NÁRODNÍ STRATEGIE PRO ČELENÍ HYBRIDNÍMU PŮSOBENÍ

NÁRODNÍ STRATEGIE PRO ČELENÍ HYBRIDNÍMU PŮSOBENÍ

Praha 2021

OBSAH

1. VÝCHODISKA NÁRODNÍ STRATEGIE PRO ČELENÍ HYBRIDNÍMU PŮSOBENÍ

1. Národní strategie pro čelení hybridnímu působení (dále jen „Strategie“)[1)] stanovuje cíle a určuje nástroje potřebné k ochraně životních, strategických a dalších významných zájmů České republiky (dále jen „ČR“) definovaných v Bezpečnostní strategii České republiky (dále jen „BS“) před nepřátelským hybridním působením. Strategie vychází z BS a je rovněž v souladu s dalšími vládními bezpečnostními dokumenty, zejména s Obrannou strategií ČR a Národní strategií kybernetické bezpečnosti ČR. Vytvoření Strategie bylo zadáno Auditem národní bezpečnosti v roce 2016. Strategie doplňuje existující soustavu bezpečnostních dokumentů prostřednictvím formulace komplexní a celospolečenské politiky čelení hybridnímu působení.

2. Bezpečnost ČR je neoddělitelná od bezpečnosti euroatlantického prostoru. Strategie proto vychází ze základních strategických dokumentů Organizace Severoatlantické smlouvy (dále jen „NATO“) a Evropské unie (dále jen „EU“), principu solidarity mezi členskými zeměmi NATO a EU a cílů spojujících členské státy těchto organizací. Strategie je tak v souladu s relevantními dokumenty NATO a EU.[2)]

3. Hybridní působení je skrytá i zjevná činnost státních či nestátních aktérů (původců hybridního působení) namířená proti zranitelným prvkům demokratického státu a společnosti. Původci hybridního působení využívají politické, diplomatické, informační, vojenské, ekonomické, finanční, zpravodajské a další nástroje s cílem narušit chod

---

1) Strategie vznikla v souladu s Metodikou přípravy veřejných strategií, schválenou usnesením vlády České republiky ze dne 28. ledna 2019 č. 71.

2) Například se Závěry Rady EU o dalším úsilí za účelem posílení odolnosti a boji proti hybridním hrozbám z 10. prosince 2019, Závazkem ke zvýšení odolnosti NATO z 8. července 2016, Komuniké z Varšavského summitu NATO 2016 z 9. července 2016, Strategií role NATO v čelení hybridním hrozbám schválené v prosinci 2015 na úrovni ministrů zahraničních věcí, Společným rámcem pro čelení hybridním hrozbám ze 7. dubna 2016 nebo revizí Koncepce Evropské unie pro vojenské operace a mise pod velením EU schválené dne 2. prosince 2019.

demokratických institucí, procesy právního státu a vnitřní bezpečnost. Hybridní působení využívá i legálních a legitimně se jevících nástrojů k dosažení nepřátelských cílů a působí proti zájmům ČR. Rychlost, rozsah a intenzita hybridního působení se zvyšuje, a to i v důsledku rozvoje nových technologií.

4. V ČR je hlavní výkonnou institucí odpovědnou za čelení takovémuto hybridnímu působení vláda ČR[3)], která také přijímá opatření reagující na konkrétní projevy hybridního působení. Za čelení jednotlivým aktivitám a projevům hybridního působení jsou v rámci svých působností odpovědné příslušné resorty, a to včetně zajištění organizační infrastruktury a personálních kapacit. V rámci struktury Bezpečnostní rady státu jako poradního orgánu vlády existují platformy pro meziresortní sdílení informací a koordinaci čelení hybridnímu působení.

5. Vláda ČR stanovuje v oblasti čelení hybridnímu působení tyto strategické cíle:

   - odolná společnost, odolný stát, odolná kritická infrastruktura,
   - systémový a celostní přístup v rámci ČR,
   - schopnost adekvátní a včasné reakce.

