MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

AUDIT NÁRODNÍ BEZPEČNOSTI

Praha, 2016

SHRNUTÍ

Evropa se po delší době relativního bezpečí potýká znovu se zhoršenou bezpečnostní situací. Po utlumení hospodářské krize posledních let, která otřásla důvěrou evropské veřejnosti v některé aspekty integrace, čelí Evropa mimořádné migrační vlně, jež přináší řadu palčivých otázek sociálních, humanitárních, politických, kulturních, a s nimi významné otázky bezpečnostní. Podle současných poznatků došlo od ledna do září roku 2016 na území EU k 11 teroristickým útokům, které si vyžádaly celkem 120 obětí. Po téměř dvou desítkách let v Evropě opět vypukl ozbrojený konflikt, došlo k anexi části území suverénního státu. Na periferii Evropy i v jejím blízkém sousedství se v posledních letech dramaticky zhoršila bezpečnostní situace ve všech ohledech včetně aspektu vojenského. Po letech se tak EU musí vypořádat s komplikovanou mezinárodní situací a potenciální vojenskou hrozbou nejen ve vzdáleném zahraničí, ale ve své bezprostřední blízkosti.

Zhoršená bezpečnostní situace v Evropě dolehla na ČR zatím jen okrajově. Přesto se musíme věnovat plné škále hrozeb, s nimiž se kontinent potýká. Nelze podceňovat ani případné vojenské hrozby. Expertní skupina složená ze zástupců všech členů bezpečnostní komunity a některých dalších ústředních orgánů státní správy, jež měla na začátku letošního roku za úkol stanovit osnovu materiálu, však i z důvodu rozsahu materiálu rozhodla omezit témata na ty oblasti hrozeb, které mají přímou vazbu na vnitřní bezpečnost státu. Vnější bezpečnostní podmínky nezasahují jen do tradičních oblastí, jako je extremismus a s ním spojená radikalizace, nebo organizovaný zločin, kde je v evropském kontextu aktuálně zaznamenán bezprecedentní nárůst trestné činnosti v oblasti převaděčství. Naši vnitřní bezpečnost ohrožují i hrozby relativně nové, související s informační válkou nebo organizovanými kybernetickými útoky. Svět se globalizoval a lokální problémy na druhé straně nebo na jiných kontinentech mohou mít zásadní vliv na bezpečnostní vývoj v naší zemi. Zároveň se ČR potýká s hrozbou, která, jakkoli není v Auditu zpracována a nejedná se o téma primárně bezpečnostní, její dopad na vývoj společnosti si v závažnosti nezadá s žádnou ze zpracovaných kapitol a každá vláda musí toto téma považovat za svou prioritu. Touto hrozbou je demografický vývoj ČR, jehož klesající křivka negativně ovlivňuje všechny aspekty života společnosti od vyšších nároků na sociální smír, po neschopnost společnosti zajistit dostatečnou pracovní sílu pro celou řadu oblastí.

Hodnocení hrozeb musí pracovat nejen s jejich přímým vlivem, ale i se všemi sekundárními dopady, které hrozba vyvolává. V případě teroristických útoků nedosahuje dopad i celého komplexu útoků spáchaných v jednom roce v rámci EU ani zlomku celkového počtu obětí, které mají na stejném území na svědomí např. dopravní nehody, jejich dopad na vnitřní bezpečnost je však mnohem širší. Patří sem radikalizace části majoritní populace, nárůst extremistických a populistických uskupení a politických proudů, které podobně jako teroristé šíří nenávist, strach a nabízejí jednoduchá a radikální řešení. Celospolečenské psychologické, ekonomické a politické dopady teroristických útoků tak mohou výrazně převážit dopady faktické.

Hrozby lze třídit podle různých kritérií (podle původce – jedinec, stát, vyšší moc aj.; podle referenčního objektu - fyzická bezpečnost, bezpečnost objektů aj.; podle oblasti, ve které se hrozba projeví - ekonomické, vojenské, ekologické, politické aj.), tato třídění používaná v akademických textech však hned z několika důvodů nepostihují potřeby shrnutí závěrů Auditu národní bezpečnosti (dále jen „Audit“). Deset témat, která Audit zpracovává, nepředstavuje vyčerpávající výčet bezpečnostních hrozeb, kterým ČR musí zvládnout jak zabránit, tak v případě jejich propuknutí musí umět těmto hrozbám efektivně čelit, ale obsahuje pouze témata, která svou závažností dosahují míry způsobilé významně poškodit kvalitu vnitřní bezpečnosti státu. Dalším důvodem je současná propojenost témat, která se projevuje i v textu provázáním odkazů mezi jednotlivými kapitolami, přičemž se nejedná pouze o oblíbené „mediální zkratky“ propojující migraci a terorismus. V rámci Auditu není výjimkou propojení i pěti a více tematických celků, přičemž vzájemné vazby mezi hrozbami propojenými zpravidla jednotícím motivem jejich původce výrazně zvyšují hodnocení jejich závažnosti.

Z toho důvodu při shrnutí textu dále zpracované hrozby nijak netřídíme.

Lze však konstatovat, že míru závažnosti zpracovaných hrozeb do velké míry ovlivňuje jejich provázanost. Do této skupiny hrozeb částečně spadá kapitola energetická, průmyslová a surovinová bezpečnost a dále kapitoly hrozby v kyberprostoru, působení cizí moci, ale i kapitola extremismus, terorismus a bezpečnostní aspekty migrace a především zastřešující kapitola hybridní hrozby a jejich vliv na bezpečnost občanů. Kapitoly, jejichž hrozby mají větší potenciál být provázané v rámci jednotné kampaně, pak častěji definují systémové nedostatky připravenosti státu hrozby detekovat, absenci strategického zakotvení řešení hrozby, nedostatečnou nebo zcela chybějící kapacitu pro plnění úkolů při předcházení a potírání hrozeb, nedostatky nebo neexistenci cvičení praktických situací souvisejících s propuknutím hrozby a částečně i nedostatky legislativní.

Vzhledem k rozsahu Auditu není smyslem shrnutí opakovat ve zkrácené formě východiska a doporučení každé jednotlivé kapitoly, je však naší ambicí vyjádřit se alespoň obecně k okruhům úkolů či doporučení, které Audit vládě předkládá k úvaze. Napříč celým dokumentem můžeme identifikovat několik oblastí, ve kterých jednotlivé kapitoly dospěly k podobným závěrům, a to jak tematicky provázaným nebo izolovaným. Vzhledem k potřebě propojit doporučení a úkoly tam, kde jejich propojení může znamenat přínos ať z hlediska tematické spřízněnosti, nebo kvůli potřebě rozložit účelně finanční prostředky státu při jejich naplňování, považujeme za nutné navržená opatření rozčlenit do větších celků a na návrhy, u nichž to jejich specifičnost odůvodňuje, poukázat zvlášť.

ČR má dílčí strategie a koncepce pro většinu jednotlivých hrozeb, nicméně ty definují, jak dosáhnout ideálního stavu. Audit si na druhou stranu stanovil za cíl zjistit, jak na tom jsme právě teď v roce 2016, jak je stát připraven čelit bezpečnostním hrozbám ve vytipovaných nejzávažnějších oblastech a jaká je jeho odolnost při přímé konfrontaci s nebezpečím. Audit posuzoval, zda máme dobře nastavenou legislativu a jak pružně je bezpečnostní systém schopný reagovat. Prověřil také schopnost komunikace a spolupráce jednotlivých složek a dále to, zda jsou adekvátně zapojeny instituce, bezpečnostní sbory, orgány krizového řízení a tam, kde je to třeba i kraje, města a obce i soukromá sféra. Zhodnotil i kapacitu, kterou stát pro předcházení nebo potlačování jednotlivých hrozeb vyčlenil. Proto můžeme vymezit následující okruhy, ve kterých závěry jednotlivých kapitol vznesly doporučení:

- **Legislativní** (doporučení od obecného požadavku revidovat právní nástroje po velmi konkrétní návrhy dílčích změn příslušné úpravy vznesly všechny kapitoly kromě antropogenních hrozeb)

Kromě opakovaných návrhů směřujících do oblasti práva trestního stojí za zmínku kritika nedostatečného zohlednění bezpečnostních aspektů v případě výkonu práva na svobodný přístup k informacím podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (působení cizí moci a hrozby v kyberprostoru).

- **Personální/kapacitní** – několik kapitol signalizovalo potřebu navýšit kapacitu osob, které se hrozbou zabývají, případně stabilizovat personální situaci u kompetentních orgánů, dále byla zmíněna i otázka zvyšování specializace. Jedná se o kapitoly hrozby antropogenní, hrozby přírodní, bezpečnostní aspekty migrace, organizovaný zločin a hrozby v kyberprostoru. V několika případech kapitoly identifikovaly přímo absenci kapacity k řešení problému (působení cizí moci, hybridní hrozby a jejich vliv na bezpečnost občanů). Častý je rovněž požadavek na další vzdělávání osob odpovědných za řešení hrozby (migrace, působení cizí moci).

V souvislosti s doporučeními, která míří do oblasti personální, není bez zajímavosti, že dvě kapitoly identifikovaly jako **problematickou úpravu zákona č. 234/2014 Sb., o státní službě**, a to konkrétně jako faktor snižující personální flexibilitu státní správy (migrace) a úpravu negativně ovlivňující otevřenost státní správy vůči odborníkům ze soukromého sektoru (organizovaný zločin).

- Z povahy činnosti bezpečnostní komunity, a to nejen v případě zpravodajských služeb, přirozeně vyplývá trend poznatky i metodu práce utajovat. Přesto v případě Auditu nejsou doporučení týkající se **potřeby posílit koordinaci pro vyhodnocování hrozeb** jen povinným upozorněním na známý fakt. Zařazení tématu hybridních hrozeb mezi 10 nejzávažnějších bezpečnostních témat odhalilo nedostatek koordinace právě v případě aktivní hybridní kampaně vedené s úmyslem poškodit nejen ČR, ale i celou evropskou integraci, které se ČR účastní. Moderní aspekt této situace je spatřován zejména v tom, že vyhodnocování a návrhy opatření nelze omezit jen na bezpečnostní komunitu, ale systém musí umět propojit větší okruh oblastí sociálního, ekonomického, právního i politického života společnosti tak, aby dokázal propojit dílčí útoky nízké závažnosti a správně odhadoval míru rizika spojeného s jejich souhrnem. Potřebu koordinace tak zdůrazňují téměř všechny kapitoly Auditu, nicméně kapitoly hybridní hrozby a jejich vliv na bezpečnost občanů a působení cizí moci zdůrazňují právě tento aspekt identifikovaného nedostatku a hodnotí jej jako závažný.

- V úzké souvislosti s předchozí poznámkou pak Audit přichází s jasně identifikovanou potřebou podpory **dlouhodobého rozvoje komunikační infrastruktury a technologií veřejné správy a eGovernmentu** pro využití při zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací. Bezpečná a dostatečně odolná cesta přenosu informací mezi dotčenými složkami státní moci, jejichž informační a rozhodovací potenciál je klíčový pro případ rychlé reakce, je nezbytným technickým předpokladem odolnosti státu vůči všem hrozbám bez rozdílu. Tento požadavek se objevuje ve více než polovině zpracovaných kapitol a je doprovázen i definicí potřeby cvičit využívání komunikačních kanálů v krizových situacích.

- Jako zásadní z Auditu vyplývá téma **spolupráce s veřejností a soukromými subjekty**, která prostupuje celou řadou kapitol ve formě **požadavku na větší zapojení soukromých subjektů na odpovědnosti za zajišťování bezpečnosti** ve spolupráci se státem (terorismus, antropogenní hrozby, přírodní hrozby), tak ve formě **aktivní komunikace státu a veřejnosti** (migrace, extremismus, působení cizí moci, terorismus, přírodní hrozby a hybridní hrozby). Z kapitol hybridní hrozby a působení cizí moci vyplynul požadavek na vytvoření koncepčního přístupu (případně posílení, jak je uvedeno) ke **strategické komunikaci** státu jak dovnitř ČR, tak vně.

- Mezi úkoly s dlouhodobým dopadem zazněl opakovaně i požadavek na **doplnění témat v rámci vzdělávacích programů školského systému**, ať už se jedná o výchovu k bezpečnosti, nebo posilování občanské nebo mediální gramotnosti (antropogenní hrozby, přírodní hrozby, hybridní hrozby, působení cizí moci).

- Několika kapitolami prochází i jednoznačná **podpora a další prohlubování bezpečnostního výzkumu**, který je jedním z nepřímých nástrojů rozvoje bezpečnosti. Umožňuje systematické využívání kapacit dynamicky se rozvíjejícího výzkumného sektoru k rozvoji schopností bezpečnostního systému. Je však třeba mít na zřeteli, že jde o nástroj, který přináší výsledky ve středně a dlouhodobém horizontu, a jeho efektivní fungování je podmíněno úzkou spoluprací ze strany potenciálních uživatelů výsledků této výzkumné činnosti v přípravě nástrojů podpory, ale zejména při realizaci projektů, testování a evaluaci výsledků a jejich transferu do praxe. Na tento aspekt rozvoje bezpečnosti odkazují kapitoly přírodní hrozby, antropogenní hrozby, bezpečnostní aspekty migrace a působení cizí moci.

Předložením materiálu ke schválení vládě práce spojená s Auditem nekončí, nicméně pozitivní je, že bezpečnostní komunita rozhodně nestojí na začátku a bez zkušeností. Audit prokázal, že zpracované hrozby jsou v systému podchyceny dobře a identifikované problémy spojené s jejich řešením jsou problémy dílčí, které pravidelně vyvstávají v běžném bezpečnostním provozu a jejich řešení jsou navrhována, diskutována a prosazována průběžně. Zároveň však Audit odhalil nedostatečnou kapacitu systému vyhodnocovat a reagovat na komplexní propojování hrozeb. V několika oblastech doporučení, na jejichž plnění panuje v bezpečnostní komunitě shoda, již byly podniknuty konkrétní kroky k plnění doporučených opatření. **Po schválení Auditu vládou MV ve**

spolupráci s dalšími gestory vypracuje akční plán k plnění jednotlivých úkolů a stanoví pravidelné termíny jeho vyhodnocování, přičemž vládu bude o plnění úkolů informovat v jím stanovených termínech. Konkrétní forma plnění doporučení bude součástí akčního plánu a vznikne ve spolupráci s gestory jednotlivých úkolů.

OBSAH

ÚVOD

Audit byl zpracován na základě zadání předsedy vlády. Věnuje se deseti okruhům hrozeb, které byly expertní skupinou v lednu roku 2016 vybrány jako osnova materiálu.

Co je cílem Auditu?

Audit ověřuje dvě základní schopnosti státu, a to schopnost identifikovat konkrétní bezpečnostní hrozbu a přijmout vůči ní preventivní opatření a schopnost reagovat na nastalou krizi, kterou je potřeba řešit. Každá kapitola tak přináší odpovědi na otázky: Je stávající **legislativa** dostatečná? Má stát k dispozici **dostatečné kapacity**? Má stát reálnou schopnost přijímat příslušná opatření a **konat v okamžiku**, kdy je to **potřeba**?

Cílem Auditu ale také je podívat se na známé hrozby změněnou bezpečnostní optikou, hledat jejich průniky, posoudit míru jejich závažnosti novým přístupem, který bere v úvahu vnitrostátní, ale i mezinárodní kontext, ve kterém se Česká republika nachází.

Komu je Audit určen?

Zpracovaný materiál má obecnou povahu. Na jeho vzniku se podílelo více než sto odborníků rozdělených do pracovních týmů podle kvalifikace. Nebylo však záměrem vytvořit materiál, který by obsáhl detailně každé vybrané téma. Naopak úkolem jednotlivých týmů bylo vytvořit rámcový přehled problémů dané oblasti, ten vyhodnotit a identifikovat ty nejzávažnější hrozby pro další vývoj naší země.

Výsledný materiál má proto obecnou povahu a ukazuje směr, kterým se vláda ČR má při řešení bezpečnostních výzev vydat. Stručnost materiálu umožňuje jednak potřebnou orientaci v něm a zároveň umožňuje jeho prezentaci veřejnosti, neboť kromě vytyčení směru dalších kroků v oblasti vnitřní bezpečnosti musí materiál plnit i informační úlohu směrem k veřejnosti.

Veřejnost má právo vědět, jakým hrozbám společnost čelí a na jaké výzvy je stát povinen se připravit. Z taktických důvodů však není možné poskytovat informace tohoto charakteru v detailech, proto značnou část práce na výsledném textu zabralo právě vyvažování informací tak, aby veřejnosti poskytly představu o problémech, před kterými stojíme, ale zároveň nepředstavovaly návod pro potenciálního útočníka.

Hodnocení hrozeb

Řada kapitol používá pro zhodnocení relevance identifikované hrozby pro ČR stupnici vysoká - střední – nízká. Tato stupnice je využita jen v těch kapitolách, kde ji pracovní skupiny považovaly za aplikovatelnou. Je však nutné upozornit, že hodnocení relevance nelze využít napříč kapitolami. Míra závažnosti jednotlivých hrozeb je tak tedy hodnocena pouze izolovaně v rámci jednotlivých kapitol. Kromě toho je třeba mít na paměti, že se míra závažnosti liší podle toho, zda je sama hrozby izolovaná, nebo zda je propojena s jinými v rámci hybridní kampaně s cílem negativně působit na fungování státu.

Struktura kapitol

Každé téma se skládá ze čtyř částí: **popisu a evaluace hrozby** a rizik z ní vyplývajících pro ČR, výčtu **odpovědných institucí** v rámci bezpečnostního systému ČR a **základních nástrojů** (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik, **SWOT analýzy dané oblasti** a na závěr **konkrétních doporučení pro vládu** k posílení odolnosti.

Nad rámec materiálu je samostatně zpracována ještě kapitola Stabilita měny a finančních institucí, kterou Česká národní banka bude předkládat BRS i vládě ke schválení nezávisle na zbytku materiálu.

TERORISMUS

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Rozsáhlá destabilizace některých států Blízkého východu a severní Afriky, nástup tzv. Islámského státu a dalších teroristických skupin, fenomén zahraničních bojovníků, migrační krize, radikalizace jednotlivců a skupin v různých segmentech společnosti (např. skrze internetovou propagandu a sociální média) – to vše jsou vzájemně provázané faktory, které ve svém souhrnu zvyšují riziko provedení teroristického útoku v Evropě.

Za terorismus lze označit takové jednání, které je politicky, nábožensky či jinak ideologicky motivováno a užívá násilí či jeho hrozby zejména s cílem vyvolat strach. Proti hrozbě terorismu není v současné době zcela imunní žádná země, ČR nevyjímaje. Na druhou stranu je relevance a struktura této hrozby v jednotlivých regionech i státech odlišná - západní Evropa je např. radikálním islamismem ohrožena z historických i demografických důvodů daleko více, než Evropa střední. Tento materiál by měl zhodnotit význam rizik plynoucích z terorismu specificky ve vztahu k ČR. Při tom je třeba vzít v úvahu aktuální nastavení a stav bezpečnostního systému, zhodnotit dostatečnost, popř. identifikovat deficity: a) legislativy, b) kapacit a c) reálné schopnosti reagovat, a následně přijmout případná doporučení ke zlepšení tam, kde je to s přihlédnutím k výše uvedeným faktorům vhodné (veškerá opatření musí vycházet z kvalitní analýzy rizik a vynaložené síly a prostředky musí odpovídat významu konkrétní hrozby).

Současný terorismus má řadu příčin, přičemž většina z nich má svůj původ za hranicemi ČR. Některé z nich není ČR bez pomoci dalších partnerů schopna zásadně ovlivnit. I tak je nicméně důležité zhodnotit aktuální připravenost a schopnost ČR předcházet teroristickým aktivitám (nejen) na svém území, omezovat následky a dopady případných teroristických útoků a aktivně se podílet na stabilizaci bezpečnostního prostředí v Evropě a ve světě.

Tato kapitola se nevěnuje problematice *kyberterorismu*[1], neboť ta je řešena v kapitole „Hrozby v kyberprostoru“. Terorismu *jakožto nástroji hybridní války* se blíže věnuje kapitola Hybridní hrozby, fenomén radikalizace je blíže pojednán v kapitole Extremismus. Při zpracovávání kapitoly byly využity poznatky i z oblasti bezpečnostního výzkumu, např. projektu „Islám v ČR: etablování muslimů ve veřejném prostoru“, který byl realizován v rámci Programu bezpečnostního výzkumu ČR v letech 2010-2015.

[1] NBÚ definuje kyberterorismus následovně: „kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.“

2. Popis a evaluace hrozby

Teroristickou hrozbu jako celek je možné rozčlenit do několika dílčích oblastí, z nichž každá si žádá samostatné zhodnocení relevance pro ČR[2]. Následující text člení teroristickou hrozbu ze tří hledisek: 1) z hlediska původce hrozby; 2) z hlediska cíle útoku; 3) z hlediska nástrojů terorismu. Při hodnocení relevance hrozby pro ČR byla použita kritéria pravděpodobnosti a závažnosti dopadu, jejichž kombinací je následně relevance hodnocena na škále nízká-střední-vysoká.

I) Teroristická hrozba z hlediska původce

a) Islámský radikalismus

Zhodnocení relevance hrozby pro ČR: **Nízká**

V současné Evropě je s teroristickou hrozbou spojován nejčastěji islámský radikalismus (je nicméně potřeba připomenout, že tomu tak nebylo vždy a např. v 70. a 80. letech dominoval Evropě terorismus separatistický a radikálně levicový). Řadu z těch útoků, které si v poslední době získaly největší veřejnou pozornost (neboť právě tou, a nikoliv reálnými dopady či počtem obětí, lze nejlépe měřit význam daného útoku), spáchaly osoby hlásící se k radikálně islamistické ideologii, případně přímo napojené na mezinárodní teroristické organizace (např. na tzv. Islámský stát).

Navzdory tomuto faktu lze hodnotit rizika plynoucí z islámského radikalismu pro ČR zatím jako nízká, nikoliv však nulová. ČR je v tomto ohledu v odlišném postavení, než země západní Evropy. Muslimská komunita v ČR je výrazně méně početná, než např. v zemích západní či severní Evropy, a doposud v ní nebyly zaznamenány rozsáhlejší radikalizační tendence. ČR doposud byla do značné míry na okraji zájmu mezinárodních teroristických organizací, které mají v naší zemi jen minimální zázemí pro svou činnost (což souvisí právě i s velikostí a charakteristikou české muslimské komunity).

