a samozvaným domobranám zo strany štátnych a neštátnych aktérov, ktoré môžu byť zneužitú na diverzné útoky proti infraštruktúre, teroristické útoky alebo vyvolávanie nepokojov.

Ekonomika SR je vo veľkej miere závislá na dovoze strategických surovín, najmä energonosičov, od jedného externého dodávateľa, a táto závislosť pretrváva aj napriek prijatým opatreniam na diverzifikáciu importu energetických surovín. Energetická závislosť je zneužiteľná na vytváranie nátlaku zo strany dodávateľa a prípadná hrozba zastavenia dodávok surovín je potenciálne efektívnym nástrojom na vyvolávanie politického tlaku na SR alebo nespokojnosti medzi populáciou postihnutou sociálnym dosahom nedostatku energií.

SR ako vyspelá moderná ekonomika využíva moderné komunikačné a dátové technológie a je prepojená s globálnou informačnou infraštruktúrou. Komplexné kybernetické útoky organizované zo zahraničia s cieľom ovládnuť kľúčové systémy a znefunkčniť digitálne služby môžu byť využité ako súčasť hybridnej hrozby.

### **III. Návrh inštitucionálneho rámca**

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

- externý alebo interný politický nátlak na najvyšších štátnych predstaviteľov a štátne inštitúcie;
- ekonomický alebo energetický nátlak ako rozšírenie politického nátlaku;
- rozsiahle sabotáže proti kľúčovej infraštruktúre<sup>3)</sup>;
- 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.

Uvedené indikátory sami o sebe sú známymi a dlhodobými hrozbami, ale ich individuálny výskyt nemožno ešte považovať za hybridnú hrozbu.

---

<sup>3)</sup> Okrem kritickej infraštruktúry aj akákoľvek infraštruktúra, ktorá má zásadný význam pre štát a spoločnosť.

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 vyššie uvedených indikátorov v širšej kampani so zjavnou snahou aktéra útoku zasahovať do situácie v SR, pričom samotný aktér nie je známy alebo popiera svoju účasť na organizovaní a realizácii útoku/kampane.

Úlohy **národného kontaktného miesta pre hybridné hrozby**, ktoré plní Situačné centrum Slovenskej republiky (ďalej len „SITCEN“) sú najmä:

- a) prijímať a ďalej distribuovať na národnej úrovni produkty Hybrid fusion cell<sup>4)</sup> (ďalej len „HFC“);
- b) informovať a zdieľať informácie súvisiace s hybridnými hrozbami s HFC;
- c) byť poradcom HFC pre hybridné hrozby, ktoré sa najviac dotýkajú Slovenskej republiky;
- d) asistovať HFC zabezpečovaním vypracúvania analýz bezpečnostnej situácie relevantnými orgánmi SR pri hodnotení a predpovediach vývoja;
- e) aktualizovať svoje kontaktné údaje pre hladký tok informácií;
- f) byť pripravený ku kontaktovaniu zo strany HFC v prípade krízovej situácie;
- g) zúčastňovať sa stretnutí národných kontaktných bodov (ďalej len „POCs“) v Bruseli;
- h) zabezpečovať kontaktovanie relevantných osôb v členskej krajine.

Úlohy **národného kooperačného centra pre hybridné hrozby**, ktoré plní Národné bezpečnostné analytické centrum (ďalej len „NBAC“) sú najmä:

- a) 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;
- b) 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;
- c) v spolupráci so SITCEN doplniť súvislosti z pohľadu bezpečnostných záujmov EÚ a NATO a rozhodnúť o potrebe spracovania výstupu pre príjemcov.

Úlohy **štátnych orgánov** sú nasledovné:

- a) prvotne vyhodnocovať nahlásené incidenty vo svojej pôsobnosti vo vzťahu k hybridným hrozbám podľa indikátorov stanovených na začiatku tejto kapitoly;
- b) postupovať informáciu o incidente podľa písmena a), ktorý spĺňa niektorý z indikátorov hybridnej hrozby na ďalšie spracovanie, posúdenie alebo vyhodnotenie NBAC;
- c) poskytnúť v rámci svojej pôsobnosti NBAC doplňujúce informácie k nahlásenému incidentu podľa písmena b), ktoré budú zo strany NBAC vyhodnotené ako hybridná hrozba.