3) V souladu s ustanovením § 28 odst. 1 zákona České národní rady č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky (kompetenční zákon) jsou v rozsahu své působnosti za připravenost a reakci na jednotlivé aktivity a projevy hybridního působení zodpovědná ministerstva a ostatní ústřední orgány státní správy.

2. STRATEGICKÝ KONTEXT

6. Dle BS prostředí, které ovlivňuje bezpečnost ČR, prochází dynamickými změnami. Jeho předvídatelnost se vzhledem k rostoucí provázanosti bezpečnostních trendů a faktorů snižuje. Pravděpodobnost přímého ohrožení území ČR masivním vojenským útokem je sice i nadále nízká, hrozbu pro bezpečnost euroatlantického prostoru včetně ČR však představuje nepřátelská činnost využívající širokého spektra nástrojů hybridního působení.

7. Původci hybridního působení mohou být státy i nestátní aktéři. Hybridní působení má komplexní povahu, a čelit mu proto lze pouze celospolečenským přístupem zahrnujícím nejen bezpečnostní složky a orgány veřejné správy, ale také relevantní součásti komerčního, mediálního, vzdělávacího a neziskového sektoru. Je namířeno proti klíčovým prvkům fungování státu a společnosti a využívá flexibilní kombinace diplomatických, informačních, vojenských, ekonomických, finančních, zpravodajských a právních nástrojů. Státními aktéry, kteří hybridní působení proti ČR využívají dlouhodobě a systematicky, jsou především autoritářské a revizionistické velmoci s regionálními či dokonce globálními mocenskými aspiracemi.

8. Hybridní působení se snaží o rozostření hranic mezi mírem, krizí a konfliktem. Záměrně usiluje o skrytost, nejednoznačnost a obtížnou přičitatelnost (atribuci) svého původce. Snaží se využívat existujících zranitelností a společenských rozporů a dále je prohlubovat. Mezi jeho cíle může patřit zpomalení či paralyzování politického rozhodovacího procesu (včetně rozhodování v oblasti obrany a bezpečnosti), oslabování důvěry občanů v ústavněprávní uspořádání a demokratické instituce a mechanismy, narušování ekonomických procesů, získání vlivu v klíčových hospodářských sektorech a strategických podnicích, manipulace či ovládnutí informačního prostředí a oslabení či ovlivnění fungování kritické infrastruktury.[4)] K tomu původci hybridního působení využívají řadu nástrojů včetně škodlivých aktivit v kybernetickém prostoru.

---

4) Kritická infrastruktura dle nařízení vlády ČR č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury, zahrnuje energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, dopravu, komunikační a informační systémy, finanční trh a měnu, nouzové služby a veřejnou správu.

9. Řada dílčích nástrojů a metod hybridního působení byla užívána i v minulosti. Došlo však k nárůstu jejich rozsahu, komplexity, technické sofistikovanosti a míry organizovanosti, což je zčásti umožněno vývojem a rozšířením nových technologií. Rozšiřující se využívání moderních technologií, například sociálních sítí a jiných internetových aplikací, přispívá k řadě nových zranitelností, které je třeba omezit.

10. ČR je vystavena hybridnímu působení zejména v těchto oblastech:

    a. ideově-hodnotové zakotvení společnosti a ústavněprávní uspořádání státu,
    b. ekonomika,
    c. bezpečnost a obrana.

Ad a: Součástí hybridního působení může být otevřené či skryté ovlivňování politických struktur (včetně politických stran) a politického rozhodovacího procesu, soudů, policie, ozbrojených sil, sdělovacích prostředků a veřejného mínění, usilující o destabilizaci či štěpení společnosti a podlomení důvěry občanů v ideově-hodnotové zakotvení země a ústavněprávní uspořádání státu, zahrnující taktéž ústavní instituce a demokratický proces.