Zkušenosti ze západní Evropy také ukazují, že radikalizace často souvisí rovněž s fenoménem sociálního vyloučení – v tomto směru je pozitivní, že naprostá většina členů české muslimské komunity je ekonomicky dobře integrovaná a v ČR nedochází k vytváření sociálně vyloučených lokalit či paralelních společenských struktur, které by fungovaly jako zázemí pro teroristické aktivity.

To vše sice snižuje relevanci hrozby islámského radikalismu pro ČR, tato ovšem v žádném případě není nulová. ČR je součástí euroatlantických struktur i globální koalice proti tzv. Islámskému státu a aktivně vystupuje proti islámskému radikalismu – to z ní samo o sobě činí možný cíl teroristického útoku. Teroristé se mohou na ČR zaměřit také kvůli (reálným či domnělým) nedostatkům v bezpečnostním systému, případně kvůli přitažlivosti některých cílů na českém území (např. židovské objekty, Rádio Svobodná Evropa atd.).

Zatímco pravděpodobnost vysokoprofilového útoku ze strany mezinárodních teroristických organizací je v ČR z výše uvedených důvodů spíše nízká, rozhodně nelze vyloučit radikalizaci jednotlivců či malých skupin inspirovaných radikální islamistickou ideologií, kteří se mohou pokusit o násilnou akci i bez vazby na etablované organizace (podrobněji viz oddíl věnovaný problematice teroristů jednajících samostatně).

[2] Následující část rozčleňuje hrozbu terorismu do jednotlivých dílčích oblastí v souladu s osnovou a metodikou k Auditu. Jednotlivé hrozby jsou hodnoceny dle relevance pro ČR na škále nulová-nízká-střední-vysoká, která zohledňuje pravděpodobnost naplnění hrozby v příštích dvou až třech letech a její možné dopady.

b) Politický extremismus, ostatní teroristické skupiny

Zhodnocení relevance hrozby pro ČR: **Nízká**

Zatímco fenomén islámského radikalismu dosud zasahuje ČR (ve srovnání se státy západní Evropy) jen v malé míře, s pravicovým (PEX) a levicovým (LEX) extremismem má ČR dlouholeté zkušenosti. Této problematice se blíže věnuje kapitola věnovaná extremismu, zde je na místě krátké zhodnocení možné teroristické hrozby, plynoucí ze skupin či jednotlivců ovlivněných radikální politickou ideologií.

V ČR působí množství skupin, které je možné označit za extremistické, přičemž některé z nich mají mezinárodní vazby. Členové těchto skupin se dopouští trestné činnosti, v některých případech i násilného charakteru. Přes vyšší četnost výskytu tohoto fenoménu ve srovnání s islámským radikalismem lze konstatovat, že riziko spáchání teroristického útoku členy PEX a LEX skupin není vyšší, než je tomu u islámských radikálů. Je tomu tak především proto, že aktivity PEX a LEX scény jsou dlouhodobě monitorovány ze strany bezpečnostních složek a v současnosti je pravděpodobnost, že tyto skupiny zahrnou do svého úsilí o systémové změny teroristické metody, spíše nízká. K tomu výrazně přispívá i názorová roztříštěnost české extremistické scény a převládající snaha získat na svou stranu sympatie širší veřejnosti, kterou by přechod k teroristickým metodám mohl narušit.

Podobně jako bylo zmíněno v případě islámského radikalismu, nelze nicméně vyloučit radikalizaci jednotlivců či malých skupin inspirovaných PEX či LEX ideologií, kteří se mohou pokusit o násilnou akci i bez vazby na etablované organizace (podrobněji viz oddíl věnovaný teroristům jednajícím samostatně).

Stejné hodnocení lze vztáhnout i na ostatní skupiny či jednotlivce ovlivněné jinou ideologií (ať již politickou či náboženskou), než je islámský radikalismus, PEX a LEX.

c) Teroristé jednající samostatně (osamělí vlci)

Zhodnocení relevance hrozby pro ČR: **Střední**

Ačkoliv ČR patří mezi několik málo evropských zemí, které ve své novodobé historii nezažily klasický teroristický útok, v uplynulých dvou letech došlo na našem území k nejméně dvěma případům napadení ze strany samostatně jednajících aktivních útočníků s tragickými následky. Jedním z nich byla střelba v Uherském Brodě v únoru 2015, která si vyžádala osm obětí na životech. Ačkoliv v tomto případě nebyl podle dostupných informací útočník motivován ideologicky, a o teroristický útok ve vlastním slova smyslu tedy nešlo, modus operandi se fakticky nelišil např. od střelby v redakci časopisu Charlie Hebdo, ke které se přihlásila mezinárodní teroristická organizace. Útoky psychicky narušených jedinců či jednotlivců motivovaných jinak než ideologicky mohou mít tedy stejný průběh i dopady, jako akce teroristů. V tomto ohledu lze na obě skupiny aplikovat i podobná opatření, proto se pro potřeby této kapitoly mezi těmito skupinami nerozlišuje.

I na základě této zkušenosti lze předpokládat, že případný teroristický útok na českém území by mohl mít spíše charakter akce jednotlivce (či malé skupiny), který může být aktivitami mezinárodních teroristických skupin inspirován, ale nemusí na ně mít žádnou přímou vazbu. V tomto případě může jít o osobu hlásící se k islámskému radikalismu, ale stejně tak může být tento jedinec motivován jinou radikální ideologií (příkladem z nedávné minulosti je útok Anderse Breivika v Norsku, který patří mezi nejkrvavější incidenty posledních let – Breivik byl pravicový extremista, který naopak vnímal islám jako hrozbu).

Radikalizaci mohou podlehnout i osoby bez bližších vazeb v okolní komunitě (např. konvertité), které mohou být inspirovány např. internetovou propagandou. Boj proti šíření nenávistného a radikálního obsahu v prostředí internetu a sociálních médií proto musí být jednou z priorit. Je rovněž důležité sledovat aktivity veškerých extremistických skupin, působících na našem území – i

kdyby tyto skupiny samy neusilovaly o provádění násilných akcí, mohou inspirovat jednotlivce, kteří se pokusí radikální program realizovat v praxi. Nemalé riziko v tomto ohledu představují (v ČR poměrně rozšířené) aktivity islamofobních skupin, kterým se dostává značné mediální pozornosti (a v některých případech i politické podpory), a které mohou:

i) přispívat k pocitu odcizení a společenského vyloučení a následné radikalizaci jednotlivců z řad muslimské menšiny v ČR,

ii) svou radikální „válečnou" rétorikou a šířením strachu a pocitu ohrožení vyprovokovat jednotlivce či malou skupinu k nezávislé násilné akci, jejímž cílem mohou být členové muslimské komunity či imigranti, ale také „zrádci" z řad politické či společenské elity či vybraných členů občanské společnosti (právě po Breivikově vzoru).

Útoku samostatně jednajícího teroristy je velmi obtížné předem zabránit, a tak je kromě prevence radikalizace nutné se soustředit rovněž na připravenost a schopnost zejména Policie ČR rychle reagovat na tyto situace, na přípravu vybraných potenciálních cílů na takovéto či obdobné útoky a v neposlední řadě na zmírňování následků případného incidentu. Velmi důležité je proto dále posilovat a důsledně implementovat opatření přijatá po útoku v Uherském Brodě (např. posilování a vybavení prvosledových hlídek Policie ČR, procvičení co největšího počtu příslušníků pořádkové policie pro situaci typu AMOK, úprava procesu vydávání a odnímání zbrojních průkazů, vznik registru přestupků atd.).

d) Zahraniční bojovníci[3]

Zhodnocení relevance hrozby pro ČR: **Střední**

Fenomén zahraničních bojovníků se týká cizinců zapojených v různých ozbrojených konfliktech (např. i v bojích na Ukrajině), ale v poslední době je skloňován zejména v souvislosti s ozbrojenými střety v Sýrii a Iráku. V tomto komplikovaném a krvavém konfliktu je zapojena řada hráčů a skupin, z nichž mnohé mají významnou zahraniční podporu. Této nepřehledné situace a mocenského vakua využily i některé teroristické organizace k ovládnutí poměrně rozsáhlého území a získání nových prostředků pro vlastní činnost (např. tzv. Islámský stát, fronta al-Nusra – přejmenována na Jabhat Fateh al-Sham, aj.). Tyto skupiny prostřednictvím propracované propagandy verbují nové sympatizanty k tomu, aby se do konfliktů na straně teroristických organizací rovněž aktivně zapojili. Nábor zahraničních bojovníků probíhá i v zemích EU, odkud již do konfliktních zón (k Sýrii a Iráku lze připočíst také Libyi či Jemen) odešly bojovat tisíce osob.

Fenomén zahraničních bojovníků představuje závažný problém zejména pro státy západní Evropy – touto cestou dochází k radikalizaci jejich občanů, kteří mohou po návratu představovat významné bezpečnostní riziko. Během pobytu v konfliktní zóně získávají bojové zkušenosti a vysoká je také míra jejich ideologické indoktrinace. Obavy panují především z toho, že by se tyto osoby mohly pokoušet o aktivní organizaci teroristických útoků na evropském území (k čemuž také skutečně dochází).

Jakkoliv se jedná do značné míry o celoevropský problém, ČR nepatří mezi státy významně zasažené tímto fenoménem. Problém nicméně představují zahraniční bojovníci (občané cizích států) tranzitující přes české území, neboť takové případy již byly v minulosti zaznamenány.

[3] Některé (zejména zahraniční) dokumenty, rozlišují mezi pojmem „zahraniční bojovníci" (*foreign fighters*) a „zahraniční terorističtí bojovníci" (*foreign terrorist fighters*), přičemž první z těchto termínů obecně označuje osoby, které se aktivně účastní zahraničního ozbrojeného konfliktu (a to nikoliv jako členové ozbrojených sil vlastního státu, případně bez jeho souhlasu), druhý termín se vztahuje úzce jen na ty zahraniční bojovníky, kteří bojují na straně teroristických organizací.

Pokud definici zahraničních bojovníků rozšíříme i na ostatní konflikty, pak je možné zmínit, že několik Čechů se účastní (nebo se v minulosti zapojilo do) bojů na Ukrajině (a to na obou stranách konfliktu). Aktivity těchto osob rovněž představují určité bezpečnostní riziko pro vnitřní bezpečnost ČR, např. v tom ohledu, že by se tito lidé mohli stát nástrojem zahraničního vlivového působení[4]. Jejich rizikovost z hlediska teroristických aktivit je nicméně v současné době spíše nízká.

Z výše uvedených důvodů hodnotíme relevanci hrozby zahraničních bojovníků pro ČR jako střední. Aby se do budoucna zabránilo jejímu zvyšování, je především důležité věnovat pozornost boji proti radikalizaci a náboru bojovníků, zneužívání internetu včetně sociálních médií, formování paramilitárních skupin a zahraničnímu vlivovému působení.

II) Teroristická hrozba z hlediska cíle útoku

a) Útok na kritickou infrastrukturu

Zhodnocení relevance hrozby pro ČR: **Střední**

Ochrana vlastní kritické infrastruktury je jedním z klíčových úkolů každého státu. V ČR je tato oblast poměrně kvalitně legislativně ošetřena (viz následující oddíl této kapitoly věnovaný popisu bezpečnostního systému). Tato oblast zahrnuje i problematiku kyberterorismu, za který lze v užším pojetí považovat politicky, nábožensky nebo ideově motivované aktivity v kyberprostoru, jako je např. úmyslné a rozsáhlé narušení počítačových sítí a zařízení se závažnými až fatálními dopady a důsledky[5]. Pro teroristické organizace představuje kritická infrastruktura spíše druhořadý cíl, a to navzdory faktu, že její narušení může způsobit závažné škody, včetně ohrožení zdraví a života velkého množství lidí.

Je tomu tak proto, že terorismus pracuje spíše s psychologickými dopady útoků (emocemi) než s objektivními následky. Hlavním záměrem teroristů je působit na veřejné mínění, šířit v populaci strach a paniku. A tak zatímco je objektivním faktem, že rozsáhlý výpadek elektrické energie může v konečném důsledku způsobit daleko větší škody a mít za následek vyšší počet obětí než např. výbuch či střelba v metru, traumatizující efekt na běžnou populaci bude ve druhém případě výrazně vyšší. Pro příklady není nutné chodit daleko do minulosti.[6]

Navzdory výše uvedenému tvrzení lze hodnotit relevanci hrozby útoku na kritickou infrastrukturu v ČR jako střední, a to především z hlediska možných závažných dopadů (které vyvažují jinak spíše nižší pravděpodobnost provedení takového útoku). Útok na kritickou infrastrukturu představuje příležitost způsobit poměrně značnou škodu s poměrně malými náklady a prostředky a ochrana některých součástí kritické infrastruktury je navíc velmi obtížná či nákladná. Riziko představuje také problém tzv. insiderů, tedy zaměstnanců (či bývalých zaměstnanců) zvýšeně ohrožených objektů, případně osob s dobrou znalostí bezpečnostních opatření a procedur. Z tohoto

[4] Této problematice se blíže věnuje kapitola Působení cizí moci.

[5] V širším pojetí lze za aktivity spojené s kyberterorismem považovat téměř jakoukoliv teroristickou činnost, kde dochází k propojení terorismu a kyberprostoru. Příkladem může být snaha o získávání finančních prostředků, rekrutace nových členů teroristických skupin i jejich výcvik. Podrobněji se problematice *kyberterorismu* věnuje kapitola „Hrozby v kyberprostoru".

[6] Útok na bostonský maraton si v roce 2013 vyžádal tři oběti. Po několik dní byl hlavním tématem mediálních výstupů doslova po celém světě a vyvolal obrovské množství reakcí. V červnu 2014 se po velké bouři ocitla bez elektrické energie velká část západní Austrálie a v přímém důsledku blackoutu (nikoliv bouře) zemřeli rovněž tři lidé. S výjimkou australských médií o této druhé události téměř nikdo neinformoval a i v samotné Austrálii byla tato zpráva spíše ve stínu jiných kauz (např. pátrání po zmizelém malajsijském letadle).

důvodu je nutné ochranu kritické infrastruktury nepodceňovat a vnímat ji jako jednu z priorit (nejen) v rámci boje proti terorismu.

b) Útok na měkké cíle

Zhodnocení relevance hrozby pro ČR: **Střední**

Jako tzv. měkké cíle (soft targets) se obvykle označují místa s vysokou koncentrací osob (nákupní centra, nemocnice, školy, prostředky hromadné dopravy, sportovní, kulturní a společenské instituce a události, instituce pečující o národní kulturní poklad[7] atd.), které nejsou nijak významně chráněné. V kontrastu s dobře zabezpečenými tzv. hard targets (letiště, jaderné elektrárny atd.) bývá míra jejich zabezpečení obecně nižší a útok na ně může mít potenciálně tragické následky pro fyzické osoby. Právě tato kombinace z nich činí potenciálně ideální cíl pro provedení teroristického útoku.

Zkušenosti z nedávné doby potvrzují, že teroristé se aktuálně na měkké cíle skutečně soustředí, a to v Evropě i mimo ni (útok v pařížských kavárnách a v koncertní hale, útok na bostonský maraton, útok na univerzitu v keňské Garisse a nákupní centrum v Nairobi atd.). Takové útoky mívají značné psychologické dopady, a přitom se dají poměrně snadno a s malými náklady provést. V poslední době jsou v tomto ohledu nejčastější útoky sebevražedných aktivních útočníků na veřejných místech, s využitím ručních zbraní (tento způsob se totiž ukazuje být z hlediska počtu obětí efektivnější, než dříve populární výbušniny, resp. improvizované nástražné výbušné systémy, a to i přes jejich relativně snadnou přípravu). Stále četnější jsou rovněž mnohonásobné útoky, kdy několik pachatelů zaútočí na větším množství míst najednou (např. nedávné útoky v Paříži a Bruselu). Takové útoky kladou zvýšené nároky na síly a prostředky, jakož i na koordinaci bezpečnostních složek.

Vzhledem k tomu, že právě měkké cíle jsou zřejmě nejpravděpodobnějším terčem možného hypotetického teroristického útoku na českém území, je relevanci této hrozby pro ČR nutné hodnotit jako střední.

c) Zvlášť ohrožené objekty a osoby

Zhodnocení relevance hrozby pro ČR: **Střední**

Kromě tzv. měkkých cílů a prvků kritické infrastruktury se mohou pravděpodobným cílem útoku stát objekty, které mají pro konkrétní teroristickou skupinu (či jednotlivce) **vysokou symbolickou hodnotu**. Do této kategorie můžeme řadit místa spojená s náboženskou symbolikou, budovy zastupitelských úřadů (zemí, které jsou častým cílem teroristických útoků), redakce časopisů, sídla médií či výstavy (které zveřejňují kontroverzní obsah), sídla úřadů veřejné správy, politických stran, policejní a vojenské objekty atd. V západní Evropě a v USA došlo v posledních letech k několika útokům specificky zaměřeným na příslušníky ozbrojených složek (policisty a vojáky), kteří reprezentují represivní složky státu a v tomto ohledu se mohou stát cílem útoku teroristů.

Zvýšené riziko platí i pro konkrétní osoby, které opět reprezentují postoje či instituce, jež mohou být zajímavé pro pachatele teroristických činů. Sem patří někteří politici, zahraniční diplomaté, ale také osobnosti aktivní ve veřejném životě (spisovatelé, novináři, herci, akademici atd.).

Vzhledem k různorodým motivům jednotlivých teroristických skupin je často obtížné rizikové osoby či objekty předem vytipovat – to platí zejména pro útoky osamělých vlků. Naopak v případě radikálního islamismu či pravicového a levicového extremismu je možné do určité míry předvídat,

[7] Zákon č. 101/2001 Sb., o navracení nezákonně vyvezených kulturních statků § 2, odst. 2.

které osoby či objekty budou pravděpodobným předmětem jejich zájmu a jsou v tomto ohledu zvlášť ohrožené.

V současné době jsou z výše uvedených cílů zvlášť chráněny (ať už přímo státem, nebo samotnými vlastníky cílů pouze ve spolupráci se státem): vybrané zastupitelské úřady a jejich diplomaté, vybraní čeští ústavní činitelé, vybraná sídla důležitých veřejných institucí, budova Rádia Svobodná Evropa, některé židovské objekty. Relevanci této hrozby pro ČR je možné hodnotit jako střední.

d) Ohrožení českých občanů či objektů v zahraničí

Zhodnocení relevance hrozby pro ČR: **Střední**

Zatímco samotné území ČR nemusí být pro teroristy primárním cílem pro provedení útoku, ohrožení českých občanů či objektů v zahraničí představuje v tomto ohledu pravděpodobnější hrozbu.

Rizikové jsou v tomto ohledu zejména únosy českých občanů, ke kterým již v minulosti opakovaně došlo (v posledních 10 letech byly zaznamenány případy únosů občanů ČR radikálními skupinami na území Iráku, Pákistánu, Libanonu a Libye). Útočníci se v těchto případech obvykle nezaměřují specificky na české občany, častěji se jedná o náhodně vybrané oběti „ze Západu“, které se pohybují bez dostatečné ochrany v rizikových oblastech, a mohou se proto stát snadným cílem.

Ohrožené mohou být i české objekty, zejména budovy zastupitelských úřadů v zahraničí. Zvýšené riziko útoku hrozí českým diplomatickým zastoupením zejména v zemích, kde aktuálně probíhá válečný konflikt, ve kterém se angažují teroristické skupiny (např. Sýrie, Afghánistán, Irák atd.).

Navzdory spíše nižší závažnosti případného dopadu, je kvůli zvýšené pravděpodobnosti útoku na české občany či objekty v zahraničí hodnocena relevance této hrozby jako střední.

III) Teroristická hrozba z hlediska nástrojů terorismu

a) Zneužití zbraní hromadného ničení, konvenčních zbraní, výbušnin a položek dvojího užití

Zhodnocení relevance hrozby pro ČR: **Střední**

Využití **zbraní hromadného ničení** pro teroristické účely je hojně diskutovanou otázkou. Ve skutečnosti existuje v historii jen velmi málo příkladů, kdy by k útoku s jejich využitím skutečně došlo (např. útok sekty Óm šinrikjó nervovým plynem v tokijském metru v roce 1995). Jejich následky ovšem mohou být velmi rozsáhlé a jejich psychologický dopad obrovský (a to dokonce i v případě nezdařeného útoku).

Některé mezinárodní teroristické organizace přímo deklarovaly snahu o získání zbraní hromadného ničení, obecně ale platí, že stále převládá soustředění se na „konvenční“ formy útoků. Využití jaderných, chemických a biologických zbraní vyžaduje expertní znalost a může být organizačně, finančně i logisticky náročné, a to i v případě konstrukce tzv. špinavé bomby nebo toxinových útoků (dopisní bomby nebo distribuce antraxu). Zabezpečení jaderných položek je v ČR na poměrně vysoké úrovni. O něco vyšší pravděpodobnost má použití improvizovaných chemických zbraní s využitím průmyslových toxických látek, případně teroristické útoky na jejich zásobníky anebo jejich přepravu. Takovou látkou může být jakákoliv chemická látka nebo směs chemických látek působících velmi rychle nepříznivě na lidský organismus, které mohou svým účinkem způsobit

zranění, zmrzačení či smrt. Vzhledem k potenciálnímu velmi ničivému efektu je ale přesto nutné věnovat této problematice zvýšenou pozornost. V této souvislosti se totiž v poslední době objevují zprávy, že by teroristé mohli získat k tomuto typu zbraní potenciální přístup (nelegální obchod s jaderným materiálem, možnost získání chemických zbraní v zemích zmítaných válečným konfliktem, potenciální spolupráce teroristů s autoritativními režimy atd.). V této oblasti je nezbytná multilaterální spolupráce, důsledné uplatňování kontrolních mechanismů v mezinárodním obchodu s položkami dvojího užití a důsledné dodržování principů bezpečného nakládání s těmito materiály.

Velké riziko plyne i z nelegálního šíření **konvenčních zbraní, výbušnin a šíření položek dvojího užití**, včetně příslušných technologií. Jak již bylo řečeno, ruční palné zbraně jsou v poslední době stále oblíbenějším nástrojem provádění teroristických útoků a tato oblíbenost pramení především z jejich relativně snadné dostupnosti. Omezení dostupnosti konvenčních zbraní pro teroristy je jedním z klíčových aspektů boje proti terorismu.