Pre plnenie úloh podľa písmena a) štátny orgán vychádza zo svojich spracovaných

---

<sup>4)</sup> Preklad v Slovenskom jazyku - Stredisko pre hybridné hrozby. Táto organizačná jednotka vznikla na základe dokumentu EÚ (odkaz č. 1 na str.1) v rámci Spravodajského a situačného centra EÚ za účelom získavania a vyhodnocovania utajovaných a voľne dostupných informácií z rôznych zdrojov zaoberajúcich sa hybridnými hrozbami. Analytické výstupy sú následne postupované členským štátom EÚ a štátom v rámci Európy. Zároveň informuje relevantné orgány EÚ.

interných predpisov alebo platných právnych predpisov v oblasti riešenia rôznych typov bezpečnostných incidentov. Informáciu podľa písmena a) postupuje štátny orgán NBAC podľa ním spracovaných jednotných pokynov pre štátne orgány na poskytovanie informácií o nahlasovaní bezpečnostných incidentov vyhodnotených ako potenciálna hybridná hrozba.

#### **IV. Opatrenia na zvyšovanie odolnosti voči hybridným hrozbám**

Princípy budovania Slovenskej republiky ako zvrchovaného a bezpečného štátu sú deklarované stratégiami a upravené právnymi predpismi a ďalšími dokumentmi na zaistenie bezpečnosti a demokratických princípov fungovania štátu a na elimináciu možných ohrození štátu a občanov.

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

Súčasnú nastavenie prijatých legislatívnych opatrení je zárukou adekvátnej reakcie štátu aj na možné hybridné hrozby a zároveň vytvára predpoklady na zvyšovanie odolnosti štátu voči ich prejavom.

Súčasťou zvyšovania odolnosti Slovenskej republiky pred hybridnými hrozbami bude zvýšenie úrovne bezpečnostného povedomia verejnosti a predstaviteľov verejnej moci o rizikách spojených s prejavmi hybridných hrozieb. Tam kde to bude účelné, zapoja štátne orgány do edukatívnych podujatí aj akademickú obec, súkromný sektor a subjekty občianskej spoločnosti.

Optimálne nastavenie národných prvkov pre vyhodnocovanie informácií, výmena skúseností v tejto oblasti a stály kontakt s prvkami obdobného zamerania na úrovni EÚ je predpokladom efektívneho riešenia problematiky hybridných hrozieb. Európske krajiny majú možnosť spolupracovať v Centre výnimočnosti pre boj proti hybridným hrozbám (ďalej len „Centrum“), ktoré zriadilo Fínsko v Helsinkách na základe výzvy EÚ adresovanej členským štátom EÚ. V súčasnosti na tomto projekte spolupracuje jedenásť členských štátov EÚ<sup>5)</sup>, Nórsko, Spojené štáty americké a možnosť zapojenia majú aj ostatné členské štáty EÚ. Centrum nadviazalo úzku spoluprácu s HFC EÚ. Taktiež má tendenciu vytvoriť priestor pre posilňovanie strategického dialógu, viesť výskumné aktivity a analytickú spoluprácu za účelom zlepšovania odolnosti a schopnosti efektívnej reakcie voči hybridným hrozbám. Vláda SR môže, na základe posúdenia podmienok členstva v Centre, zvážiť aj takúto formu spolupráce.

#### **V. Záver**

Naliehavosť riešenia problematiky hybridných hrozieb ovplyvňujúcich bezpečnostné prostredie SR si vyžaduje okrem nastavenia možností adekvátnej reakcie na elimináciu ich prejavov aj účinnú prevenciu. Ambíciou koncepcie je aj zvýšiť povedomie spoločnosti o možnostiach výskytu prejavov hybridných hrozieb a vytvoriť základ pre organizačno-inštitucionálne nastavenie identifikácie aktivít a informačných tokov k rozhodovacím orgánom ako reakcie na analýzu incidentov, ktoré môžu viesť k hybridným hrozbám.

---

<sup>5)</sup> Fínsko, Francúzsko, Nemecko, Lotyšsko, Litva, Poľsko, Švédsko, Veľká Británia, Estónsko, Španielsko, Holandsko, stav k 06.02.2018.