Ad b: Hybridní působení může negativně ovlivňovat ekonomické zájmy státu. Může využívat závislosti ČR na dodávkách strategických surovin ze zahraničí (ropa, zemní plyn, jaderné palivo) a otevřenosti české ekonomiky a její orientace na export a zahraniční investice a půjčky do strategických sektorů hospodářství nebo vedoucí ke strategické závislosti na jejich poskytovateli. Může usilovat o ovládnutí strategických sektorů ekonomiky a jednotlivých klíčových podniků včetně těch, které jsou součástí kritické infrastruktury ČR. Hybridní působení se může projevit i prostřednictvím využívání moderních technologií a technologických řešení, jako jsou 5G sítě nebo umělá inteligence, pocházejících ze zemí s odlišnou ideově-hodnotovou orientací, soukromým sektorem. Rizikem je v této souvislosti také korupce, propojování diplomacie, obchodu a špionáže či vystupování v zájmu cizí moci.

Ad c: Bezpečnost ČR může být ohrožena otevřeným či skrytým použitím ozbrojeného násilí, namířeného například proti vojenskému angažmá ČR v rámci misí, operací a dalších aktivit NATO a EU, nebo agresivním nasazením zpravodajských služeb či speciálních sil jiných států na území ČR. Součástí hybridního působení může být mobilizace zájmových (nábožensky, etnicky, národnostně či jazykově definovaných) skupin či kriminálních skupin k činnosti proti bezpečnostním zájmům ČR a k narušování veřejného pořádku. Rizikem je také hybridní působení usilující o zpomalení či paralýzu rozhodovacích procesů v oblasti obrany a bezpečnosti, a to i v souvislosti s kolektivní obranou v rámci NATO a politickou a vojenskou spoluprací v rámci EU.

3. STRATEGICKÉ CÍLE

Odolná společnost, odolný stát, odolná kritická infrastruktura

11. Odolností se rozumí schopnost státu a společnosti se bez významných negativních dopadů vypořádávat s dlouhotrvajícím a intenzivním hybridním působením a v případě vzniku škod je bez prodlení napravit a obnovit plně funkční stav.

12. ČR bude v rámci svého bezpečnostního systému posilovat schopnosti včasné detekce nepřátelských hybridních aktivit, jejich přičitatelnosti (atribuce) konkrétním útočníkům a včasné reakce na ně. ČR bude schopna včas rozpoznat hybridní působení a bude na něj schopna adekvátně reagovat. Veřejné určení původce hybridního působení je politickým rozhodnutím vlády.

13. ČR bude dále posilovat odolnost státu a společnosti na základě komplexního, celospolečenského přístupu k bezpečnosti. Účelem posilování odolnosti je omezování zranitelností, jichž původci hybridního působení využívají.

14. ČR bude posilovat schopnosti prvků kritické infrastruktury uchovávat svoji dostatečnou funkčnost pro případ svého vystavení hybridnímu působení.

15. ČR bude využívat robustní a transparentní systém prověřování zahraničních investic do strategických sektorů ekonomiky a klíčových podniků, především těch, které jsou součástí kritické a další důležité infrastruktury státu.

16. ČR bude snižovat svou strategickou závislost na zemích s odlišnou ideově-hodnotovou orientací. Takováto závislost by mohla být zneužita v působení proti zájmům ČR.

17. ČR bude systematicky zvyšovat povědomí (jak klíčových společenských skupin, tak veřejnosti jako celku) o existenci hybridního působení a jeho charakteru. Problematika čelení hybridnímu působení bude součástí příslušných vzdělávacích programů a osvětových akcí. Za tímto účelem bude rozvíjena spolupráce mezi veřejnou správou, mediální sférou, komerčním, vzdělávacím a neziskovým sektorem a občanskou společností.

18. ČR bude dále posilovat schopnost identifikovat své zranitelnosti a provádět zátěžové testy simulující hybridní působení v rámci celé veřejné správy a kritické infrastruktury. V této oblasti bude vláda ČR rozvíjet spolupráci i s komerčním, mediálním, neziskovým a vzdělávacím sektorem.