Pravděpodobnost útoku za využití zbraní hromadného ničení je v ČR poměrně nízká, významné by ale v takovém případě byly dopady takové události. Naopak zneužití konvenčních zbraní a položek dvojího užití má nižší případné dopady, je ovšem vyšší z hlediska pravděpodobnosti. Relevanci této hrozby pro ČR je proto možné hodnotit jako střední.

b) Financování terorismu a ostatní podpůrné aktivity

Zhodnocení relevance hrozby pro ČR: **Střední**

Ač se ČR nemusí stát přímo terčem teroristického útoku, může svou nečinností či nedůsledností neúmyslně přispět ke zvýšení ohrožení terorismem v jiných zemích. Teroristé mohou využívat ČR při získávání či převodu finančních prostředků, české území může sloužit jako tranzitní pro přesun osob s napojením na teroristické skupiny, případně může být vnímáno jako „bezpečný přístav“ pro úkryt před bezpečnostními složkami jiných států či přípravu teroristického útoku.

V roce 2015 se v médiích objevily zprávy, že někteří teroristé vnímají Prahu jako bezpečné tranzitní místo, neboť se zde lze údajně snáze vyhnout pozornosti bezpečnostních složek. Jakkoliv může být takové přesvědčení mylné či nepodložené, nelze vyloučit, že teroristé mohou české území dále využívat. Je proto důležité se na tyto aktivity soustředit a v maximální možné míře jim zamezovat.

Relevanci této hrozby pro ČR je možné hodnotit jako střední.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Základní dokumenty

Stěžejním dokumentem, který upravuje strategický rámec boje proti terorismu v ČR je **Strategie České republiky pro boj proti terorismu od r. 2013** (dále v této kapitole jen „Strategie“). Obsahově Strategie postihuje pět stěžejních oblastí – spolupráci zainteresovaných subjektů v boji proti terorismu, ochranu obyvatelstva a dalších potenciálních cílů, bezpečnostní výzkum a komunikaci s veřejností, prevenci radikalizace a rekrutování do teroristických skupin a nezbytný vhled do legislativního ukotvení problematiky boje proti terorismu. Platnost tohoto dokumentu není časově omezena a případná aktualizace by tak měla vyvstat z aktuální potřeby. Z pohledu pracovní skupiny

Auditu je obsah Strategie v plném rozsahu stále platný a v tuto chvíli není nutné přistupovat k jeho změně.

K implementaci Strategie přijala vláda ČR dne 31. srpna 2016 nový **Akční plán pro boj proti terorismu pro léta 2016 až 2018**. Tento Akční plán se skládá ze tří samostatných dokumentů. Jedná se o „**Legislativní návrhy v oblasti vnitřní bezpečnosti**“ a „**Protiteroristický balíček**“, které oba obsahují konkrétní kroky, které mají vést ke snížení rizika teroristického útoku a s ním spjatých negativních následků[8]. Třetím dokumentem je pak „**Návrh opatření ke zvýšení bezpečnosti na mezinárodních letištích v ČR**“ MD, který obsahuje některá opatření v oblasti bezpečnosti civilního letectví.

Legislativa

ČR nemá speciální „protiteroristický zákon“, problematika trestní odpovědnosti za terorismus je nicméně plně postižena v **Trestním zákoníku** (40/2009 Sb.). Zde mají vztah k terorismu zejména: §311 (Teroristický útok), §312 (Teror), §272 (Obecné ohrožení), §290 (Získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou), §292 (Zavlečení vzdušného dopravního prostředku do ciziny), §314 (Sabotáž), §140 (Vražda), §174 (Braní rukojmí), §175 (Vydírání), §279 (Nedovolené ozbrojování), §280 (Vývoj, výroba a držení zakázaných bojových prostředků), §281 (Nedovolená výroba a držení radioaktivní látky a vysoce nebezpečné látky), §282 (Nedovolená výroba a držení jaderného materiálu a zvláštního štěpného materiálu) a §357 (Šíření poplašné zprávy), popř. v některých případech i (verbální) trestné činy narušující soužití lidí § 352 až 356 (např. Nebezpečné vyhrožování ad.).

V současné době je v legislativním procesu **novela Trestního zákoníku**, která dále upravuje např. problematiku financování terorismu, podpory a propagace terorismu či vyhrožování teroristickým trestným činem. Dle návrhu by se mělo jednat o úpravy § 311, § 129 (kde je nově definován pojem „Teroristická skupina“), § 312, § 361, S novelou souvisí i změna zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Pracovní skupina Auditu plně podporuje přijetí této novely Trestního zákoníku v navrhovaném znění, neboť tato novela konkretizuje některé skutkové podstaty a předchází některým výkladovým otázkám a umožní tak efektivnější trestní postih zločinů souvisejících s terorismem.

Některým dílčím nedostatkům ve stávající legislativě, které mohou mít dopad na boj proti terorismu (např. uchovávání údajů z telekomunikačního provozu, využití zpravodajských informací v důkazním řízení, či rozšíření kontrol přeshraničního převozu peněžní hotovosti) se blíže věnuje již zmiňovaný materiál „Legislativní návrhy v oblasti vnitřní bezpečnosti“. Viz také část Doporučení.

Odpovědné instituce a orgány

1. **Vláda ČR** - Postavení vlády a její místo v bezpečnostním systému ČR ve vztahu k boji proti terorismu vymezuje zejména Ústava ČR; ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR; zákon č. 2/1969 Sb., kompetenční zákon, zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon); zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, a další právní předpisy. Vláda je jako vrcholný orgán výkonné

[8] Materiál „Legislativní návrhy v oblasti vnitřní bezpečnosti“ byl schválen usnesením vlády č. 779 ze dne 31. srpna 2016. Materiál „Protiteroristický balíček“, který byl schválen usnesením vlády č. 711 ze dne 27. července 2016, obsahuje opatření nelegislativního charakteru a podléhá stupni utajení dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů.

moci odpovědná za zajišťování bezpečnosti státu a za řízení a funkčnost celého bezpečnostního systému ČR. Vláda je ze své činnosti odpovědná Poslanecké sněmovně Parlamentu ČR.

Vláda je oprávněna vyhlásit nouzový stav, je-li nebezpečí z prodlení, může ho vyhlásit předseda vlády. Důležitý je rozdíl mezi činností vlády v běžném stavu a při krizových situacích, včetně válečného stavu, kdy vláda především vyhodnocuje možná rizika a hrozby v oblasti bezpečnosti ČR a činí nezbytná opatření ke snížení, popřípadě vyloučení těchto rizik (k tomuto účelu mimo jiné využívá své pracovní a poradní orgány).

Vláda je dále oprávněna mimo jiné: rozhodnout na návrh ministra vnitra o použití Armády ČR k záchranným pracím, k zabezpečení letecké přepravy, o povolání vojáků, příslušníků Vězeňské služby či Celní správy ČR k plnění úkolů policie atp.; zadávat úkoly zpravodajským službám, koordinovat a kontrolovat jejich činnost; jmenovat a odvolávat ředitele BIS a ředitele NBÚ; udílet souhlas se jmenováním a odvoláním ředitele ÚZSI, ředitele VZ. Vláda rozhoduje o návrhu ministra vnitra na vyhlášení (zrušení) stupně ohrožení terorismem (popř. ruší či potvrzuje ministrovo předběžné rozhodnutí o vyhlášení).

Předseda vlády je předsedou BRS.

2. **Bezpečnostní rada státu** – BRS je stálým pracovním orgánem vlády pro koordinaci problematiky bezpečnosti ČR a přípravu návrhů opatření k jejímu zajišťování. BRS tvoří předseda vlády a další členové vlády podle rozhodnutí vlády. BRS připravuje vládě návrhy opatření k zajišťování bezpečnosti ČR. Základním úkolem BRS je podílet se na tvorbě spolehlivého bezpečnostního systému státu, zabezpečovat koordinaci a kontrolu opatření k zajišťování bezpečnosti ČR a mezinárodních závazků. BRS má pět stálých pracovních orgánů, mezi které patří **Výbor pro vnitřní bezpečnost** (předsedou výboru je ministr vnitra), **Výbor pro koordinaci zahraniční bezpečnostní politiky** (předsedou je ministr zahraničních věcí), **Výbor pro obranné plánování** (předsedou je ministr obrany), **Výbor pro zpravodajskou činnost** (předsedou je předseda vlády) a **Výbor pro civilní nouzové plánování** (předsedou je ministr vnitra). V rámci Výboru pro zpravodajskou činnost je zřízena **Společná zpravodajská skupina** (SZS), která je předurčena pro výměnu zpravodajských informací a zajištění koordinace mezi zpravodajskými službami CR, Policií CR, MV a MZV. Do systému orgánů BRS je zařazen **Ústřední krizový štáb**, který je pracovním orgánem vlády k řešení krizových situací.

3. **Ministerstvo vnitra** – MV plní úkoly v oblasti vnitřní bezpečnosti a veřejného pořádku, a je tak mezi ústředními správními úřady jedním z hlavních gestorů boje proti terorismu. Součástí jeho působnosti jsou také související otázky azylu a migrace, schengenské spolupráce, kontrolních mechanismů pro obchodování se zbraněmi atd. Experti MV se účastní jednání pracovních skupin se vztahem k terorismu na nadnárodní úrovni (pracovní skupina CODEXTER v rámci Rady Evropy, TWG v rámci EU atd.). Ministr vnitra navrhuje vládě vyhlášení stupně ohrožení terorismem a související opatření a v případě nebezpečí z prodlení tento stupeň dočasně vyhlašuje.

4. **Policie ČR** – Působnost Policie ČR je dána zákonem č. 273/2008 Sb., o Policii ČR. Klíčovou roli v policejní struktuře v oblasti boje proti terorismu má zejména **Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování** (NCOZ). NCOZ, konkrétně sekce terorismu a extremismu je na základě pokynu policejního prezidenta č. 103/2013 pověřen šetřením, prověřováním a vyšetřováním trestné činnosti organizovaných zločineckých skupin (§ 361 trestního zákoníku) nebo zvlášť závažných a organizovaně páchaných zločinů v oblasti terorismu a extremismu a financování terorismu. V rámci odboru funguje **Národní kontaktní bod pro terorismus** (NKBT), jako jedno jeho oddělení, které představuje mechanismus, který umožňuje nepřetržitou spolupráci a výměnu operativních informací mezi zpravodajskými službami a policií o možném ohrožení

teroristickým útokem či o podezřelých osobách či skupinách. Svou nezastupitelnou roli v boji proti terorismu pak má i Útvar rychlého nasazení, krajské zásahové jednotky, popř. další útvary pořádkové policie, použitelné pro rychlý zásah proti ozbrojeným teroristům a obdobným (aktivním) útočníkům.

5. **Ministerstvo zahraničních věcí** – MZV je hlavním garantem vztahů ČR s ostatními státy a mezinárodními organizacemi, v rámci své působnosti v zahraniční bezpečnostní politice se věnuje i problematice terorismu, která má silný mezinárodní prvek. MZV také zajišťuje účast na skupině COTER (Council Working Party on Terrorism).

6. **Bezpečnostní informační služba** – Působnost BIS je vymezena zákonem č. 153/1994 Sb. o zpravodajských službách ČR. Podle § 5 odst. 1 písm. e) tohoto zákona BIS zabezpečuje informace týkající se organizovaného zločinu a terorismu. K tomu je oprávněna využívat specifické prostředky získávání informací, definované zákonem č. 154/1994 Sb. o BIS. BIS informace předává prezidentu republiky, předsedovi vlády a jejím členům. Státním a policejním orgánům BIS předává informace o zjištěních, která náleží do jejich působnosti. Usnesením vlády č. 1060 z 13. září 2006 byla BIS určena jako místo pro soustředění a vyhodnocování informací důležitých pro boj proti terorismu. BIS při zajišťování informací spolupracuje zejména s Úřadem pro zahraniční styky a informace, Vojenským zpravodajstvím, Policií ČR, konkrétně s NCOZ. BIS také spolupracuje s řadou zahraničních zpravodajských služeb v rámci mezinárodních platforem.

7. **Úřad pro zahraniční styky a informace** - ÚZSI je zpravodajskou službou ČR, jejímž prvořadým cílem, snahou a posláním je zabezpečovat pro ústavní činitele a orgány státní správy ČR včasné, objektivní a kvalitní zpravodajské informace, které mají původ v zahraničí a jsou důležité pro bezpečnost a ochranu zahraničně politických a ekonomických zájmů ČR. Smyslem práce ÚZSI je chránit ČR proti hrozbám, majícím původ v zahraničí, včetně hrozby mezinárodního terorismu. Působnost služby je upravena zákonem č. 153/1994 Sb., o zpravodajských službách ČR.

8. **Vojenské zpravodajství** - VZ se na plnění úkolů bezpečnostního systému v oblasti terorismu podílí zejména v oblasti zachycení hrozby, tedy v získávání takových zpravodajských informací, které budou způsobilé určit, že se jedná o hrozbu terorismu, v oblasti ohodnocení hrozby vůči aktivu ČR a stanovení míry rizika pro ČR. Působnost VZ je stanovena v rámci legislativy zákony č. 153/1994 Sb. a č. 289/2005 Sb. s primární orientací do oblasti obrany státu, pouze v rámci této působnosti se VZ podílí i na plnění úkolů v oblasti terorismu.

9. **Národní bezpečnostní úřad** - Působnost NBÚ v oblasti kybernetické bezpečnosti je stanovena zákonem č. 181/2014 Sb., o kybernetické bezpečnosti. Vzhledem k současným aktivitám teroristických skupin a organizací v kyberprostoru a vzhledem k možným dopadům jejich aktivit na kybernetickou bezpečnost ČR či na její zajišťování, má NBÚ kompetence a povinnost tuto problematiku v rámci své působnosti řešit. V rámci zákona č. 181/2014 Sb. se jedná především o ty části zákona, které se váží ke kybernetickým bezpečnostním incidentům a kybernetickým bezpečnostním událostem, které mohou mít i podobu kyberterorismu. NBÚ byl dále ustanoven gestorem kybernetické bezpečnosti usnesením vlády ČR č. 781 ze dne 19. října 2011. Kybernetickou bezpečností se dle Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020, která byla schválena usnesením vlády ČR č. 105 ze dne 16. února 2015, rozumí souhrn různých opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v ČR. NBÚ dle tohoto dokumentu má dále pomáhat identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků včetně kyberterorismu.

10. **Ministerstvo spravedlnosti** – MSp má působnost v oblasti justiční spolupráce, otázek extradice a mezinárodní právní pomoci. Do jeho gesce spadá trestní zákoník i Trestní řád. Je tak hlavním gestorem trestní politiky státu, včetně oblasti stíhání terorismu.

11. **Hasičský záchranný sbor a Integrovaný záchranný systém** - Řešení následků teroristických útoků co do následků na majetku, na životech a zdraví apod., spadá do působnosti HZS ČR, který odpovídá za záchranné a likvidační práce, respektive IZS (tedy zejména jeho hlavní složky HZS ČR, Policie ČR a ZZS), jehož národní koordinací je HZS ČR pověřen. Tomu odpovídají i typové činnosti složek IZS v případě např. použití špinavé bomby, hrozby použití nebo nálezu nástražného výbušného systému, chemického útoku v metru, útoku aktivního střelce, atd. Kapacitám a schopnostem HZS ČR se věnují kapitoly „Přírodní hrozby" a „Antropogenní hrozby"."

12. **Ministerstvo financí** – V rámci MF působí Finanční analytický útvar (FAÚ). Ten zajišťuje úkoly, které pro ministerstvo vyplývají ze zvláštních právních předpisů pro boj proti legalizaci výnosů z trestné činnosti a financování terorismu, a ze zvláštních právních předpisů upravujících oblast uplatňování mezinárodních sankcí za účelem udržování a obnovy mezinárodního míru a bezpečnosti, ochrany lidských práv a boje proti terorismu (dále jen „mezinárodní sankce"), v návaznosti na opatření přijatá Radou bezpečnosti OSN a orgány EU. Zajišťuje činnosti, které pro ministerstvo vyplývají ze zákona č. 104/2013 Sb.

13. **Ministerstvo dopravy** - V oblasti ochrany civilního letectví před protiprávními činy působí MD jako vrcholný orgán, který koordinuje postupy v této oblasti s dotčenými ústředními orgány státní správy v rámci Meziresortní komise pro bezpečnost civilního letectví. Systém ochrany civilního letectví před protiprávními činy vytváří Úřad pro civilní letectví, který rovněž vydává a aktualizuje národní bezpečnostní programy. V případě mimořádných situací, které bezprostředně a vážně ohrožují civilní letectví, má MD pravomoc vydat příkazy k provádění letů na dobu nezbytně nutnou. Další mimořádná opatření se řídí § 86f zákona č. 49/1997 Sb., o civilním letectví. Fyzická ochrana letišť se skládá z komplexní soustavy konkrétních bezpečnostních opatření, jež vyžadují spolupráci státních orgánů, bezpečnostních složek a provozovatelů letišť. V případě, že je civilní letectví bezprostředně ohroženo zvláště závažným protiprávním činem, je provozovatel letiště povinen přijmout mimořádná opatření. V ČR je ochrana letišť legislativně upravena v zákoně č. 49/1997 Sb., o civilním letectví, dále v Národním bezpečnostním programu ochrany civilního letectví ČR před protiprávními činy a rovněž je nutné v této oblasti plnit ustanovení příslušných nařízení EU.

14. **Ministerstvo zdravotnictví** - Z hlediska reakce na možné hrozby terorismu jsou v působnosti MZdr zdravotní služby, ochrana veřejného zdraví, zdravotnická vědeckovýzkumná činnost, řízení poskytovatelů zdravotních služeb v přímé řídící působnosti MZdr a zacházení s návykovými látkami, přípravky, prekursory a pomocnými látkami. Primárním úkolem zdravotnického systému v ČR je minimalizace následků teroristického útoku s dopadem na životy a zdraví osob, což je zajištěno poskytováním neodkladné přednemocniční a nemocniční zdravotní péče při událostech, které kromě jiných aspektů narušení bezpečnosti přinášejí situace s hromadným postižením osob na zdraví nebo s ohrožením veřejného zdraví, a to včetně hrozeb s použitím chemických, biologických nebo jaderných materiálů. Z hlediska ochrany veřejného zdraví obyvatelstva se jedná o koordinaci souboru opatření zahrnujících prevenci, stanovení protiepidemických opatření a možnosti kauzální léčby.

15. **Ministerstvo kultury** - MK nemá působnost v oblasti terorismu. Nicméně do zpracované Koncepce rozvoje muzejnictví v ČR v letech 2015 až 2020, byl zařazen úkol Omezení rizik v souvislosti s terorismem. V návaznosti na tento úkol MK sleduje a vyhodnocuje události spojené s terorismem a v součinnosti s MV, Policií ČR a vrcholným managementem institucí pečujících o národní kulturní poklad připravuje soubor preventivních opatření a ochrany k omezení rizika teroristického útoku v těchto institucích.

16. **Státní úřad pro jadernou bezpečnost** - SÚJB vykonává státní správu a dozor při využívání jaderné energie a ionizujícího záření, v oblasti radiační ochrany a v oblasti jaderné, chemické a biologické ochrany. Do jeho působnosti, dané zákonem č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon), zákonem č. 19/1997 Sb., a zákonem č. 281/2002 Sb. [9]Do kompetence SÚJB nepatří fyzická ochrana obyvatelstva. Implementací výše uvedených zákonů se zprostředkovaně snižuje možnost zneužití nebezpečných chemických látek, biologických agens a jaderných materiálů pro teroristické účely.

17. **Národní korespondent pro terorismus** – Působí v rámci Nejvyššího státního zastupitelství. Funkce je zřízena na základě zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních. Funkcí národního korespondenta je zajištění snazší a rychlejší výměny informací s národním členem Eurojustu[10].

C. SWOT analýza

Silné stránky

- Nízká atraktivita a slabé zázemí v ČR pro činnost mezinárodních teroristických skupin (ve smyslu organizování teroristických útoků na území ČR);
- Málo početná a dobře integrovaná muslimská komunita v ČR, která nevykazuje četnější známky radikalizace; v ČR nedochází k vytváření takových sociálně vyloučených lokalit či paralelních společenských struktur, které by fungovaly jako zázemí pro teroristické aktivity;
- Dobře fungující Integrovaný záchranný systém, schopný zvládat případné následky teroristického útoku;
- Dopady migrační vlny na ČR jsou zatím pouze nepřímého charakteru a významně nezvyšují riziko terorismu na území ČR;
- Občané ČR nejsou mezi zahraničními bojovníky, kteří bojují v konfliktech na Blízkém východě a v severní Africe na straně teroristických organizací;
- Fungující mezinárodní spolupráce na úrovni policie a zpravodajských služeb;

[9] Dnem 1. 1. 2017 nabývá účinnosti nový atomový zákon č. 263/2016 Sb.

[10] Dále působí v celé soustavě státního zastupitelství, zejména ve vztahu k vrchním státním zastupitelstvím, která od nabytí účinnosti novely vyhlášky č. 23/1994 Sb., o jednacím řádu státního zastupitelství, zřízení poboček některých státních zastupitelství a podrobnostech o úkonech prováděných právními čekateli, provedené vyhláškou č. 226/2016 Sb., vykonávají dozor v přípravném řízení ve věcech teroristických trestných činů a trestných činů souvisejících, rovněž působí jako garanti meziresortní spolupráce a spolupráce se zahraničím, při výměně informací a vzdělávacích akcích.

- ČR má vlastní strategii boje proti terorismu a implementovala naprostou většinu evropské legislativy se vztahem k boji proti terorismu;
- Proaktivní a preventivní přístup protiteroristických složek, kdy i po pouze jednotlivých incidentech (či incidentech mimo ČR) jsou přijímána systémová opatření ke zlepšení schopností reagovat (opatření k posílení odolnosti zejména po střelbě v Uherském Brodě v roce 2015, protiteroristický balíček a legislativní opatření po událostech v Paříži a Bruselu, opatření po žďárském útoku, průběžné přijímání opatření směrem k měkkým cílům).

Slabé stránky

- Omezená schopnost ČR výrazněji ovlivnit události za hranicemi EU, které mají značný vliv na riziko terorismu (destabilizace oblasti Blízkého východu a severní Afriky, migrační vlna, nástup tzv. Islámského státu a dalších teroristických skupin atd.).
- Nemožnost předvídat útoky teroristů jednajících samostatně.
- Omezené vlastní zkušenosti ČR v oblasti teroristických útoků (ČR nezaznamenala ve své novodobé historii na svém území teroristický útok v pravém slova smyslu).
- Omezená schopnost demokratickými prostředky tlumit rostoucí vliv radikálních, populistických a xenofobních skupin, které mohou vést k radikalizaci jednotlivců i majoritní společnosti atd.
- Omezené finanční prostředky vynaložitelné na prevenci a zvládání hrozby terorismu.
- Některé dílčí nedostatky právní úpravy (v oblasti uchovávání údajů z telekomunikačního provozu, nemožnost využití zpravodajských informací v důkazním řízení, cizinecká problematika atd.).
- Omezený vliv ČR v rámci EU (terorismus je problémem, který je nutné řešit na celoevropské úrovni; ČR v tomto ohledu nepatří mezi lídry evropské diskuse, což je částečně dáno i nižším významem této hrozby pro ČR).
- Pověst ČR jakožto islamofobní země (ke které přispívají vyjádření některých politiků, hojně medializovaná v zemích Blízkého východu a severní Afriky).
- Nedostatečné komunikační prostředí pro využití moderních technologií pro zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací.

Příležitosti

- Možnost učit se ze zkušeností západních zemí s terorismem, aniž bychom byli v tuto chvíli terorem bezprostředně zasaženi. Je možné provádět opatření za situace, kdy teroristický útok na českém území bezprostředně nehrozí.
- Zabránit radikalizaci a sociálnímu vyloučení osob ohrožených radikalizací dříve, než k ní dojde (v západní Evropě takové sociálně vyloučené lokality s velkým potenciálem teroristické radikalizace již existují, u nás dosud nikoliv, a je tedy možné zabránit jejich budoucímu vzniku).
- Příznivý vývoj vnějších faktorů (který se nicméně může v čase měnit) – snaha o stabilizaci Iráku, vyřešení konfliktu v Sýrii a Libyi, postupující vojenské operace proti tzv. Islámskému státu v Sýrii a v Iráku, příměří v Sýrii a úsilí o útlum migrační vlny, dohoda EU s Tureckem.

- Příležitost zavést fungující spolupráci mezi státem a majiteli měkkých cílů, která zmírní dopady případného budoucího útoku.
- Příležitost být konstruktivním hráčem v rámci EU a podílet se na hledání společných řešení v oblasti boje proti terorismu a migrace z hlediska významu a výhodnosti pro ČR.
- Příležitost zlepšit systém ochrany kritické infrastruktury (fyzické i kybernetické).
- Příležitost oslabit některé teroristické skupiny skrz opatření k omezení financování terorismu.

Hrozby

- Teroristé jednající samostatně.
- Nárůst xenofobních nálad a populismu v důsledku teroristických útoků v zahraničí, migrační vlny a aktivit českých populistických a islamofobních skupin, které mohou vést k radikalizaci jednotlivců či malých skupin a násilnému extremismu.
- Útok na měkké cíle.
- Ohrožení českých občanů či objektů v zahraničí.
- Financování terorismu a ostatní podpůrné aktivity.
- Útok na zvlášť ohrožené objekty a osoby.
- Útok na kritickou infrastrukturu.
- Vliv cizích státních aktérů na radikalizaci osob či vybraných skupin (salafismus, vytváření paramilitárních skupin a podpora extremistických proudů např. ze strany Ruské federace atd.).
- Zahraniční bojovníci.
- Zneužití zbraní hromadného ničení, konvenčních zbraní, výbušnin a položek dvojího užití;
- Rizika plynoucí z migrační krize.
- Islámský radikalismus.
- Politický extremismus a ostatní teroristické skupiny.

D. Doporučení k posílení odolnosti

Série návrhů opatření již byla vládou v roce 2016 přijata ve dvou dokumentech:

a) Protiteroristický balíček[11]

b) Legislativní návrhy v oblasti vnitřní bezpečnosti

[11] Materiál podléhá stupni utajení dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů, tudíž není možné návrhy opatření do textu Auditu uvést.

Tento materiál ukládá úkoly v následujících oblastech:

1. Uchovávání údajů z telekomunikačního provozu
2. Zákon o ÚZSI
3. Zpravodajské informace jako důkaz
4. Rušení pobytu cizinci, který je na území ČR
5. Utajované informace ve správním řízení
6. Řízení o udělení mezinárodní ochrany na vnitřní hranici
7. Akce s větším počtem osob (hromadné akce) a pravomoci policie
8. Obecné zhodnocení aktuální právní úpravy v oblasti postihu terorismu a souvisejících bezpečnostních hrozeb
9. Rozšíření kontrol přeshraničního převozu peněžní hotovosti

Další opatření:

1. Věnování pozornosti problematice radikalizace a rekrutování. Je nutné, aby příslušné orgány věnovaly pozornost známkám radikalizace jednotlivců či malých skupin (nejen) v prostředí muslimské komunity – tato radikalizace se může manifestovat různými způsoby, např. prostřednictvím sociálních sítí či jiných aktivit v kybernetickém prostředí. Je důležité, aby stát zasáhl ve chvíli, kdy osoby, které mohou mít širší vliv na danou komunitu (např. imámové), zneužívají svého postavení k šíření extremistických výkladů islámu, které jsou neslučitelné se zásadami demokratické společnosti, případně přímo vyzývají k násilí.
2. V tomto ohledu je také vhodné sledovat financování a podporu podobných aktivit ze zahraničí.
3. Pozornost je nutné věnovat také radikalizaci ve věznicích – zkušenosti ze západní Evropy ukazují, že právě kriminální prostředí představuje důležitý radikalizační faktor.
4. Posilovat opatření ve vztahu k aktivnímu útočníkovi – zejména pokračovat v procvičování pořádkové policie v akcích typu AMOK, vznik registru přestupků atd.
5. Věnovat pozornost problematice ochrany měkkých cílů před teroristickými útoky. Útokům na měkké cíle lze zabránit (nebo zmírnit jejich následky) posilováním jejich zabezpečení (je ale nutné vyvažovat hledisko bezpečnosti s hlediskem nákladovosti a efektivity), ale také výcvikem personálu těchto míst apod. Obecným problémem zabezpečení měkkých cílů je, že jsou většinou ve vlastnictví soukromých subjektů, a klíčová je tedy v tomto ohledu spolupráce státu s privátní sférou a spoluúčast samotných měkkých cílů na svém zabezpečení. MV byl vládou uložen úkol zpracovat návrh vytvoření celonárodního systému podpory zabezpečení vybraných měkkých cílů. Tato aktivita navazuje na dlouhodobé zkušenosti ze spolupráce např. s vlastníky židovských objektů.
6. V souvislosti s problematikou zahraničních bojovníků je nutné věnovat pozornost také otázkám formování paramilitárních skupin na českém území a zahraničnímu vlivovému působení.
7. Posilování ochrany kritické infrastruktury, fyzické i kybernetické.

8. Podpora dlouhodobého rozvoje komunikační infrastruktury a technologií veřejné správy a eGovernmentu pro využití při zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací.
9. Přijetí novely Trestního zákoníku, kterou připravilo Ministerstvo spravedlnosti, a která upravuje i některá ustanovení ve vztahu k terorismu.
10. Navrhnout změnu legislativy, která by v neodkladných případech umožnila zpravodajským službám a orgánům činným v trestním řízení na základě konkrétních informací nasadit úkony podléhající za normálních okolností schválení jiného státního orgánu (typicky soud) ihned, přičemž by žádost o povolení byla předložena v dodatečné lhůtě (např. 48 hodin). Typicky by se jednalo o případy, kdy je možné předejít spáchání nebo opakování teroristického útoku, stejně jako následně objasnit a minimalizovat škodlivé následky terorismu.
11. Navrhnout změnu legislativy, která by umožnila pro účely zjišťování nebo ověření poznatků o teroristických trestných činech okamžitý přístup k informacím o majitelích a disponentech bankovních a obdobných účtů, o účtech, které jsou ve styku se zájmovým účtem, o zůstatku na zájmovém účtu, a která by umožnila přístup k výpisu finančních transakcí na zájmovém účtu.
12. Novelizace legislativy s cílem mimo jiné umožnit stíhat i službu v nestátních cizích silách je v současné době řešena v pracovní skupině Ministerstva spravedlnosti. Tuto oblast je třeba jistě zařadit mezi problémy, které tato kapitola Auditu doporučuje vyřešit.

EXTREMISMUS

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

V rámci Auditu jsou pod pojmem extremismus[12] chápány vyhraněné ideologické postoje, které vybočují z ústavních norem, vyznačují se prvky netolerance a útočí proti základním demokratickým ústavním principům. Mezi tyto principy patří mj. úcta k právům a svobodám člověka a občana, ochrana menšin při rozhodování většiny, svoboda a rovnost lidí v důstojnosti a právech, nezadatelnost, nezcizitelnost, nepromlčitelnost a nezrušitelnost základních práv a svobod bez rozdílu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického nebo jiného smýšlení, národního a sociálního původu, příslušnosti k národnostní nebo etnické menšině, majetku, rodu nebo jiného postavení. Tyto extremistické postoje jsou způsobilé přejít v aktivity, které působí destruktivně na stávající demokratický systém.

Extremismus má hlubší příčiny sociální (nejen národnostní, ale politické, lokální, rodinné, náboženské tenze ústící v hledání alternativních sociálních vazeb, ritualizaci jednání, vytváření mýtů apod.), psychologické (sugesce, nápodoba, deprivace, afekt, davové jednání) a biologické (agrese, teritorialita).

Extremismus se vyskytuje vždy a ve všech společnostech. Nelze ho nikdy zcela vymýtit. Lze pouze minimalizovat hrozby s ním spojené namířené proti pluralitnímu demokratickému systému. Míra ohrožení souvisí s vnějšími faktory sociálními (míra společenské koheze, soužití s menšinami, migrace), politickými (důvěryhodnost mainstreamových politiků) a ekonomickými (hospodářská krize, korupce, nezaměstnanost) a s vnitřními faktory represivními (schopnost paralyzovat tvrdé extremistické jádro) a preventivními (schopnost zabránit radikalizaci většinové společnosti, schopnost chránit potenciální oběti extremistů). V případě výraznějších negativních společenských, politických či ekonomických změn platí pravidlo, že extremisté patří mezi první subjekty, které je kritizují a snaží se na této kritice profitovat. Některé příčiny mohou být reálné, jiné jsou uměle vykonstruované prostřednictvím propagandistického šíření dezinformací. Dále platí, že státní i nestátní subjekty potřebují obvykle až několik let k tomu, aby se naučily konkrétní extremistickou hrozbu efektivně zvládat a potlačovat.

Skryté nebezpečí extremismu spočívá v přejímání extremistických idejí do mainstreamového myšlení a v jeho šíření ve společnosti. Zpočátku tak ohrožuje jen určitou minoritu, když však začne zasahovat totalitním způsobem do života majority, bývá už zpravidla pozdě.

Protiextremistická politika se často chybně soustředí pouze na extremistické „klienty“. Přitom se zapomíná, že jejím prvořadým zájmem by měla být ochrana práv a svobod jejich obětí. Úkolem státu není samoúčelně se z jakési ritualizované setrvačnosti zabývat extremistickými skupinami. Jeho ambicí má být neustále analyzovat hrozby vyplývající ze strany extremistů pro jejich reálné i potenciální oběti a být schopný tyto oběti efektivně chránit, zajistit jim pocit bezpečí a podmínky pro důstojný život. „Obrat k oběti“ proběhl v některých západoevropských zemích, ČR na něj stále čeká.

[12] V definici se vychází z konceptu, který používá MV.

Obrat k obětem umožňuje nabídnout zdůvodnění, proč se protiextremistické aktivity dělají. Záměr paralyzovat extremisty není samoúčelný. V prvé řadě stát chrání určité skupiny obyvatel, následně pak právo každého občana mít svůj pohled na svět a podle něj žít svůj život. Extremisté jsou charakterističtí tím, že si nejprve vybírají za své nepřátele slabé sociální skupiny. Po získání dostatečného podílu na moci se soustředí na eliminaci všech společenských skupin i jednotlivců, kteří s nimi nesouhlasí. Extremismus tedy znamená ve svém důsledku ohrožení práv a svobod každého občana tohoto státu[13].

Kapitola Extremismus předpokládá přesahy do jiných kapitol v rámci Auditu, zejména Terorismu (zohledňuje rizika spojená s náboženským extremismem), Hrozeb v kyberprostoru, Bezpečnostních aspektů migrace, Působení cizí moci a Hybridní hrozby a jejich vliv na bezpečnost občanů.

2. Hrozba extremismu z hlediska původce

Společnost v ČR si kvůli specifickým historickým zkušenostem vytvořila určitou imunitu či nedůvěru vůči myšlenkám pravicového i levicového extremismu. Tato imunita se však s časovým odstupem od konkrétních historických událostí oslabuje. Objevují se stále nové trendy, extremistické skupiny se mezinárodně provazují, čímž získávají nové zkušenosti a možnosti, a některé extrémní prvky se dostávají i do politického mainstreamu.

a) Pravicový extremismus, protimuslimský a protiimigrantský extremismus[14]

Od 90. let vnímá česká společnost jako výraznější hrozbu pro demokracii extremismus pravicový. Jeho nejkrajnější formy dosahují často primitivní podoby, jeho exponenti se nezřídka dopouštěli a dopouštějí různých forem fyzického násilí. K tradičnímu pravicovému extremismu je zakořeněn odpor také kvůli negativnímu obrazu nacistů, který stále přetrvává ve společnosti.

Pravicově extremistická scéna postupně prochází dynamickým vývojem. Ten je v první řadě přirozeným důsledkem preventivních a represivních opatření státu proti projevům pravicového extremismu. Současně je ovlivněn i rostoucí mezinárodní provázaností, která přispívá k výměně zkušeností a sdílení nových přístupů. Z politologického hlediska je současná pravicově extremistická scéna těžko uchopitelná. Různé skupiny či jednotlivci v průběhu času mění své postoje, názory, dávají si různá jména, či uzavírají stále nová spojenectví. Pro pravicově extremistickou scénu nebyl a není konstantou ucelený systém politických názorů. Tyto politické rámce tvoří pouze nejasnou a

[13] Tento způsob vidění problematiky extremismu je veřejnosti prostřednictvím občanské společnosti a zahraničních institucí částečně předáván. Tato komunikace směrem k majoritě ovšem často nefunguje. Lidskoprávní instituce jsou často chápány jako příliš odtržené od reality, jejich poselství bývají mnohdy přijímána s nedůvěrou či dokonce s nelibostí. Proto je důležité naučit se obrat k obětem vysvětlovat veřejnosti jako něco užitečného, co se dotýká každého občana. Teprve poté se mohou reálně promítnout do praxe školení policistů či jiných zaměstnanců veřejné správy, jak správně postupovat ve vztahu k obětem trestné činnosti s extremistickým podtextem.

[14] Při hodnocení závažnosti dopadu byly brány v úvahu především životní, strategické a další významné zájmy ČR, tak jak je definuje BS 2015. Zejména tedy: zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel, bezpečnost a stabilita, především v euroatlantickém prostoru, prevence a zvládání místních a regionálních konfliktů a zmírňování jejich následků, podpora demokracie, základních svobod a principů právního státu, zajištění vnitřní bezpečnosti a ochrany obyvatelstva, prevence a potlačování bezpečnostních hrozeb ovlivňujících bezpečnost ČR a jejích spojenců, snižování kriminality, vytváření podmínek pro tolerantní občanskou společnost, potlačování extremismu a jeho příčin. V případě kritéria pravděpodobnosti byl brán v úvahu historický vývoj extremistické scény, současné trendy, zkušenosti ze zahraničí, statistická data k trestným činům s extremistickým podtextem, či sociologické průzkumy. Dále byla brána v úvahu schopnost státu i občanské společnosti se jednotlivým hrozbám účinně bránit. Výsledného hodnocení hrozeb bylo dosaženo na základě expertního konsensu.

proměnlivou kulisu pro trvalé konstanty. Těmi je neustálé hledání nepřátel a agresivní vymezování vůči nim.

Pro většinu pravicových extremistů není klíčové, zda se hlásí k nacismu, fašismu, či k českému vyhrocenému nacionalismu. V této oblasti dovedou dělat často těžko uvěřitelné názorové obraty, konzistentnost je výjimkou. Napříč všemi názorovými proudy se shodnou na jediné věci – na nenávisti k určitým minoritním skupinám obyvatel. V ČR je tato nenávist specificky zaměřená primárně proti Romům, Židům, dále k jiným etnickým a národnostním menšinám, cizincům, sexuálním menšinám, bezdomovcům či narkomanům. V poslední době se stupňuje v souvislosti s terorismem a migrací nenávist k muslimům a imigrantům. Vyostřuje se rovněž nepřátelství k názorovým odpůrcům.

Proměnlivé jsou nejen politické názory, ale i skupiny, vůči kterým se pravicoví extremisté vymezují. V současné době bylo zcela upozaděno nepřátelství k Romům a bylo nahrazeno nepřátelstvím k muslimům a imigrantům. Důležité je mít nepřítele, podružné je, kdo jím v danou chvíli zrovna je.

Další důležitou konstantou pravicově extremistické scény (ale i té levicově extremistické) je pak naprosto rozdílné vystupování uvnitř a vně komunity[15]. Zatímco v rámci vnitřních kontaktů neváhají pravicoví extremisté prezentovat názory či provádět aktivity, které jsou jednoznačně závadové či nezákonné, jejich prezentace pro majoritu tyto postoje či činnosti záměrně maskuje. Tato strategie, určená pro rekrutování nových členů a sympatizantů, je často velmi účinná. V případě některých protiromských shromáždění v roce 2013 se např. ukázalo, že některé názory a aktivity extremistů převzala část majority. V krajních případech pak z těchto shromáždění extremisty vytlačila. Objevili se noví názoroví vůdci či organizátoři, kteří tradiční extremisty zastínili.

Od roku 2015 navíc dochází ke kvalitativnímu posunu na extremistické scéně. Původní pravicově extremistické skupiny ustupují do pozadí. Vyčerpaly svůj potenciál, oslabila je policejní represe spolu s kampaněmi občanské společnosti a médií. Navíc získaly nálepku subjektů „nepřijatelných ve slušné společnosti“ pro asociálnost, primitivnost a přílišnou radikalitu některých členů či sympatizantů.

V souvislosti s migrační vlnou a teroristickými útoky v Evropě se na celém kontinentu prosazují stále častěji protiimigrantské a protimuslimské subjekty. Ty často nejsou zatížené spojením s tradičními militanty, dávají si pozor na to, aby se pohybovaly v mezích zákona. V jejich řadách se pohybují vzdělanější, schopnější a lépe finančně vybavení lidé. Ti dovedou získat na svou stranu i veřejně známé osobnosti, včetně politiků. V oblasti rétoriky i aktivit se nicméně profilují velmi podobně jako tradiční extremistické subjekty. Vyšší kultivovaností projevu se jim daří oslovit širší spektrum veřejnosti.

Spojujícím prvkem extremistických uskupení není (zástupná) ideologie (nacismus, fašismus, vyhrocený nacionalismus), ale nenávist podle etnického, náboženského či jiného klíče. Tedy podle charakteristik, které někdy dotčení lidé ani nemohou ovlivnit. Ve všech etapách české novodobé historie platilo, že tyto subjekty dokáží formulovat problém, ale nedokáží ho řešit. Jimi navrhovaná řešení jsou na první pohled zpravidla velmi snadná a rychlá, ale často jsou v rozporu s obecně uznávanými demokratickými principy nebo se zákonem. Naopak jen zvyšují společenské napětí a zužují prostor pro hledání konstruktivního řešení. Růst významu extremistických hnutí znamená polarizaci a štěpení společnosti. Případné uchopení moci jejich exponenty by znamenalo omezení svobod a zavádění totalitních praktik.

Naštěstí je zatím Evropa, včetně ČR, ušetřena existence charismatických extremistických vůdců, kteří by dokázali sjednotit různé extremistické proudy a získat výraznější podíl na moci. Nicméně částečné úspěchy některých extremistických stran v několika evropských zemích dokazují, že nástup skutečně charismatické osobnosti předválečného typu by byl pro demokracii velmi těžkou zkouškou.

[15] Např. squatting.

Aktivity extremistických subjektů jsou mj. prostředkem k nabourávání demokratického pluralitního systému. Proto je nezbytné počítat s tím, že se mohou těšit podpoře ze strany cizího státu usilujícího o oslabení české demokracie a vyvázání ČR ze spojenectví s ostatními evropskými demokratickými státy.

Nedílnou součástí extremistické scény, která vždy vyžaduje zvýšenou pozornost, jsou radikalizovaní militantní jedinci či skupiny, které se nezdráhají použít násilí k prosazování svých cílů a proti jiným skupinám osob. Ti se dopouštějí násilí vůči osobám z řad jejich nepřátel, zejména názorových oponentů, ale i vůči policii, která pro ně zosobňuje „státní moc". Radikalita těchto osob může být snadno zneužitelná jednotlivými názorovými vůdci, kteří se obvykle přímo fyzického násilí nedopouštějí, ale inspirují k němu jiné osoby.

V době internetu představuje značné riziko i seberadikalizace osob, které se běžně nezapojují do veřejných extremistických aktivit a bezpečnostním složkám tudíž nejsou známy.

b) Levicový extremismus

Desetiletí komunistické diktatury vyvolala v české společnosti nedůvěru k utopickým představám o uspořádání společnosti podle učení marxismu-leninismu. Na levicově extremistické scéně se proto od 90. let výrazněji prosazují spíše myšlenky anarchistické.

Anarchisté se potýkají při prosazování svých myšlenek s několika problémy. V první řadě jde o neschopnost dohody ke spolupráci uvnitř samotného hnutí. To totiž tvoří řada individualit s často odlišnými názory, které nejsou ochotny ke kompromisům a nedokáží své ambice podřídit práci pro tým. Anarchistické hnutí je paralyzováno difúzními debatami mezi jednotlivými názorovými autoritami a kolektivy, které jsou pro většinu společnosti těžko srozumitelné a mnohdy i velmi neatraktivní. Druhým klíčovým momentem je nezájem či nedůvěra velké části společnosti k jejich obecně formulovaným ambicím na změnu společenského uspořádání.

Anarchisté jsou si vědomi svého omezeného vlivu na formulování obecných společenských, politických či ekonomických témat i své nejednotnosti. Proto si ke své sebeprezentaci pro veřejnost vybírají omezený okruh relativně nekonfliktních oblastí. Sem lze zařadit např. antifašistické aktivity, ochranu životního prostředí, pomoc osobám bez domova, podporu alternativního způsobu života či alternativní kultury. Aktuálně se zaměřili i na téma pomoci uprchlíkům.