19. ČR vybuduje systém strategické komunikace schopný efektivně, koherentně, věrohodně a včasně předávat informace veřejnosti a dalším typům cílového publika, a to jak průběžně a preventivně, tak v reakci na konkrétní krizovou situaci. Tento systém bude založen na koordinaci a synchronizaci komunikačních aktivit všech relevantních resortů a prvků veřejné správy.

Systémový a celostní přístup v rámci České republiky

20. Pro efektivní čelení hybridnímu působení bude posílena meziresortní spolupráce a nadresortní koordinace. ČR zvýší svou schopnost koordinace a sdílení informací mezi všemi relevantními domácími aktéry s cílem pokrýt celé spektrum užívaných nástrojů hybridního působení a zajistit trvalé situační povědomí v odpovídající kvalitě. Pro účely efektivnější výměny informací budou optimalizovány platformy v rámci Bezpečnostní rady státu a vznikne funkce koordinátora agendy čelení hybridnímu působení. Poznatky o hybridním působení a souvisejících otázkách budou pravidelně sdíleny v rámci expertní skupiny.

21. ČR bude pravidelně prověřovat připravenost svého bezpečnostního systému čelit hybridnímu působení prostřednictvím cvičení na národní i mezinárodní úrovni. Výsledky těchto cvičení budou využívány k dalšímu zefektivnění bezpečnostního systému ČR.

Schopnost adekvátní a včasné reakce

22. Členství ČR v NATO a EU je klíčovým nástrojem odstrašování původců hybridního působení. ČR se proto bude nadále aktivně účastnit činností a iniciativ těchto dvou organizací, které se týkají čelení hybridnímu působení. ČR bude usilovat o to, aby schopností NATO a EU čelit hybridnímu působení nejen využívala, ale sama k nim také hmatatelně přispívala.

23. Solidarita a vzájemná podpora členských zemí NATO a EU představuje efektivní nástroj prevence hybridního působení i reakce na jeho konkrétní projevy. ČR proto bude jednotu a solidaritu zemí NATO a EU aktivně podporovat včetně případného kolektivního pojmenování nepřátelských hybridních aktivit, jež může odradit jejich původce od pokračování v této činnosti.

24. ČR bude podporovat rovněž další rozvoj spolupráce mezi NATO a EU, která je nezbytná pro pokrytí celého spektra užívaných nástrojů hybridního působení. V tomto smyslu bude přispívat k činnosti i dalších mezinárodních iniciativ včetně Evropského centra excelence pro čelení hybridním hrozbám v Helsinkách.

25. Za účelem odstrašování aktérů využívajících metod hybridního působení bude ČR rozvíjet schopnosti reakce, které mohou zvyšovat náklady a snižovat zisky užití hybridního působení proti jejím zájmům. ČR identifikuje typové reakce na hybridní působení a tyto reakce bude pravidelně procvičovat.

26. ČR bude pokračovat v práci na indikátorech hybridního působení, které jí umožní efektivní a včasnou reakci.

27. ČR bude v reakci na hybridní působení pro sdělování koordinovaných stanovisek státu využívat svůj systém strategické komunikace. Tato komunikace bude zaměřena na domácí i zahraniční publikum včetně původců hybridního působení.

28. ČR vyhodnotí a rozpracuje možnosti užití veřejného určení aktérů hybridního působení.

29. ČR je připravena na nepřátelskou hybridní činnost reagovat odvetnými opatřeními (včetně sankcí) a dalšími nástroji svými i nástroji mezinárodních organizací, jichž je členem. Součástí adekvátní reakce bude i rozvoj schopnosti vyhodnocovat její účinnost, což bude sloužit jako zpětná vazba pro další postup.

4. IMPLEMENTACE

30. Strategie bude pravidelně aktualizována v návaznosti na vývoj mezinárodního bezpečnostního prostředí. Na Strategii bude navazovat akční plán obsahující konkrétní opatření a kroky. Jeho plnění bude každoročně vyhodnocováno a plán bude dle potřeby aktualizován.