Při bližším pohledu na vyjádření radikálních představitelů anarchismu však lze zaznamenat jejich extremistická východiska. Ta jsou založena na nenávisti třídní, nenávisti k názorovým oponentům a nenávisti ke státní moci a celému systému. Anarchisté si uzurpují monopol na správný pohled na uspořádání společnosti a při jeho prosazování nejsou ochotni akceptovat jakékoli kompromisy. V žádném případě nepřistupují k demokratickému dialogu a nerespektují pluralitní politický systém. Mají vlastní představu o prosazování svých cílů. Radikální část anarchistů navíc považuje za legitimní používání násilí. Tito radikálové si pak násilí chtějí monopolizovat. V ČR je relativně běžné fyzické napadání názorových odpůrců (zejména z řad neonacistů), či ničení cizího majetku (např. žhářské útoky).

Anarchistická scéna je stejně jako krajní pravice internacionalizovaná a čeští anarchisté přebírají řadu trendů ze zahraničí. V této souvislosti je třeba upozornit na to, že v zahraničí ze strany anarchistů dochází při různých příležitostech k masovým veřejným násilnostem (tzv. rioty) a v krajních případech k teroristickým útokům, vraždám či loupežím. Podobně jako u pravicových extremistů se i u krajní levice lze obávat výskytu tzv. osamělých vlků, neboli militantních radikálů, kteří se nezapojují do veřejných aktivit a čekají na vhodnou příležitost k provedení násilného aktu.

Marxisticko-leninské skupiny lze v současnosti považovat za marginální. Mladí levicoví radikálové z tohoto spektra se potýkají s nezájmem svých vrstevníků, osobními animozitami a přehnanou politickou ambiciózností některých vůdčích postav. Jejich organizace a skupiny jsou zpravidla

dlouhodobě nefunkční. Aktivnější jednotlivci se proto zapojují do aktivit etablovaných levicových politických uskupení a organizací. V jejich rámci vytváří radikální platformy a pozvolna přenáší některé extrémní názory do mainstreamu. Vzhledem k určitým názorovým shodám na jednotlivých tématech (antifašismus, podpora radikálního feminismu, aj.) není vyloučena ani spolupráce s anarchistickou scénou.

c) Hodnocení hrozeb

Specifikace hrozby	**Pravicoví, proti-muslimští a protiimigrační extremisté**	**Levicoví extremisté**
Štěpení společnosti – vytváření antagonismů.	Vysoká hrozba	Střední hrozba
Nárůst napětí na základě etnického, náboženského či názorového klíče včetně demonstrací a projevů násilí.	Střední hrozba	Střední hrozba (relevantní pouze názorové hledisko)
Přejímání extremistických prvků do politického mainstreamu.	Vysoká hrozba	Střední hrozba
Výskyt radikalizovaných militantních jedinců či malých skupin, kteří mohou k prosazení svých zájmů použít násilí.	Střední hrozba	Střední hrozba
Vznik politicko extremistického subjektu s charismatickým vůdcem.	Střední hrozba	Nízká hrozba
Vznik extremistických domobran.	Střední hrozba	Nízká hrozba
Zneužívání tuzemských extremistických platforem cizími státy.	Střední hrozba	Střední hrozba

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Základní dokumenty

V obecné rovině je problematika extremismu zmíněna v **Bezpečnostní strategii ČR**. Nicméně základními dokumenty, které se na úrovni státní správy věnují přímo a pouze problematice extremismu jsou každoročně vydávané **Zprávy o extremismu a Koncepce boje proti extremismu**. Koncepce boje proti extremismu je každoročně vyhodnocována. Dokumenty jsou schvalovány vládou. Zprávy o extremismu popisují významné události a trendy za uplynulý rok. Jsou vydávány od roku 1997. Přispívají do nich MV, Policie ČR, zpravodajské služby, Nejvyšší státní zastupitelství, Nejvyšší soud, Probační a mediační služba, Vojenská policie či Generální inspekce bezpečnostních sborů. Koncepce boje proti extremismu je rozčleněna do pěti kapitol: Komunikací proti demagogii, Vědomostí proti totalitářům, Jednotná protiextremistická platforma, Odbornost a imunita a Pomoc obětem trestné činnosti.

Legislativa

Pojem extremismus není v zákonech ČR přímo zakotven. V praxi však existuje několik právních norem, které jsou pro jeho postih využitelné. Pracovně bývají nazývány trestné činy s extremistickým podtextem. ČR je zároveň vázána celou řadou mezinárodních úmluv, které se vztahují k extremismu. Trestná činnost s extremistickým podtextem se promítla i do české judikatury. Z hlediska legislativy jsou pak klíčové i rozsudky mezinárodních soudních orgánů, např. Evropského soudu pro lidská práva.

Bazálními dokumenty pro oblast extremismu jsou Listina základních práv a svobod a evropské normy. V boji proti extremismu lze využít ustanovení v oblasti správního i trestného práva (omezení práva na svobodu projevu, sdružovacího, shromažďovacího, petičního či pracovního práva - např. nemožnost vykonávat některá povolání v bezpečnostní oblasti pro extremisty).

Právní normy nabízejí orgánům činným v trestním řízení možnost přísného postihu násilí s extremistickým podtextem. V kapitole o terorismu jsou specifikovány zákony se vztahem k tomuto jednání či k jeho podpoře. České i mezinárodní normy pak vymezují deklaratorně demokratické hodnoty a odsuzují historické totalitní režimy.

V bezpečnostní komunitě převládá názor, že legislativní rámec je dostačující, je pouze potřeba s právními nástroji, které mají úřady k dispozici, efektivně pracovat.

Odpovědné instituce a orgány

Efektivní protiextremistická politika patří pravidelně mezi priority vlády. Koordinační úlohu plní v rovině ústředních orgánů státní správy **MV**. Klíčovou roli pak sehrává **Policie ČR**. V rámci policie se do protiextremistických opatření zapojuje několik útvarů. Policie disponuje po linii služby kriminální policie a vyšetřování specialisty na extremismus. **BIS** v rámci své působnosti vymezené zákonem zabezpečuje informace o záměrech a činnostech namířených proti demokratickým základům, svrchovanosti a územní celistvosti ČR. Činnostmi, jejichž důsledky mohou ohrozit bezpečnost ČR v obecné rovině se zahraničním extremismem, se zabývá zpravodajská služba s vnější působností - **ÚZSI**. Do boje proti extremismu se zapojuje i **VZ**. Různé úkoly s přesahy do protiextremistické politiky plní i **další bezpečnostní sbory a složky bezpečnostního systému**.

Kromě bezpečnostních složek se ovšem do protiextremistických aktivit zapojují **i další resorty a úřady: MSp, MŠMT, MK, MPSV ad**. Zejména v oblasti prevence plní řadu úkolů instituce v rámci **Úřadu vlády** a na mezinárodním poli i **MZV**.

Nezastupitelnou roli v potírání extremismu ovšem hraje i **nestátní sféra**. Kromě aktivit **občanské společnosti a seriózních žurnalistů** je třeba vyzdvihnout práci některých **nevládních organizací** a specializovaných **akademických pracovišť**.

Na mezinárodním poli je pro ČR zavazující **členství** v některých **mezinárodních organizacích či spolupráce s nimi.** Zejména v oblasti potírání rasismu a xenofobie lze zmínit **Radu Evropy a EU** (významnou roli hraje zejména Agentura pro základní práva), **Organizaci pro bezpečnost a spolupráci v Evropě** (v jejím rámci fungující Úřad pro demokratické instituce a lidská práva), **Visegrádskou skupinu** (Pracovní skupina zemí V4 a Rakouska pro boj s extremismem). V obecné rovině se tématu extremismu věnuje i **OSN**. Kromě těchto institucí lze vysledovat celou řadu **mezinárodních platforem**, které se přímo nebo zprostředkovaně bojem s extremismem zabývají.

Hodnocení represivních a preventivních aktivit

Represe

Dynamika extremistických hnutí se vměstnává do určitých opakujících se cyklů. Ty charakterizuje zpočátku rychlý vzestup nového či modifikovaného hnutí. To postupem času nabývá na síle a začíná se stále více radikalizovat. Státní aparát na něj zpočátku nedokáže flexibilně reagovat. Po důkladném posouzení situace z hlediska bezpečnostních rizik a porušování právních předpisů a po překonání série zdlouhavých byrokratických překážek pak dokáže aplikovat, zpravidla po předchozím apelu či dokonce naléhání od občanské společnosti, příslušná represivní opatření. Represe následně vyvolá v řadách extremistů pocity strachu a nedůvěry. Snižuje se jejich radikalita. Represivní opatření jsou často medializována a v rámci medializace dochází k poukazování na některá skrytá negativa a protiprávnost chování extremistů. Tím se snižuje jejich věrohodnost v očích veřejnosti a omezuje se jejich podpora.

V ČR platí, že nejefektivnějším postupem je důsledná represe proti tvrdému extremistickému jádru. Pro represi platí jedno důležité pravidlo - musí být aplikována včas. Leckdy pak stačí, když policie jasně deklaruje, že určitý typ nezákonného jednání nebude v žádném případě tolerovat.

Represivní protiextremistický aparát je relativně dobře systémově zabezpečen. Policie disponuje dostatečným množstvím specialistů po linii pořádkové i kriminální policie. Ve srovnání s jinými zeměmi můžeme konstatovat, že má i relativně kvalitní materiálové a technické vybavení. Existuje celá řada školení v oblasti extremismu, metodických pomůcek i relevantních interních aktů řízení. Byla nastavena opatření, která mají za cíl bránit extremistům v infiltraci do bezpečnostních složek.

Práci Policie ČR v oblasti extremismu ale komplikují zejména tyto tři jevy:

- Nepružnost velké byrokratické instituce.
- Téma extremismu je často policisty chápáno jako „politické“, často v souvislosti s ním čelí přímému či nepřímému tlaku rozličných politiků. Někdy sami jednají tak, aby se v prvé řadě tomuto tlaku vyhnuli.
- Vnímání určitých společenských témat v policii kopíruje nálady ve společnosti. Někteří policisté se navíc v rámci výkonu své služby setkávají jen s určitým (zpravidla negativním) segmentem reality. Proto i tato profesní skupina musí často čelit různým předsudečným tendencím.

Schopnost flexibilně reagovat v oblasti represe na nové trendy stojí na nadstandardních aktivitách omezeného množství kvalitních profesionálů po linii uniformované i neuniformované policie, kteří dokáží čelit třem výše zmíněným jevům a prokáží schopnost nepodléhat politickým či společenským tlakům.

V oblasti justičního aparátu se ČR potýká s nedostatkem expertů, kteří se dokáží v oblasti extremismu orientovat, mají přehled o současné scéně a s ní souvisejících rizicích. Neznalost reálné situace může vést k podceňování nebezpečnosti extremistů, a vnímání jejich trestné činnosti jako relativně neškodného projevu mladické nerozvážnosti nebo touhy po revoltě.

Největší aktuální výzvou je potírání nezákonného a závadového obsahu na internetu. Zde čelí bezpečnostní složky těmto hlavním problémům:

- Obrovské množství takového obsahu.
- Nedostatek kvalifikovaných policejních specialistů.
- Umisťování takových obsahů na servery ve třetích zemích s odlišnou právní úpravou, která znemožňuje jejich postih.

Tradiční a dlouhodobá chyba, kterou lze přičítat značnou měrou MV, spočívá v tom, že nedochází ke zdůvodňování represivních postupů, jejich vysvětlování, zařazení do širšího kontextu. Veřejnost je informována často izolovaně, o jednotlivostech vytržených ze souvislostí. To umožňuje extremistickým subjektům formulovat obraz mučedníků, kteří se jakožto „jediná skutečná opozice" stali obětí „šikany státu" a „politické policie". Policie pak není vnímána jako těleso, které chrání zájmy občanů, ale jako jakýsi přirozený soupeř extremistů. Konkrétně pak je poselství, že policie ochránila určitou skupinu obyvatel před nebezpečnými militanty s extrémními názory, zaměněno za informaci, že policie se střetla s radikály.

Prevence

Prevence politické radikalizace je celoevropskou výzvou, na kterou dosud nebyla nalezena adekvátní odpověď. V ČR nejsou doposud ujasněny ani základní předpoklady pro její aplikování. Tedy není jasné:

- Kdo ji má iniciovat, organizovat, financovat, vyhodnocovat (státní x nestátní sektor, který resort).
- Komu má být určena, aby měla nějaký efekt (definování cílové skupiny).
- Jaké má být poselství (pravicový x levicový extremismus, obhajoba pluralitní demokracie, zaměření jen na extremismus x zaměření na související jevy).
- Jaké kanály využívat (média, kampaně, přednášky, kulturní a sportovní akce, sociální sítě).
- Jaký má být měřitelný výsledek (co lze považovat za úspěch a jak ho měřit).

V ČR, s určitým zpožděním oproti zemím západní Evropy, bylo aplikováno několik různých protiextremistických preventivních projektů. Celá řada byla velmi pečlivě připravena a lze prokázat, že měla pozitivní efekt. Minimálně stejné množství projektů však vznikalo narychlo v reakci na určité situace, respektive náhle vzniklou poptávku, bez jasného zadání, bez angažmá skutečných expertů, bez jasně definovaného cíle a bez definování způsobu měření úspěchu. Tímto ukvapeným způsobem byly nejenom prohospodařeny prostředky, ale byly i promarněny příležitosti. Na obhajobu ČR je však třeba říci, že podobnou zkušeností si prošla i řada států západní Evropy.

ČR disponuje velkým množstvím odborníků na extremismus (znalců scény a její historie), ale naproti tomu nemá takřka žádné odborníky na „prevenci extremismu" a souvisejících jevů. Potírání extremismu je, alespoň na úrovni státní správy, často chápáno pouze v represivní rovině. Dokud si důležitost prevence extremismu neuvědomí politická reprezentace, nelze na úrovni státní správy, ale i samosprávy, očekávat výraznější změnu. Státní správa musí formulovat poptávku, musí se přihlásit k odpovědnosti, musí navazovat partnerské vztahy s dalšími subjekty státními i nestátními. Tradičně je nositelem nových impulsů nevládní sektor. Přetrvávajícím problémem je vzájemná nedůvěra mezi státními i nestátními subjekty. Tu lze překonat jen dlouholetou spoluprací obou platforem. V některých zemích pak existují samostatné instituce či pobočky institucí, které se věnují koordinaci a organizování preventivních aktivit v oblasti politické radikalizace (např. německá Spolková centrála pro politické vzdělávání).

Běžnou chybou protiextremistických opatření je jejich nepřesné zacílení. Na úrovni státní správy se jedná o velké projekty typu obecně formulovaných celostátních strategií či národních akčních plánů, v menším měřítku pak lze zmínit kampaně zaměřené „na celou společnost" či na „mladé lidi". Tyto chyby jsou způsobeny tím, že se na jejich koncipování podílejí úředníci či aktivisté bez patřičného vzdělání a profesní zkušenosti. Pro jasné definování cílové skupiny pak často chybí validní sociologická a psychologická data. V bezpečnostní komunitě v západních zemích se pak stále častěji hovoří o prevenci zacílené přímo na extremistické „klienty". Typickým příkladem této prevence jsou

tzv. exitové programy, které mají pomoci „klientům“ opustit extremistické prostředí. Získání „polepšeného“ jedince z extremistického prostředí pak představuje z hlediska bezpečnosti velké množství výhod.

Poselství preventivních aktivit je další klíčovou neznámou. Zkušenosti ukazují, že nevhodným konceptem je strašení extremismem. Popularizaci demokratických hodnot je obtížné důvěryhodně a přesvědčivě uchopit. Většina projektů je směřována proti extrémně pravicovým subjektům. Preventivní kampaně proti současné extrémní levici, zejména anarchistům, fakticky neexistují. Public relations extremistů jsou často nesrovnatelně kvalitnější než některé projekty či kampaně státu či neziskového sektoru.

U volby kanálů k přenosu informací platí více než u ostatních bodů důležité pravidlo – je třeba, aby je obsluhovali zkušení profesionálové. U kanálů s dopadem na velké množství recipientů existuje velmi nebezpečné riziko – špatně realizovaný projekt může vyvolat opačný efekt, než jaký autoři zamýšleli.

S postupem času jsou kladeny stále vyšší nároky na kvalitu provedení preventivních projektů. Zpravidla už nelze vystačit s konstatováním, že „projekt se osvědčil“ či „splnil svůj účel“. Je nutností, aby byly nastaveny měřitelné indikátory úspěchu, podobně jako v komerčním sektoru. Kvalitativní data mohou poskytnout např. sociologické výzkumy. Pokud by měla být prevence zaměřena na samotné extremistické „klienty“, bylo by potřeba zkoumat i psychologické faktory např. u odsouzených za trestnou činnost s extremistickým podtextem.

Existují dokonce názory, aby se preventivní projekty tematizující extremisty, vůbec nedělaly. Podle tohoto konceptu je třeba se zaměřit pouze na problémy, na které extremisté poukazují, rychle nalézt alternativu k populistickým a často nereálným extremistickým návrhům a tuto alternativu pak urychleně veřejnosti představit a začít prosazovat do praxe.

V souvislosti se soustředěním se neonacistického hnutí na romskou otázku věnovaly státní orgány velké úsilí potírání jeho exponentů. Stát se po určitou dobu jednostranně zaměřoval na neonacisty, jako by byli výhradní příčinou problémů v sociálně vyloučených lokalitách a jako by se tyto problémy eliminací neonacistů měly vyřešit. Že se jednalo o chybnou strategii, ukázaly např. události ve Šluknovském výběžku v roce 2011, kde byli hlavními aktéry nepokojů občané bez vazeb na extremistickou scénu.

Podobné riziko chybného uchopení problému vzniká v souvislosti s migrační krizí. Stát nedokázal dosud jednoznačně reagovat na obavy občanů spojené s imigranty. Tedy zejména veřejně a jasně komunikovat dlouhodobější opatření, která omezí rizika terorismu, zabrání vzniku nekontrolovatelných ghett a zneužívání sociálního systému.

C. SWOT analýza

Silné stránky

- Dobré systémové zabezpečení represivního aparátu.
- Kvalitní legislativní rámec.
- Disponování, byť omezenou, skupinou profesionálů, kteří odvádějí kvalitní práci v oblasti represe.

Slabé stránky

- Nepochopení, v čem spočívá hrozba extremismu. Společnost často nechápe princip obětí, kdy obětí se v důsledku může stát každý občan.
- V oblasti bezpečnostní politiky se stále pracuje se zastaralým a neudržitelným konceptem pravicového a levicového politického extremismu.
- Nízká flexibilita, schopnost rychlé adekvátní reakce bezpečnostních složek. Zejména policie je vystavena častým a intenzivním politickým tlakům. Dochází k častým personálním i koncepčním změnám. To má za následek absenci: odpovědnosti za plnění stanovených úkolů, strategického směřování, výchovy a vzdělávání expertů, dostatečné a rychlé komunikace napříč relevantními útvary a dostatečného a efektivního využívání stávajících sil a prostředků, včetně komunikační infrastruktury.
- Nejasný a nefungující koncept prevence. Stát spoléhá na represi a umí aplikovat pouze represi. Dlouhodobě se jedná o neudržitelný stav.
- Špatná spolupráce mezi státním a nestátním sektorem. Špatná spolupráce mezi jednotlivými subjekty v rámci státního sektoru i mezi jednotlivými subjekty v rámci nestátního sektoru.
- Omezený počet dostatečně erudovaných a profesně zkušených expertů na prevenci extremismu a souvisejících jevů.

Příležitosti

- Fungování pluralitní demokracie. Existence občanské společnosti a nezávislých médií.
- Členství ČR v nadnárodních demokratických institucích a z toho plynoucí povinnost dodržovat určité demokratické závazky.
- Historickou zkušeností podmíněný odpor a nedůvěra k extremistickým totalitním ideologiím.
- Nejednotnost extremistické scény, absence charismatických vůdců.
- ČR je ve srovnání s jinými evropskými zeměmi etnicky i nábožensky poměrně homogenní.

Hrozby

- Obecně schopnost extremistů štěpit společnost a oslabovat ČR vytvářením antagonismů na základě etnického, náboženského, třídního či jiného klíče. **Vysoké riziko**.
- Další nárůst napětí na základě etnického či náboženského klíče včetně demonstrací a projevů násilí. Lokální spouštěcí incidenty mají stále potenciál mobilizovat veřejnost. Dochází i k polarizaci v rámci majority, kdy vznikají animozity mezi stoupenci různých názorových proudů. **Vysoké riziko**.
- Přejímání extremistických prvků do politického mainstreamu. **Vysoké riziko**.
- Možný výskyt radikalizovaných militantních jedinců či malých skupin, kteří mohou k prosazení svých zájmů použít násilí. **Střední riziko**.
- Možný vznik politicko extremistického subjektu s charismatickým vůdcem, který dokáže sjednotit extremistickou scénu a oslovit další potenciální příznivce. **Střední riziko**.

- Vznik extremistických domobran, které se mohou, mnohdy nelegálně, ozbrojovat a své možné projevy a aktivity cílit proti určitým skupinám osob na základě etnického či náboženského klíče. **Střední riziko**.
- Zneužívání tuzemských extremistických platforem cizími státy za účelem oslabení fungování pluralitní demokracie v ČR. **Střední riziko**.

D. Doporučení k posílení odolnosti

1. Klíčovým předpokladem je prosazování a propagace konceptu obětí. Tento koncept s sebou může přinést tato pozitiva:
    a. Snížení atraktivity extremistických uskupení.
    b. Snížení ochoty veřejně známých osobností, včetně politiků, parazitovat na extremistických tématech. Snížení jejich schopnosti (zejména v případě politiků) negativně ovlivňovat práci aktérů protiextremistické politiky.
    c. Zvýšení motivace aktérů protiextremistické politiky.
    d. Zlepšení podmínek práce aktérů protiextremistické prevence.
    e. Ujasnění konceptu prevence a otevření nových možností pro preventivní práci.
2. Opuštění konceptu extremismu v oblasti bezpečnostní politiky. Nové definování hrozeb při zdůrazňování ochrany státu a systému pluralitní demokracie.
3. Nové definování rizikových skupin v bezpečnostní komunitě s důrazem na jejich schopnost ohrožovat demokratické principy státu. To by mělo umožnit efektivní dělbu práce mezi bezpečnostními složkami.
4. Školení policejních a justičních specialistů v nových trendech a možnostech postihu extremistů. Zvýšení spolupráce mezi policií a státními zastupitelstvími, např. formou společných vzdělávacích akcí, instrukčně metodických zaměstnání. Klíčové je osobní setkávání mezi policejními experty a státními zástupci.
5. Propojení statistik policie, státních zastupitelství a soudů, aby bylo možné dohledat a analyzovat průběh jednotlivých trestních řízení.
6. Posílení schopností policie vyšetřovat kybernetickou kriminalitu v souladu se strategickým dokumentem Rozvoj Policie ČR v letech 2016 – 2020.
7. Pokračování v opatřeních, která mají bránit infiltraci extremistů do bezpečnostních složek.
8. Zajištění inovace policejních informačních systémů, zabránění duplicitám, zvýšení schopnosti sdílet potřebná, i víceobjemová, data. Rozvoj komunikačního prostředí s důrazem na využití moderních technologií.
9. Pro prosazení konceptu obětí musí stát angažovat a spolupracovat se zkušenými profesionály v oblasti komunikace, výchovy a vzdělávání. Musí si jasně stanovit, co od nich očekává a musí je dostatečně motivovat.
10. Zapojení těchto profesionálů je třeba prosazovat zejména v oblasti prevence. Hledání inspirace v západních zemích, zejména ve Velké Británii a v Německu. Poučení se z chyb v jiných státech
11. Prohlubování spolupráce mezi státní správou, samosprávou a nevládním sektorem.

12. Otevřenost státní správy, zejména v oblasti poskytování informací o extremistické scéně, obětech extremistů a souvisejících jevech. Protiextremistickou politiku nelze provádět izolovaně, bez informování veřejnosti. Opatření proti extremistům je nutné veřejnosti vysvětlovat a zdůvodňovat. Je nutné rovněž nabízet alternativu k řešení problémů, na které poukazují extremisté. Je třeba mít na paměti, že v současné době média s jejich profesionály dokáží daleko kvalitněji a efektivněji než státní správa předávat veřejnosti určitá poselství.

ORGANIZOVANÝ ZLOČIN

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Organizovaný zločin bývá opakovaně označován za závažnou hrozbu pro bezpečnost ČR a prioritní oblast činnosti orgánů státní správy. O jeho přítomnosti na území ČR není pochyb. Otázky ale vzbuzuje již samotná definice organizovaného zločinu, neboť v českém prostředí obecně přijímaná definice tohoto fenoménu neexistuje[16]. Vznikají tedy pochyby o tom, jaké aktivity pod tento pojem spadají, což spolu s vysokou latencí organizované kriminality přispívá k obtížné vyčíslitelnosti rozsahu této hrozby. Zároveň šíře pojmu „organizovaný zločin" znemožňuje podrobný popis všech jeho druhů v rámci této kapitoly.

Hlavní motivací organizovaného zločinu je finanční zisk, vedlejší motivací je posílení možností realizace tohoto zisku zvyšováním vlivu na rozhodování státních orgánů v relevantních oblastech (zejména rozdělování veřejných finančních prostředků, ale i legislativní činnost), případně posílení vlastní obranyschopnosti infiltrací do orgánů činných v trestním řízení. Zároveň je snahou zločineckých skupin provádět svoji činnost skrytě a nebudit tak ani pozornost orgánů činných v trestním řízení, ani pohoršení veřejnosti. S tím je spojený částečný odklon od násilných aktivit (nájemné vraždy) k méně nápadným formám činnosti (vydírání, podvody).

Běžné občany problematika organizovaného zločinu zpravidla osobně nezasahuje, neboť jim zločinecké skupiny přímo neškodí. V oblasti distribuce určitých komodit – např. nelegálních drog, zbraní a padělaných dokumentů mohou být organizované skupiny některými občany dokonce vnímány spíše jako poskytovatelé žádaných služeb než jako zločinci.

V současné době se projevuje odlišné vnímání dvou hlavních oblastí organizovaného zločinu – jeho klasická a moderní varianta. Aktivity klasického organizovaného zločinu spočívají v zjevně ilegálních aktivitách – např. obchodu s drogami, zprostředkování nelegální migrace, padělání dokladů a dalších činnostech, které jsou v současné době státem poměrně efektivně postihovány.

Naopak moderní organizovaný zločin spočívá spíše v nežádoucím ovlivňování rozhodnutí veřejných orgánů, vytváření klientelistických a korupčních sítí a ovlivnění normotvorby. Všechny tyto aktivity jsou obtížně prokazatelné, jejich velká část může být považována za legitimní a legální a jejich škodlivý charakter vyplývá pouze z jejich celkového důsledku, kterým je zpravidla neefektivní využití veřejných finančních prostředků. Zpravidla jsou tyto aktivity velmi obtížně prokazatelné a postižitelné a stávající represivní nástroje na ně nestačí. Pro účely tohoto textu považuje za aktivity spadající pod pojem organizovaného zločinu jak jeho klasickou, tak moderní variantu.

Organizovaný zločin se vyvíjí a mění v čase. Tento vývoj je zcela nezbytné důkladně sledovat, analyzovat a adekvátně na něj reagovat. V současné době převažuje trend profesionalizace organizovaného zločinu se specializací jednotlivých účastníků na přesně vymezené činnosti.

[16] V zákoně č. 40/2009 Sb. (trestním zákoníku) je v § 129 definován pojem organizovaná zločinecká skupina, v §361 trestný čin účasti na organizované zločinecké skupině a v § 107 pachatelství ve prospěch organizované zločinecké skupiny. Nicméně žádná z těchto definic nevyčerpává celý pojem „organizovaný zločin" a zejména nespecifikuje šíři aktivit pod něj spadajících. Další dílčí definice jsou obsaženy v dokumentech EU a OSN.

Profesionální zločinci nabízejí své služby různým zájemcům a místo semknutých uzavřených skupin fungují spíše rozprostřené zločinecké sítě, jejichž členové jsou zapojování do konkrétních aktivit podle své specializace. Tyto sítě využívají moderních komunikačních prostředků a šifrovaného spojení, které ztěžuje jejich identifikaci. Souvisejícím jevem je využívání profesionálních služeb právníků, daňových poradců a účetních firem pro zastírání nelegální činnosti a legalizaci výnosů z ní.

Další výraznou tendencí je přesun aktivit organizovaného zločinu do kyberprostoru[17]. Nejedná se pouze o již zmíněnou komunikaci, která je v tomto prostředí rychlejší, efektivnější a obtížněji zachytitelná a přiřaditelná, ale také o celou novou škálu aktivit, které rozvíjejí portfolio zločineckých skupin. Jde zejména o různé typy podvodného jednání (např. vylákávání plateb na základě smyšlených či upravených podkladů a faktur), kybernetické kriminality (elektronické vydírání, šíření škodlivých programů, krádeže identity, provozování nelegálních tržišť v síti skrytého internetu apod.) a postupů spojených s legalizací výnosů z trestné činnosti (převody virtuálních měn). Zločinecké skupiny využívají v tomto globálním prostředí buď technologickou převahu nad orgány činnými v trestním řízení, nebo alespoň vyšší stupeň anonymity. Orgány činné v trestním řízení se musí činnosti těchto skupin přizpůsobovat ve výrazně méně flexibilním prostředí daném zákonnými a organizačními limity jejich činnosti. Pro státní orgány je také mnohem obtížnější adekvátně zaplatit odborníky v oblasti IT, zatímco zločinecké skupiny si jejich služby mohou s ohledem na výnosnost této činnosti bez problémů dovolit. V oblasti organizované kriminality páchané na internetu předpokládáme vysokou míru latence trestné činnosti vzhledem k obtížnému zjišťování některých typů případů.

Tato kapitola se detailněji nevěnuje aktuální situaci v oblasti migrace a problematice nelegální migrace, neboť toto téma je řešeno v jiné kapitole materiálu. Zároveň není věnován širší prostor organizované internetové kriminalitě (kyberkriminalitě), neboť toto téma je řešeno v kapitole „Hrozby v kyberprostoru“.

2. Popis a evaluace hrozby

Hrozby v této kapitole jsou hodnoceny z hlediska jejich dopadu na finanční (daňové příjmy, efektivita výdajů) a jiné zájmy státu[18] a dále z hlediska odhadovaného rozsahu jejich výskytu. Kritérium pravděpodobnosti vypuknutí u těchto hrozeb není aplikovatelné, neboť všechny uváděné hrozby jsou již v ČR do určité míry přítomny. Vzhledem ke skrytému charakteru činnosti organizovaného zločinu není možné rozsah těchto aktivit zcela přesně vyčíslit. Relevance hrozby je hodnocena na stupnici nízká – střední - vysoká dle kombinace výše uvedených faktorů. Přestože považujeme aktivity klasického organizovaného zločinu (obchod s drogami, obchod s lidmi, obchod se zbraněmi, padělání, organizovanou majetkovou trestnou činnost - krádeže motorových vozidel, kapsářské skupiny a další) za velmi závažné, vzhledem k omezenému rozsahu kapitoly odkazujeme na nedávno zpracované materiály reagující na tyto druhy trestné činnosti zmíněné v části B.

Zároveň v těchto oblastech považujeme situaci za dostatečně zmapovanou a chceme se v této kapitole věnovat spíše tématům méně popsaným a pro stát ve svém důsledku závažnějším.

[17] Tato tendence je potvrzena i ve Zprávě o činnosti státního zastupitelství za rok 2015 (http://www.nsz.cz/images/stories/PDF/Zpravy_o_cinnosti/2015/Zprava_o_cinnosti_SZ_za_rok_2015_-_textova_cast.pdf)

[18] Z hlediska BS 2015 jde zejména o tyto zájmy – zachování všech náležitostí demokratického právního státu, zajištění vnitřní bezpečnosti a ochrany obyvatelstva, snižování kriminality s důrazem na hospodářskou kriminalitu, organizovaný zločin, kybernetickou kriminalitu a boj s korupcí, zvyšování efektivity a profesionality státních institucí a soudnictví.

I) Prorůstání organizovaného zločinu do veřejné správy a orgánů činných v trestním řízení

Zhodnocení relevance hrozby pro ČR: **Vysoká**

Infiltrace organizovaného zločinu do struktur veřejné správy a orgánů činných v trestním řízení má zásadní negativní dopad na funkčnost a efektivitu veřejné správy a je průvodním jevem i dalších níže uvedených hrozeb. Trvalým problémem je jmenování osob (úředníků) ovlivňujících výkon veřejné správy a rozdělování finančních prostředků na základě užšího výběru předem vytipovaných jednotlivců, kteří jsou zároveň loajální kriminálním strukturám. I po vytlačení osob aktivně participujících na dysfunkčních praktikách z orgánu státní správy či veřejné samosprávy přetrvává jejich vliv na řadové zaměstnance. Tento vliv se projevuje i v kladení překážek vyšetřování ze strany řadových zaměstnanců, z nichž někteří jsou k podílu na trestné činnosti nuceni pod pohrůžkou ztráty zaměstnání, případně se na této trestné činnosti vůbec nepodílejí.

Někteří spolupracovníci a členové kriminálních organizací vytlačení z exponovaných funkcí jsou zaměstnáváni na méně viditelných místech s vlivem na státní či veřejnou správu (např. veřejně vlastněné právnické osoby), odkud mohou nadále realizovat aktivity související s nelegálním vyváděním finančních prostředků z veřejných rozpočtů. Pokračuje přitom stav, kdy vlivová osoba kriminální organizace umístěná do funkce ve státní správě či veřejné samosprávě je odměňována formou platu, který je díky zastávané pozici již sám o sobě značně nadprůměrný. Na méně významných pozicích v samosprávě či veřejně vlastněných právnických osobách bývá plat často doplněn různými poradenskými smlouvami, odměnami apod. Z hlediska transparentnosti výběrových řízení jsou problematické schůzky členů výběrových komisí s uchazeči mimo rámec tohoto řízení, které mohou být motivovány snahou o ovlivnění jeho průběhu.

Objevují se také kontakty organizovaného zločinu do prostředí orgánů činných v trestním řízení, dohledových a dozorových orgánů státní správy a průnik organizovaných skupin do legislativního procesu nejen na úrovni lokálních samospráv, ale i na vládní a parlamentní úrovni. Kriminální struktury si tímto způsobem zajišťují přístup k neveřejným informacím. V oblasti justice existuje podezření na ovlivňování výsledků trestních kauz obcházením systému přidělování napadlé agendy.

Jako problematické jsou vnímány některé detaily úpravy výběrových řízení dle zákona č. 234/2014 Sb. o státní službě. Je třeba zvážit posílení podmínek pro zamezení účasti nežádoucích osob (pokud nemají záznam v trestním rejstříku) ve výběrových řízeních. Zároveň analyzovat dopad omezení příchodu odborníků ze soukromého sektoru na některé pozice státní správy. Zároveň je nutné využívat všechny prostředky motivace státních zaměstnanců, vytvářet podmínky pro koncepční práci s lidskými zdroji v oblasti veřejné správy. Přehlížení těchto zásad by mohlo nahrávat organizovanému zločinu, neboť by usnadnilo získávání státních zaměstnanců ke spolupráci na zločineckých aktivitách.

II) Zneužívání veřejných zakázek a veřejných rozpočtů

Zhodnocení relevance hrozby pro ČR: **vysoká**

Zcela zásadní plýtvání rozpočtovými prostředky způsobené aktivitami organizovaného zločinu se odehrává v oblasti veřejných zakázek a veřejných dotací. Složité systémy zadávání a udělování dotací a veřejných zakázek spojené s absencí důsledného systému kontroly a individuální odpovědnosti u konkrétních rozhodnutí vedou k situaci, kdy je celá řada projektů manipulována ve prospěch zločineckých skupin.

Ze strany kriminálních struktur se objevuje snaha řídit veřejné zakázky již od samého prvopočátku za účelem následného vyvádění finančních prostředků do soukromých rukou. V praxi se objevuje účelové dělení veřejných zakázek na tzv. zakázky podlimitní, pro které není třeba vypisovat výběrové

řízení. Opakovaně se také do výběrových řízení přihlašují spolčené firmy s předem domluvenou a výrazně navýšenou cenovou nabídkou. Organizované skupiny se uchylují k využívání nejrůznějších zprostředkovatelů a za přísliby úplatků získávají potřebné informace a podporu k prosazení svých zájmů. V některých případech je předem domluveno, která firma danou zakázku vyhraje a která dělá v daném výběrovém řízení tzv. křoví. Aby byli všichni zástupci firem spokojeni, tak při dalším výběrovém řízení a vyhlášení vítěze veřejné zakázky se role vymění. Když se do výběrového řízení přihlásí jiná firma, která může narušit předem domluvený výběr, je zpravidla organizátory výběrových řízení vyřazována z formálních důvodů pro banální nedostatky. Obdobně zmanipulovaná bývají řízení v případě udělování dotací.

Problematika fyzických osob, které se účastní zadávacího řízení v rámci veřejných zakázek, byla v minulosti opakovaně diskutována. Výsledkem diskuse bylo zavedení nového druhu citlivé činnosti v rámci zákona č. 137/2006 Sb., o veřejných zakázkách. Požadavek na jistou bezúhonnost těch osob, které se podílejí na významných veřejných zakázkách, je zohledněn i v novém zákoně o veřejných zakázkách - zákon č. 134/2016 Sb.

III) Organizovaná daňová kriminalita

Zhodnocení relevance hrozby pro ČR: **vysoká**

Intenzivní činnost organizovaného zločinu ohrožuje nejen veřejné výdaje popsané v předchozí části, ale také veřejné příjmy zejména ve formě neodvedených daní (zejména DPH a spotřební daň). Legálně fungující společnosti na podkladě fiktivních faktur získaných od nelegálních struktur předstírají vyšší vynaložené náklady a zatajují ve skutečnosti dosažený zisk. Tímto jednáním si snižují základ daně, a dojde tak k vyměření a zaplacení daně v nižší částce, než jaká odpovídá zákonu. Problémem je nejasná hranice mezi legální daňovou optimalizací a krácením daně, která vede k tomu, že toto krácení DPH se stalo „běžnou“ součástí legálního podnikání. Problematická je samotná konstrukce DPH a jejího přiznávání a odvodu, kde zvlášť u některých komodit bude její krácení stále předmětem zájmu kriminálních skupin. Postupným zaváděním principu přenesení daňové povinnosti (reverse charge) se daří možnosti jejího krácení eliminovat, avšak organizované skupiny snadno přecházejí na nové druhy „obchodovaného zboží“ (nově např. masné výrobky).

Mezi významné problémy v této oblasti patří také vytváření organizovaných struktur společností, jejichž cílem je inkaso nadměrných odpočtů daně z přidané hodnoty (tzv. karuselové podvody). Tento fenomén je dostatečně znám a proto není dále rozváděn[19].

V některých oblastech obchodování (pohonné hmoty, elektronika a další) dochází kvůli těmto podvodům k likvidaci poctivého podnikání – vzhledem k masivnímu zasažení těchto segmentů nejsou v konečném důsledku poctiví podnikatelé schopni konkurovat na trhu výslednou cenou zboží a z trhu odcházejí. Situaci také komplikuje účast cizinců v postavení organizátorů a zejména v pozicích bílých koní. Tyto osoby, vybavené falešnými pasy, se snadno a nekontrolovatelně pohybují v rámci Evropy, jsou využívány často pro jediný úkon (založení s. r. o. nebo bankovního účtu) a v rámci odhalování trestné činnosti jsou neustanovitelné a nedohledatelné. České subjekty zařazené do podvodných řetězců mají zcela běžně vedeny účty v bankách v zahraničí, čímž tyto peníze dostávají z dosahu správce daně a současně výrazně komplikují následné objasňování v trestním řízení a také zajišťování výnosů z trestné činnosti.

[19] V roce 2016 došlo k zlepšení stavu v této oblasti. Dovozy textilu, kde byla popisovaná nelegální činnost nejčastější, výrazně poklesly. Celní správě ČR se podařilo způsobem přimět čínské celní orgány ke spolupráci. V současné době čínská strana zodpověděla převažující většinu dožádání vzájemné administrativní pomoci. Není možno tvrdit, že by tento problém neexistoval i nadále, na druhou stranu se v současné době velmi těžce odhaduje jeho rozsah. Problematika si zasluhuje nové provedení analýzy.

Mezi další významné typy organizované trestné činnosti patří i nadále krácení celních poplatků při dovozu zboží ze států mimo EU (zejména z Čínské lidové republiky, pachateli jsou zpravidla občané Vietnamu). Její intenzita zůstává v posledních několika letech nezměněna. I nadále dochází k umělému snižování hodnoty zboží pomocí padělaných dokladů při jeho vstupu na území EU a tím i k vyměřování mnohem nižších celních poplatků (zneužíván je tzv. celní režim 4200, do kterého je zboží propuštěno v jiném členském státu s možným určením v tuzemsku). Klíčovým bodem těchto technik zůstávala stejně jako v předchozích letech tzv. služba k proclení[20]. Hlavním problémem je neexistence možnosti nezávislého ověření pravosti průvodních dokladů dováženého zboží, které jsou předkládány při celním řízení. Příslušné orgány Čínské lidové republiky totiž ve většině případů spolupráci při ověřování pravosti průvodních dokladů k čínskému exportnímu zboží bojkotují nebo ji pouze účelově předstírají. Nedostatečná je také v některých případech spolupráce příslušných orgánů sousedních zemí.

Do této oblasti spadá také nelegální provozováním loterií a jiných podobných her, kdy cílem je vyhnout se primárně daňovým povinnostem, jimiž jsou zatíženi provozovatelé legálně provozující loterie a jiné podobné hry. Zejména se jedná o nelegální provozování těchto aktivit prostřednictvím internetu, provozování tzv. kvízomatů a technických herních zařízení provozovaných neoprávněně pod záštitou spolků nebo svěřenských fondů. Vzhledem k rozsahu této činnosti většinou jde o organizované zločinecké skupiny. K 1. červenci 2016 vznikla k potírání tohoto druhu kriminality tzv. Hazardní kobra, složená ze zástupců Policie ČR, Celní správy ČR a Finanční správy. Inspirací pro její vznik bylo úspěšné fungování tzv. Daňové kobry.

IV) Legalizace výnosů z trestné činnosti

Zhodnocení relevance hrozby pro ČR: **střední**

Aktivity organizovaných zločinecký struktur generují vysoké zisky, které se logicky jejich příslušníci snaží opětovně využít ve svůj prospěch a pokud možno je zlegalizovat investicí do legálních statků (obchodních společností a nemovitostí). Významným problémem v této oblasti je vytváření vysoce sofistikovaných struktur obchodních společností s cílem legalizovat v nich prostředky pocházející z trestné činnosti. Jedná se o trestnou činnost s velkou úrovní právní erudovanosti. Skupiny obchodních společností jsou zakládány podle českého práva, ale také zahraničních právních úprav a sídlí v mnoha státech, zejména pak v tzv. offshore destinacích. Společným jmenovatelem těchto zahraničních destinací je skutečnost, že je zde vysoká míra ochrany soukromí, případně tyto destinace vůbec nespolupracují se zahraničními orgány činnými v trestním řízení. V určitých případech mohou tyto struktury předstírat skutečnou podnikatelskou činnost vytvářením obchodních smluv, oběhem faktur apod. Předmět těchto obchodních vztahů je však zcela fiktivní, nicméně často se jedná o těžko prokazatelná plnění (reklamní služby, poradenství). Cílem těchto struktur je uskutečnit velké množství mezibankovních převodů, které znemožní tok peněz sledovat a zároveň vrátit tyto prostředky osobě, která je do systému vložila a nově s nimi bude disponovat jako s legitimním příjmem. Výnosem z této trestné činnosti pro její realizátory jsou poplatky za vyprání peněz. Pachateli této trestné činnosti jsou nezřídka advokátní kanceláře. Sídla advokátních kanceláří jsou také využívána jako sídla firem s cílem komplikovat práci orgánů činných v trestním řízení odkazem na advokátní tajemství.

[20] Tato služba zajišťuje přepravu zboží a také dodává falešné dokumenty uměle snižující jeho hodnotu. Zároveň také vyřizuje všechna potřebná povolení a zajišťuje hladký průběh celního odbavení. Firmy, které by měly plnit daňové a celní povinnosti, jsou často fiktivní nebo účelově založené, sídlí mimo ČR a povinné platby neodvádějí.

V) Zneužití legitimních služeb pro účely organizovaného zločinu

Zhodnocení relevance hrozby pro ČR: **střední**

Organizovaný zločin pro svoje činnosti běžně využívá různých služeb, které jsou samy o sobě legální. Jejich nelegální aspekt nevychází z povahy těchto samotných služeb, ale z účelu jejich použití (např. přeprava drog poštovní službou, převod ukradených peněz na bankovní účet). Zneužívány jsou zejména služby finančních institucí, poskytovatelů telekomunikačních služeb, daňových, právních a účetních poradců, ale také nové technologie a platební nástroje dostupné všem občanům.

Ovládnutí či založení finanční instituce (např. kampeličky) organizovaným zločinem může sledovat dva základní cíle - legalizovat výnosy z trestné činnosti v rámci legálního podnikání na finančním trhu a tunelovat vložené prostředky střadatelů, resp. kampeličky jako takové. Nižší nároky na zakládání a fungování kampeliček a nižší míra dohledu nad jejich činností ze strany příslušných orgánů toto jednání umožňují. Pachateli této trestné činnosti jsou zločinecké skupiny, které se pohybují v oblasti legálního podnikání a zároveň v oblasti šedé ekonomiky či přímo kriminální činnosti. Ovládnutá finanční instituce pak nehlásí podezřelé obchody a nespolupracuje se státními orgány. Je znemožněna kontrola finančních toků a zločinecká skupina má kontrolu nad dotazy policie. Zneužívány jsou také služby převodu peněz do zahraničí (např. Western Union), s jejichž pomocí jsou nelegálně získané finanční prostředky převedeny v hotovosti na prakticky nedohledatelné subjekty v zahraničí.

Legitimní oprávnění a nástroje usnadňující podnikání či život občanů jsou využívána ve prospěch nelegálních struktur mimo jiné v těchto případech:

- neomezené zakládání společností jednou osobou (z hlediska organizovaného zločinu jde zpravidla o tzv. bílé koně)
- vysoký limit na hotovostní platby a výběry[21] (umožňuje rychle přesouvat velké objemy nelegitimně získaných peněz)
- umisťování sídel do tzv. office housů (kde je daná společnost zpravidla nekontaktní)
- možnost používání anonymních předplacených platebních karet (neztotožnitelné transakce)
- virtuální měny (opět problematické ztotožnění iniciátorů transakce)
- svěřenské fondy (vyvádění majetku získaného trestnou činností)

Zaznamenána byla také koupě poskytovatele telekomunikačních služeb zločineckou skupinou pro účely vytvoření vlastní uzavřené skupiny volajících. Tento operátor nabízí klientovi avízo při dotazech orgánů činných v trestním řízení. Problematické je také umisťování elektronických dat v datových úložištích mimo sídlo společnosti, často na serverech v zahraničí a využití mezinárodních telekomunikačních služeb se sídly v zahraničí (Facebook, WhatsApp, Gmail,…).

Podobně jako v předchozím případě není zneužití legitimních služeb a oprávnění přímou novou hrozbou, ale „pouze“ napomáhá úspěšnému páchání organizované trestné činnosti.

[21] V současné době jde o 270 000 Kč.

VI) Kriminalita spojená s insolvenčním řízením

Zhodnocení relevance hrozby pro ČR: **nízká**

Od roku 2014 byl zaznamenán nárůst podvodných insolvenčních návrhů, které většinou spojují tyto tři okolnosti - podání insolvenčního návrhu u zjevně místně nepříslušného soudu, využívání procesní úpravy k obstrukcím insolvenčního řízení a pochybná pohledávka navrhovatele podložená smlouvou o dílo, zápůjčkou či směnkou. Tyto návrhy jsou zneužívány v konkurenčním boji a mají také sloužit k nelegálnímu obohacení navrhovatelů, případně skupin stojících za nimi. V účelově založených firmách podávajících insolvenční návrhy se v pozicích jednatelů často nacházejí cizinci (občané Polska a Maďarska), kteří jsou nedohledatelní. Tyto insolvenční návrhy jsou obvykle po odborné stránce velmi dobře zpracovány, což nasvědčuje tomu, že pachatelé mají dobrý právní servis poskytovaný k těmto účelům a jedná se o aktivity organizovaného zločinu.

Dalším problémem současných insolvenčních řízení je možnost koluze insolvenčního soudce nebo správce s některými z účastníků řízení a následné účelové zvýhodnění těchto účastníků oproti ostatním.

Vzhledem k existenci novely[22] insolvenčního zákona, jejímž cílem je omezení šikanózních insolvenčních návrhů, vyšší dohled nad insolvenčními správci a posílení transparentnosti celého procesu, je relevance této hrozby hodnocena jako nízká.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Organizovaný zločin spadá podle kompetenčního zákona č. 2/1969 Sb. do gesce MV a na jeho aktivním potírání se podílejí orgány činné v trestním řízení. Do boje proti organizovanému zločinu se v různé míře zapojují i další ministerstva, jejich podřízené složky a další státní orgány, zejména Ministerstvo financí (Finanční správa ČR, Celní správa ČR, Finanční analytický útvar), Ministerstvo spravedlnosti (trestněprávní legislativa) a Úřad vlády ČR (oblast drogové problematiky a korupce). Hlavní role v boji proti organizovanému zločinu připadá Policii ČR, v jejímž rámci se touto problematikou zabývají zejména Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování a Národní protidrogová centrála služby kriminální policie a vyšetřování. Skutkově jednodušší případy jsou řešeny v rámci jednotlivých krajských ředitelství policie službou kriminální policie a vyšetřování. Významnou roli v oblasti hrají i zpravodajské služby, které na problematice participují v rámci své působnosti a předávají v souladu s ustanovením § 8 odst. 3 zákona č. 153/1994 Sb. Policii ČR poznatky k případnému rozpracování.

V roce 2014 vznikl specializovaný tým **Daňová Kobra** za účasti Útvaru odhalování korupce a finanční kriminality služby kriminální policie a vyšetřování (nyní Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování), Generálního finančního ředitelství a Generálního ředitelství cel. Daňová Kobra řeší skutkově složité případy daňových úniků a daňové kriminality, a to především v oblasti daně z přidané hodnoty a spotřební daně. V roce 2016 došlo k rozšíření kompetencí Celní správy ČR v trestním řízení, kdy pověřené celní orgány jsou nyní příslušné k prověřování i těch trestných činů, kde došlo ke zkrácení daně z přidané hodnoty.

[22] Sněmovní tisk č. 785, ke konci září 2016 je projednáván ve druhém čtení v Poslanecké sněmovně Parlamentu ČR.

Organizovaný zločin využívá pro svoje potřeby nedostatků zákonů upravujících oblasti, které spadají do jeho zájmových sfér (legislativa upravující oblast veřejných zakázek, insolvenčního řízení, obchodních korporací, veřejných výdajů a další). Jednou z nejsilnějších zbraní proti aktivitám zločineckých skupin jsou kvalitní zákony upravující tyto procesy a jejich kontrolu.

Obecně platným nástrojem boje proti organizovanému zločinu je trestněprávní a navazující legislativa (zákon č. 40/2009 Sb., trestní zákoník[23], zákon č. 273/2008 Sb., o Policii ČR, zákon č. 141/1961 Sb., trestní řád, zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob[24] a další navazující předpisy). Tato oblast je dlouhodobě stabilní, nicméně jsou v ní spatřovány dílčí nedostatky – viz návrhy opatření dále v textu.

Hlavním strategickým materiálem v této oblasti je **Koncepce boje proti organizovanému zločinu na období let 2015 - 2017**[25], která byla schválena vládou ČR 12. listopadu 2014 usnesením číslo 919. Tato koncepce obsahuje vyhodnocení úkolů z předchozího materiálu, přehled o situaci v oblasti organizovaného zločinu a také 12 konkrétních opatření v oblasti monitorování situace, rozvoje systémových opatření a posílení mezinárodní spolupráce. Tématu se také věnují další koncepční materiály (**BS 2015[26], Národní strategie protidrogové politiky na období 2010 – 2018[27], Vládní koncepce boje s korupcí na léta 2015 až 2017[28], Národní strategie boje proti obchodování s lidmi v ČR na období 2012 - 2015**[29] a další). Lze tedy konstatovat, že oblast je z koncepčního a strategického hlediska ošetřena dostatečně.

C. SWOT analýza

Všechny kategorie jsou seřazeny podle relevance.

Silné stránky

- Klidná bezpečnostní situace v ČR bez závažných incidentů vyžadujících významné nasazení bezpečnostních složek
- Stabilní stav trestněprávní legislativy
- Dobrá schopnost orgánů činných v trestním řízení čelit klasickým formám organizovaného zločinu
- Členství ČR v nadnárodních demokratických institucích a s ním spojená přijímaná opatření (zejména v oblasti legalizace výnosů z trestné činnosti)
- Mezinárodní spolupráce v rámci EU (Europol, společné vyšetřovací týmy, informační systémy)
- Dostatečné dlouhodobé strategické a koncepční zajištění oblasti

[23] Viz poznámka pod čarou číslo 14.
[24] Zákon prošel v roce 2016 novelizací (č. 183/2016 Sb.), která mění původní pozitivní výčet trestných činů, které mohou být právnické osobě přičítány, na výčet negativní, vylučující pouze konkrétní trestné činy, za které právnickou osoba nemůže být trestně stíhána. Dochází tím fakticky k rozšíření trestní odpovědnosti právnických osob.
[25] http://www.mvcr.cz/soubor/koncepce-boje-proti-organizovanemu-zlocinu-na-obdobi-let-2015-2017.aspx
[26] http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf
[27] http://www.vlada.cz/assets/ppov/protidrogova-politika/strategie_web.pdf
[28] http://www.korupce.cz/assets/protikorupcni-strategie-vlady/na-leta-2015-2017/Vladni-koncepce-boje-s-korupci-na-leta-2015-az-2017.pdf
[29] http://www.mvcr.cz/soubor/material-obchod-s-lidmi-pdf.aspx

- Daňová KOBRA jako příklad efektivní spolupráce složek bez nutnosti měnit legislativu a navyšovat výdaje

Slabé stránky

- Nedostatečná odolnost státní správy proti infiltraci kriminálních struktur ve vztahu k zákonu o státní službě.
- Některé dílčí nedostatky právní úpravy (oblast uchovávání údajů z telekomunikačního provozu, pomalá příprava nového trestního řádu).
- Vysoká administrativní zátěž příslušníků Policie ČR.
- Nedostatečná personální, materiální i legislativní připravenost v oblasti kybernetické kriminality (včetně adekvátního ohodnocení expertů).
- Nedostatek expertů pro oblast daňového šetření a rozkrývání závažné hospodářské trestné činnosti, nedostatečné policejní vzdělávání v této oblasti.
- Špatná mezinárodní spolupráce s geograficky i kulturně vzdálenými zeměmi (Vietnam, Čínská lidová republika, daňové ráje).
- Nemožnost kontrolovat pohyb osob v rámci schengenského prostoru a pohyb zboží v rámci celního území Evropské unie.
- Absence jednotné a uznávané definice organizovaného zločinu.

Příležitosti:

- Nová a připravovaná legislativa (zákon o střetu zájmů, registr smluv, elektronická evidence tržeb, nový zákon o veřejných zakázkách, zákon o prokazování původu majetku, centrální registr účtů).
- Výrazný pokles registrované kriminality umožňuje věnovat více prostředků pro boj s organizovaným zločinem.
- Koncepce rozvoje Policie ČR do roku 2020 – vytvoření strategického rámce pro střednědobé období[30].
- Schválené navyšování početního stavu policistů.
- Rozvoj finančního šetření v práci Policie ČR.
- Širší využití bezpečnostního výzkumu.
- Rozšíření týmů na principu Kobra do dalších oblastí.

[30] Materiál prošel vnitrorezortním připomínkovým řízením, byl projednán Výborem pro bezpečnost Poslanecké sněmovny Parlamentu ČR a je připravováno jeho předložení do mezirezortního připomínkového řízení.

Hrozby

- Nová a připravovaná legislativa (zákon o střetu zájmů, registr smluv, elektronická evidence tržeb, nový zákon o veřejných zakázkách, zákon o prokazování původu majetku, centrální registr účtů) – zejména její nevhodná implementace[31].
- Přechod organizovaného zločinu na více sofistikovanou trestnou činnost.
- Rizika plynoucí ze současné migrační krize (včetně nevhodné vízové liberalizace).
- Přesun kriminálních aktivit do kyberprostoru vedoucí k jejich těžšímu detekování.
- Účast bývalých příslušníků bezpečnostních složek na činnosti organizovaných skupin.

D. Doporučení k posílení odolnosti

Doporučení v této kapitole vychází z využití identifikovaných příležitostí a omezení dopadu možných hrozeb. Je třeba podotknout, že velké množství zejména legislativních opatření je v současné době přijímáno či navrhováno (viz výše v části C položka Příležitosti, případně v jiných dokumentech uváděných v části B tohoto materiálu). Vzhledem k tomu, že definitivní podoba některých zákonů není ještě známa a jejich efektivita bude záviset také na způsobu jejich implementace, není v tuto chvíli možné přinos jednotlivých nových návrhů a zákonů vyhodnotit. Nové zákony mohou přinést jak výrazné zlepšení, tak výrazné zhoršení současného stavu.

Jako velmi potřebná je třeba hodnotit opatření navrhovaná v materiálu Legislativní návrhy v oblasti vnitřní bezpečnosti, zejména úpravu uchovávání údajů z telekomunikačního provozu, využití zpravodajských informací jako důkazu v trestním řízení a rozšíření kontrol přeshraničního převozu peněžní hotovosti. Podobně přijetí a vhodná implementace Koncepce rozvoje Policie ČR do roku 2020 zajistí tomuto klíčovému bezpečnostnímu sboru odpovídající podmínky pro dlouhodobý rozvoj a posílí tím jeho kapacity v boji proti organizovanému zločinu.

Další navrhovaná opatření:

1. Zlepšit kapacitu (personální, odbornou, materiální i technologickou) orgánů činných v trestním řízení čelit kyberkriminalitě, získávat informace ze zabezpečené elektronické komunikace, znalecky zkoumat moderní komunikační zařízení a sdílet potřebná data v rámci informačních systémů. Pro odborníky na tuto problematiku je nutné zajistit adekvátní vzdělávání a dostatečně motivující platové prostředky.
2. Posílit týmy vyšetřující závažnou hospodářskou kriminalitu, neboť tako trestná činnost způsobuje státu nejvyšší finanční škody. Investice do této oblasti se mnohonásobně vyplatí ve formě uchráněných hodnot. Pro odborníky na tuto problematiku je nutné zajistit adekvátní vzdělávání a dostatečně motivující platové prostředky. V oblasti kriminality spojené s realizací veřejných zakázek a udílení dotací je třeba zvýšit schopnost Policie ČR danou trestnou činnost aktivně vyhledávat.
3. Revize trestní legislativy, zejména přijetí nového komplexního trestního řádu, který bude mimo jiné reagovat na současný vývoj v oblasti moderních technologií (komunikační technologie, kyberkriminalita, virtuální měny), dále vyhodnocení efektivity a dostatečnosti opatření v zákoně o Policii ČR.

[31] Tento bod je záměrně uváděn jak v příležitostech, tak v hrozbách – viz níže.

4. Prohloubit důvěru, kontakty a možnosti sdílení informací mezi zpravodajskými službami a útvary Policie ČR, aby docházelo k častější spolupráci v boji proti organizovanému zločinu a předávání takových informací, které budou všemi stranami tohoto vztahu využitelné.
5. Pořádat společná školení zástupců orgánů činných v trestním řízení ohledně nových trendů organizované trestné činnosti a možnostech jejího postihu.
6. Rozšířit dostupnost a provázanost statistických dat v oblasti organizovaného zločinu.
7. V oblasti celních a daňových úniků opětovně zavést povinnost výběr DPH při propouštění zboží do režimu volný oběh i u plátců daně. ČR je jednou z mála zemí, která tuto povinnost dovozcům neukládá. Zvážit úpravu zákona č. 234/2014 Sb., o státní službě, která by umožňovala větší otevřenost státní správy odborníkům ze soukromého sektoru, zjednodušovala průběh výběrových řízení a obsahovala pojistky proti pronikání organizovaného zločinu do státní správy.

PŮSOBENÍ CIZÍ MOCI

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Působení cizí moci není pro žádný suverénní stát věc neznámá, přičemž důvody pokusů cizí moci získávat informace a na jejich základě vliv v jiném státě sahají od ekonomického významu, přes sílu v otázkách mezinárodních vztahů až po historické aspekty již zaniklých nebo nově utvářených sfér vlivu. Neomezuje se na nepřátelsky naladěné členy mezinárodního společenství, nicméně pro potřeby Auditu je třeba věnovat primární pozornost těm projevům cizí moci, které pro ČR mohou znamenat bezpečnostní hrozbu. V souladu se současnými poznatky vyplývajícími jak z informací poskytovaných zpravodajskými službami, tak z jiných zdrojů lze takto hodnotit působení ze strany Ruské federace, Čínské lidové republiky, ale i některých nestátních aktérů jako je tzv. Islámský stát.

Jako tradiční a průběžně monitorované lze vnímat snahy cizí moci působit v ekonomické oblasti, ať už se jedná o získávání informací o ekonomických aktivitách subjektů stojících mimo strukturu státu, tak o ovlivňování strategických ekonomických rozhodnutí na úrovni vedení státu, dále všechny ostatní formy špionáže (ve smyslu soustřeďování zneužitelných informací ze strany zpravodajských služeb cizího státu), které nejsou prováděny s ekonomickou motivací.

Staronovým projevem působení cizí moci je pak propaganda a šíření dezinformací jako prostředek informační války, kterou se cizí mocnosti pokouší ovlivňovat stát v oblasti řízení a využívání komunikačních a informačních kanálů nebo technologií, jejichž prostřednictvím působí na veřejné mínění. Vedle rizik působení cizí moci v oblasti ekonomické, kde nedostatečné řešení aktivit cizí moci může vést k důsledkům různé závažnosti od ekonomicky nevýhodných situací a oslabování hospodářského postavení státu přes vznik nadměrné závislosti na konkrétním investorovi – cizí moci, až po ztrátu ekonomické nezávislosti státu z důvodů nedostatečné diverzity surovinových zdrojů, struktury investic nebo energetické nezávislosti[32], se tak znovu ve větší míře objevuje aktivizovaná politická propaganda, která testuje především odolnost společnosti vůči ovlivňování, ale má významný vliv i na názory a kroky odpovědných osob na všech úrovních rozhodovacího procesu ve státě. Současná propaganda cizí mocnosti se zaměřuje z velké části na **dezinformační kampaň** a její metoda nepracuje s propagováním určitého světonázoru, ideologie nebo způsobu života, ale spíše s relativizací a rozmělňováním informací, bořením struktury vnitro-společenské důvěry. Proto je i samotný termín propaganda vnímán jako zastaralý a v současnosti je k pojmenování tohoto projevu působení cizí moci používán právě termín dezinformační kampaň. Taková kampaň je jako projev informační války součástí hrozeb hybridních, kterým se věnuje zastřešující kapitola, a tedy jednou z nejvážnějších hrozeb zejména vzhledem k informační otevřenosti demokratických společností a silně omezeným možnostem státu založeného na principu vlády práva na takovou situaci reagovat.

S tématem dezinformační kampaně pak velmi úzce souvisí oblast mediálního práva, a to na úseku regulace vlastnické struktury médií ve státě a možnosti prověřování zákonnosti obsahu médií.

[32] Tématu se blíže věnuje kapitola Energetická, surovinová a průmyslová bezpečnost.

Samostatnou kapitolu pak tvoří problematika nových médií (zpravodajství na internetu, sociální sítě apod.)

2. Třídění rizik, hrozeb a jejich důsledků

Faktory, které v oblasti působení cizí moci představují pro ČR riziko, členíme na **rizika přicházející zvenčí (faktory externí) a vnitřní slabiny systému (faktory interní).**

Mezi externí faktory řadíme:

- **Cílenou snahu cizí moci**
  - ovlivňovat veřejné mínění v ČR (zejména podkopávat důvěru v samostatný demokratický právní stát), v rozporu se zájmy ČR

    Tato snaha je uplatňována všemi dostupnými prostředky, zejména cílenou prací s informacemi, podporou tradičních animozit ve společnosti, rozdmýcháváním kritických nálad vůči establishmentu a integračním strukturám, případně využíváním negativního postoje části veřejnosti vůči nadnárodním uskupením, jejichž je ČR členem, a spojencům. Těmito metodami je ve společnosti vyvolávána představa, že stát je řízen špatně, že orientace na euroatlantické integrační struktury je pro zemi škodlivá apod.
  - ovlivňovat veřejnou správu a politické představitele

    Jak vyplývá z výročních zpráv BIS, budují v ČR přístupové a vlivové sítě mezi zástupci parlamentních politických stran, státními úředníky a lobbisty jak ruské, tak čínské zpravodajské služby.
  - ovlivňovat chování státu prostřednictvím ekonomických nástrojů

    Posilování přítomnosti cizí moci postupným získáváním vlivu v určitých sektorech hospodářství.
  - získávat zákonem chráněné a jiné veřejně nepřístupné informace, jejichž získání může vést k ohrožení nebo poškození zájmů státu.

Mezi externí řadíme i následující faktory, jejichž povaha je však mnohdy **smíšená**:

- **Cizinecké komunity** vytvářející zázemí pro aktivity cizích států[33].

V ČR lze sledovat činnost několika uskupení na bázi příslušnosti k určité menšině, jejichž oficiální činnost je vedena jako obchodní, kulturní, vědecká nebo náboženská, které však často vystupují jako organizátoři akcí na podporu názorů, jež neobstojí v demokratické diskuzi, případně organizují návštěvy kulturních a politických představitelů nedemokratických režimů a v neposlední řadě existuje i podezření, že financují nebo zprostředkovávají financování aktivit, které nejsou v souladu se zájmy ČR.

- **Koncentraci vlastnictví médií v cizích rukou a u omezeného počtu osob.**

[33] Tématu se částečně věnuje kapitola Terorismus.

- **Existenci relativně velkého množství mediálních a kvazi-mediálních projektů v českém nebo slovenském jazyce** s proxy agendou působících na českou veřejnost.

Jako interní faktory v oblasti působení cizí moci identifikujeme:

- **Slabou odolnost veřejnosti proti ovlivňování a snahám snižovat důvěru v demokratický právní stát** - slabá či absentující občanská a mediální gramotnost.
- **Slabou odolnost veřejné správy a politické reprezentace proti ovlivňování a získávání informací včetně oblasti kybernetické odolnosti.**
- **Působení politických entit a představitelů otevřeně hájících zájmy odlišné od zájmů ČR.**
- **Působení bývalých vrcholných představitelů státu pod vlivem zájmů odlišných od zájmů ČR.**
- **Působení ekonomických subjektů hájících zájmy odlišné od zájmů ČR.**
- **Absenci systematických nástrojů státu k obraně proti dezinformačním kampaním.**
- **Nedostatečnou schopnost motivovat cizinecké komunity ve prospěch zájmů ČR.**

Samotné hrozby pak lze v prostředí, kde působí popsané faktory v různé míře provázanosti a různé intenzitě, třídit na **tři okruhy.** Spolu s nimi pak lze uvést i jejich **důsledky, z nichž některé již byly v ČR zaznamenány.**

I) Ovlivňování veřejného mínění

Zhodnocení relevance hrozby pro ČR: **Vysoká**

- cílené podkopávání důvěry v samostatný demokratický právní stát a budování vstřícnosti vůči zájmům cizích států
- Šíření dezinformací prostřednictvím mediálních a kvazi-mediálních platforem včetně sociálních sítí, „nezávislých“ nevládních organizací, veřejně známých osobností včetně politických představitelů, kteří podléhají vlivu nebo prosazují zájem odlišný od zájmů ČR.
- Využívání médií s koncentrovaným vlastnictvím k prosazení mocenských zájmů
- Podněcování nepřátelských postojů vůči ČR v rámci cizineckých komunit a jejich zapojení do aktivit proti zájmům ČR.

Důsledek - Radikalizace veřejnosti[34]

- Nárůst extremistických a protisystémových postojů (ohrožujících zájmy ČR) ve společnosti a mezi politickou reprezentací.
- Nárůst podpory extremistických a protisystémových stran a hnutí, zvýšení jejich zastoupení v Parlamentu ČR a zastupitelských orgánech územní samosprávy.
- Snížení podpory pro ústavní uspořádání ČR a její začlenění do euroatlantických struktur, zvýšená podpora pro jeho revizi.

[34] Téma je rozpracováno v kapitolách Terorismus a Extremismus.

- Snížení důvěry občanů ve schopnost státu naplňovat životní zájmy ČR (BS 2015) (politická nezávislost ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel) a strategické zájmy ČR (zajištění vnitřní bezpečnosti a ochrany obyvatelstva).
- Radikalizace menšin zaměřená proti zájmům ČR.
- Narušování veřejného pořádku a bezpečnosti v důsledku incidentů při shromažďování, ozbrojování a občanských nepokojů.

II) Ovlivňování rozhodování na všech úrovních veřejné správy v rozporu se zájmy ČR

Zhodnocení relevance hrozby pro ČR: **Vysoká**

- Působení na pracovníky veřejné správy
- Působení na politické a ústavní představitele, a to jak stávající, tak využívání neformálního vlivu bývalých vrcholných představitelů státu. Na okraji pozornosti nestojí ani političtí představitelé v opozici, u kterých je spatřován potenciál do budoucna.

Důsledek - **Přijetí rozhodnutí poškozujících zájmy ČR**

- Snížení důvěryhodnosti a vyjednávací pozice ČR vůči spojencům a partnerům
- Poškození strategického zájmu ČR (BS 2015): posilování soudržnosti a efektivnosti NATO a EU a zachování funkční a věrohodné transatlantické vazby.
- Potenciální ohrožení životního zájmu ČR (BS 2015): politické nezávislosti ČR

III) Získávání zákonem chráněných informací nebo jiných veřejně nepřístupných informací, jejichž získání může vést k ohrožení nebo poškození zájmů státu

Zhodnocení relevance hrozby pro ČR: **Střední**

Důsledek - **Únik informací** schopných ohrozit bezpečnostní, politické a ekonomické zájmy ČR.

K evaluaci hrozeb, tedy k posouzení jejich závažnosti byla zvolena následující kritéria:

- **Závažnost hrozeb ve vazbě na závažnost zájmu, na který hrozba cílí** (třídění zájmů podle BS ČR – životní, strategické, další významné)
- **Rychlost a intenzita nástupu důsledků hrozby** (měřitelné v některých kategoriích na základě průzkumů veřejného mínění, popsaných jevů v ČR podle popsaných zkušeností ze zahraničí ad.)

Z pohledu chráněných zájmů vypočtených v BS 2015 (kritérium č. 1) pak lze konstatovat, že všechny tři definované hrozby v důsledku cílí na zájmy, které BS 2015 hodnotí jako životní. Ochranu těchto zájmů strategie vnímá jako základní povinnost vlády i všech orgánů veřejné správy. Pro jejich zajištění a obranu je ČR připravena využít všech legitimních přístupů a použít všechny dostupné prostředky. Hrozba **Ovlivňování veřejného mínění** cílí primárně na následující životní zájmy: zajištění

politické nezávislosti ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel.

Tato hrozba samozřejmě představuje závažné riziko i pro řadu zájmů, které BS 2015 označuje jako strategické. Zde spatřujeme výrazné riziko hrozby pro

- posilování soudržnosti a efektivnosti NATO a EU a zachování funkční a věrohodné transatlantické vazby,
- naplňování strategického partnerství mezi NATO a EU, včetně posilování jejich spolupráce při komplementárním rozvíjení obranných a bezpečnostních schopností,
- podpora demokracie, základních svobod a principů právního státu,
- zajištění vnitřní bezpečnosti a ochrany obyvatelstva,
- zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky,
- zajištění energetické, surovinové a potravinové bezpečnosti ČR a adekvátní úrovně strategických rezerv,
- prevence a potlačování bezpečnostních hrozeb ovlivňujících bezpečnost ČR a jejích spojenců.

Ovlivňování rozhodování na úrovni ústředních orgánů státní správy a vyšší v rozporu se zájmy ČR pak bylo vyhodnoceno jako hrozba primárně cílící na zájmy definované jako strategické (nad rámec výčtu shora lze uvést ještě zajištění kybernetické bezpečnosti a obrany ČR), přičemž při dlouhodobém působení nebo při propuknutí hrozby u většího množství vysoce postavených představitelů státu, resp. v případě volebního úspěchu politického uskupení, které je třeba i skrytě pod vlivem cizí moci, se pak hrozba s absolutní závažností může cílit na zájmy životní. Lze však předpokládat, že v případě ovlivnění byť i vysoce postaveného představitele státu se stále bude při jeho dalších krocích jednat o ovlivnění individuálních rozhodnutí spadajících do jeho pravomoci, nedojde však k ovlivnění strategických rozhodnutí na úrovni kolektivní. I tak je ovšem nutné mít na paměti, že určití jednotlivci mají pro bezpečnost státu klíčový význam vzhledem k významnému vlivu např. na ozbrojené složky státu. Tato hrozba může samozřejmě zcela významně ovlivnit drtivou většinu zájmů, které BS 2015 označuje jako další významné.

Získávání citlivých nebo zákonem chráněných informací pak z trojice definovaných hrozeb v drtivé většině případů cílí na ohrožení zájmů definovaných jako další významné, v menší míře pak strategické. Je však nutno mít na paměti, že tato hrozba je zároveň prostředkem a nástrojem umožňujícím ohrožení zájmů životních, neboť soustavný sběr poznatků z prostředí, na které chce cizí moc působit, je prostředkem k dosažení vlivu na veřejnost i politickou reprezentaci.

Kritérium (č. 2) **rychlosti a intenzity nástupu důsledků hrozby** je měřitelné obtížně. Nicméně v situaci, kdy běžné kritérium hodnocení hrozby, tedy pravděpodobnost, že bude realizována, postrádá smysl, neboť všechny tři popsané hrozby jsou v prostředí ČR již realitou, je nutné zvolit kritérium jiné. V případě ovlivňování veřejného mínění by určité vodítko mohly přinést cílené a opakované průzkumy veřejného mínění, které však v ČR takto podrobně prozatím neproběhly.[35]

[35] První cílené šetření proběhlo v září 2016, kdy Agentura STEM provedla průzkum na reprezentativním vzorku 1061 respondentů. Bylo testováno, do jaké míry veřejnost věří v dezinformace šířené pro-kremelskými, tzv. "alternativními" médii. Z šetření vyplývá, že 25,5 % Čechů věří dezinformacím, 24,5 % věří alternativním (dezinformačním) médiím více než

(Průzkumy v ČR[36] na téma nedemokratických alternativ vládnutí nevykazují v posledních letech žádné větší výkyvy v názorech obyvatel, ani pokud se týká podpory takového vývoje, ani vnímání vývoje jako hrozby. Na druhou stranu lze však z prvního cíleného průzkumu vyhodnotit vysokou míru spoléhání se na alternativní zdroje informaci a náchylnost veřejnosti považovat zkreslené informace za pravdivé.) Toto kritérium tak lze zejména analyticky zpracovat na základě zkoumání již proběhlých pokusů o ovlivnění v zahraničí (např. kauza Lisy z Německa nebo dezinformace šířené před referendem v Holandsku ad.) Stejně tak v případě dalších dvou hrozeb by kvantifikace rychlosti a intenzity nástupu jejich důsledků předpokládala doposud neprovedené hodnocení řady jednotlivých útoků a posouzení, zda jejich jednotícím cílem je působení cizí moci ve formě tzv. hybridní kampaně[37].

Při evaluaci hrozeb v této kapitole je tak zejména třeba mít na paměti, že ačkoli ve všech třech definovaných oblastech hrozeb cizí moc v ČR dlouhodobě působí, aktuálně je zaznamenán zřetelný nárůst aktivity.

Na závěr pak je třeba upozornit na skutečnost, že demokratická společnost nesmí při potírání hrozeb nikdy využít nedemokratické prostředky, což je zároveň její slabá, ale i nejsilnější stránka. To ovšem neznamená, že se musí spolehnout jen na stávající prvky bezpečnostního systému a nemůže uvažovat o posílení vlastní odolnosti, k čemuž současná zhoršující se bezpečnostní situace přináší příležitost ve formě vyšší míry pochopení pro bezpečnostní aspekt při posuzování změn systému a jeho celkovou vyšší ostražitost. Každé opatření však musí projít důkladným testem proporcionality a musí být podrobeno otevřené veřejné debatě.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

V oblasti předcházení a potírání hrozeb zpracovávaných v rámci této kapitoly v současnosti neexistuje jedna instituce, která by koncentrovala drtivou většinu odpovědnosti, proto je při výčtu nutné začít popisem role vlády a dále následovat rozborem více či méně rozptýlených nástrojů a kompetencí jednotlivých institucí.

Vláda ČR

Obecná, průřezová role vlády při předcházení a potlačování bezpečnostních hrozeb, pramenících z působení cizí moci, vyplývá z jejího ústavního postavení vrcholného orgánu výkonné moci (čl. 67 odst. 1 Ústavy ČR). Vláda v tomto postavení řídí, kontroluje a sjednocuje činnosti ministerstev (§ 28 odst. 1 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR), která působí ve specializovaných působnostech, vymezených kompetenčním zákonem.

---

tradičním, 50,2 % české veřejnosti si myslí, že za stovky tisíc syrských uprchlíků, kteří přicházejí do Evropy, nesou zodpovědnost Spojené státy americké; 28,3 % Čechů si myslí, že ruský vojenský zásah v Sýrii pomáhá řešit evropskou migrační krizi; pouze 31,5 % dotázaných považuje členství v EU za dobrou věc.
Pokud by se konalo referendum o vystoupení ČR z EU, 40,6 % lidí by se s největší pravděpodobností rozhodlo až na základě kampaně probíhající před referendem. http://www.evropskehodnoty.cz/wp-content/uploads/2016/09/Dopady-dezinforma%C4%8Dn%C3%ADch-operac%C3%AD-v-%C4%8Cesk%C3%A9-republice.pdf.

[36] http://cvvm.soc.cas.cz/media/com_form2content/documents/c1/a7529/f3/pd160324.pdf.

[37] Téma jednotícího úmyslu kampaně je rozpracováno v zastřešující kapitole hybridní hrozby.

Speciální role vlády je založena na jejím koordinačním vztahu ke zpravodajským službám ČR, za jejichž činnost odpovídá a ukládá jim úkoly v mezích jejich působnosti. Oprávnění ukládat úkoly zpravodajským službám je svěřeno i prezidentu republiky (§ 7 a § 8 odst. 4 zákona č. 153/1994 Sb., o zpravodajských službách ČR).

Zpravodajské služby

ZS mají vzhledem k povaze hodnocených hrozeb významnou úlohu při získávání, shromažďování a vyhodnocování informací v celém širokém spektru působení cizí moci, zahrnující samozřejmě i zabezpečování informací o původcích propagandy, nepřátelské vůči zájmům ČR, a o dalších okolnostech a jevech, souvisejících s jejím šířením a pronikáním.

Základní metodou ZS je získávání informací a jejich vyhodnocování, k čemuž mají v příslušné legislativě upraveny nástroje pro získávání informací, které je nutné s ohledem na narůstající a zcela nové hrozby modifikovat a přizpůsobit novému bezpečnostnímu prostředí, stejně jako i kapacity a prostředky k jejich uplatňování.

Strategické materiály a legislativa:

zákon č. 153/1994 Sb., o zpravodajských službách ČR,

zákon č. 154/1994 Sb., o BIS,

zákon č. 289/2005 Sb., o Vojenském zpravodajství.

Ministerstvo vnitra

V současné době je role MV roztříštěna do nepropojených úseků správy vnitřních věcí, jejichž vliv na oblast působení cizí moci je vždy jen dílčí. Jedná se o: vnitřní pořádek a bezpečnost včetně analýzy trendů vývoje, shromažďovací právo, registrace politických subjektů, otázky cizinecké a pobytové politiky, udělování občanství, personální otázky spojené s výkonem státní služby a řada dalších. Významnou úlohu uvnitř resortu plní také Policie ČR, a to zejména v okamžiku, kdy některý z projevů působení cizí moci dosáhne intenzity trestného činu[38].

Komplex nástrojů ve všech dotčených oblastech resortu nebyl v minulosti konstruován ani systémově posuzován z hlediska možnosti odvrátit hrozbu působení cizí moci jako formu hybridního útoku vedeného s jednotícím cílem cizí moci[39]. Prvotní posouzení, které bylo v rozsahu kapitoly zpracováno, nezaznamenalo až na výjimky v oblasti trestního práva (viz část doporučení) výrazné legislativní nedostatky v rozsahu využitelných nástrojů, spíše identifikovalo výrazný nedostatek souhrnného hodnocení problematických zjištění a koordinace činnosti při jejich řešení.

Strategické materiály a legislativa:

Stát disponuje koncepčními materiály k dílčím oblastem v gesci resortu, tyto dílčí materiály ovšem neobsahují hodnocení problematik z hlediska ohrožení ze strany cizí moci, ani nehodnotí účinnost stávajících nástrojů při potírání identifikovaných hrozeb.

[38] Tyto projevy mohou naplnit celou škálu skutkových podstat od tradičního vyzvědačství, přes podstaty chránící obchodní tajemství, dopravované zprávy a soukromí, přes šíření poplašné zprávy po různé druhy trestných činů narušujících soužití lidí a trestné činy proti lidskosti, míru a válečné trestné činy.

[39] Blíže v kapitole Hybridní hrozby.

Stejně tak právní úprava v dostatečné míře ošetřuje všechna odvětví včetně úpravy nástrojů sankčních a jiných, které mohou být aplikovány při potírání hrozeb.

Národní bezpečnostní úřad

Roli NBÚ v problematice řešení hybridních hrozeb a působení cizí moci na území ČR lze spatřovat především v zajišťování kybernetické bezpečnosti a navyšování odolnosti české IT infrastruktury (zejména tedy její kritické části[40]) proti kybernetickým útokům. Mimo kybernetickou bezpečnost rozhoduje NBÚ především o vydání a zrušení platnosti osvědčení o bezpečnostní spolehlivosti fyzickým i právnickým osobám a plní úkoly v oblasti ochrany utajovaných informací, což jsou důležité aktivity v rámci boje s působením cizí moci na území ČR a hybridními hrozbami.

Strategické a další koncepční materiály:

Národní strategie kybernetické bezpečnosti ČR na období let 2015 až 2020

Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020

Memorandum o porozumění (MOU) v oblasti kybernetické obranné spolupráce mezi NATO a ČR

Legislativa:

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)[41]a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Ministerstvo zahraničních věcí

MZV je ústředním orgánem státní správy ČR pro oblast zahraniční politiky, zabezpečuje vztahy ČR k ostatním státům, mezinárodním organizacím a integračním seskupením. MZV vydává povolení k dlouhodobému pobytu členům personálu zastupitelského úřadu cizího státu nebo mezinárodní vládní organizace akreditované v ČR anebo jejich rodinným příslušníkům registrovaným MZV a prohlašuje jej za neplatné. MZV prostřednictvím svých zastupitelských úřadů uděluje diplomatické vízum a zvláštní vízum a má rovněž právo tato víza prohlásit za neplatná. Dle Vídeňské úmluvy pak přijímající stát může kdykoliv a bez povinnosti uvést důvody pro své rozhodnutí oznámit vysílajícímu státu, že šéf mise nebo kterýkoliv člen diplomatického personálu mise je persona non grata anebo že kterýkoliv jiný člen personálu mise je nepřijatelný.

Strategické materiály a legislativa:

Bezpečnostní strategie ČR z r. 2015

Koncepce zahraniční politiky ČR z r. 2015

zákon č. 326/1999 Sb., o pobytu cizinců na území ČR a změně některých zákonů, ve znění pozdějších předpisů.

Vídeňská úmluva o diplomatických stycích (vyhl. MZV č. 157/1964 Sb.).

[40] Kritická informační infrastruktura (KII) a významné informační systémy (VIS).

[41] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (tzv. vyhláška o kybernetické bezpečnosti) Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Ministerstvo kultury

MK plní roli gestora legislativy, nástroje k regulaci obsahu rozhlasového a televizního vysílání jsou v rukou nezávislého ústředního správního úřadu - Rady pro rozhlasové a televizní vysílání, která vykonává zákonné kompetence i ve vztahu k audiovizuálním mediálním službám na vyžádání. Legislativa obsahuje postup pro udělování licencí k provozování vysílání. I zde má kompetence Rada, která v řízení o udílení licence k provozování analogového rozhlasového vysílání obligatorně posuzuje i transparentnost vlastnických vztahů ve společnosti žadatele a disponuje i celou řadou dalších nástrojů. Právní úprava obsažená v tiskovém zákoně je na základě Článku 17 Listiny základních práv a svobod postavena na liberálním přístupu – vyžaduje pouze evidenci periodického tisku Ministerstvem kultury. Stanoví, že za obsah tisku odpovídá jeho vydavatel, který je v tomto ohledu vázán pouze obecnými právními předpisy.

Legislativa:

Zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů.

Zákon č. 132/2010 Sb., o audiovizuálních mediálních službách na vyžádání a o změně některých zákonů (zákon o audiovizuálních mediálních službách na vyžádání).

Zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů.

Ministerstvo školství, mládeže a tělovýchovy

Mezi nástroje s výraznou účinností v boji proti působení cizí moci zejména v oblasti dopadu desinformačních kampaní a podkopávání důvěry v demokratický právní stát a budování vstřícnosti vůči zájmům cizích států je vzdělávání v občanské a mediální gramotnosti. Význam těchto nástrojů musí být zdůrazněn v průběhu celého systému vzdělávání. K tomu slouží nástroje, které má MŠMT k dispozici v souladu se školským zákonem zejména při tvorbě tzv. vzdělávacích programů.

Legislativa:

Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání.

C. SWOT analýza

Silné stránky

- Ustálené demokratické ústavní a politické zřízení, fungující stát, hospodářská stabilita, nízká nezaměstnanost a z nich plynoucí relativní spokojenost veřejnosti s kvalitou života.
- Členství ČR v evropských a euroatlantických integračních strukturách.
- Dlouhodobé monitorování situace v oblasti působení cizí moci ze strany zpravodajských služeb.
- Fungující mezinárodní spolupráce a výměna informací na úrovni bezpečnostní komunity.
- Robustní veřejnoprávní média institucionálně nezávislá na státní moci.

- Rozvinuté aktivity neziskového, žurnalistického a akademického sektoru v oblasti rozkrývání dezinformací cizí moci.
- Nejednotnost cizineckých diaspor v ČR.

Slabé stránky

- Podceňování hrozby Působení cizí moci na úkor jiných hrozeb.
- Absence jednotného postoje k hrozbě napříč politickým spektrem.
- Nejednoznačný postoj veřejnosti k vnímání existence a významu hrozby.
- Nezbytnost hájit garantovaná práva a svobody (např. svoboda projevu a další) a demokratické principy uplatňování státní moci při potírání hrozby a s tím spojená omezená možnost reakce ze strany státu.
- Slabá odolnost veřejnosti proti ovlivňování a snahám snižovat důvěru v demokratický právní stát metodou dezinformačních kampaní
- Nedostatečná schopnost státu zajistit kvalitní vzdělávání v oblasti občanské a mediální gramotnosti.
- Slabá odolnost veřejné správy a politické reprezentace proti ovlivňování a získávání informací, případy vědomé i nevědomé spolupráce.
- Nedostatečné prověřování dodavatelů a subdodavatelů informačních a komunikačních technologií (ICT) a samotných ICT produktů (software i hardware) v institucích významných pro bezpečnost státu.
- Špatně nastavené politiky kybernetické bezpečnosti v institucích významných pro bezpečnost státu a podcenění edukace zaměstnanců v oblasti kybernetické bezpečnosti.
- Omezené finanční prostředky institucí významných pro bezpečnost státu vynaložitelné na prevenci a zvládání kybernetických hrozeb či adekvátní ohodnocení specialistů na problematiku ICT.
- Nedostatečná schopnost motivovat cizinecké komunity ve prospěch zájmů ČR.
- Úprava zákona č. 106/1999 Sb., o svobodném přístupu k informacím, umožňující příliš široké vydávání informacích týkajících se bezpečnosti státu.
- Nedostatečné možnosti regulátora mediálního prostoru zjišťovat informace potřebné pro výkon stávajících oprávnění.
- Absence strategické komunikace státu jako reakce na dezinformace a pro posílení vlastní důvěryhodnosti.
- Neschopnost státu rychle vyhodnocovat závažnost jednotlivých dezinformací a neschopnost zpracovat rychlou reakci.

Příležitosti

- Relativně otevřená identifikace záměrů ze strany cizí moci, možnost analyzovat již proběhlé pokusy o ovlivňování v zahraničí i již uskutečněné reakce ze strany partnerských států.

- Zvýšená pozornost věnovaná dané problematice v jiných členských státech EU a v rámci evropských struktur (např. StratComm team EEAS), možnost zapojit se do společných iniciativ a podílet se na hledání společných řešení.
- Možnost těžit z konkrétních zkušeností několika států, které nedávno nově nastavily systémová opatření proti působení cizí moci.
- Zájem řešit hrozbu jak ze strany státu, tak ze strany nevládního sektoru a akademické obce – synergie v přijímaných opatřeních.
- Historická zkušenost obyvatelstva s ovlivňováním řízení státu ze strany velmoci.

Hrozby

- Ovlivňování veřejného mínění v neprospěch demokratického právního státu anebo ve prospěch cizí moci.
- Selhání systému detekce aktivit cizí moci.
- Závažné poškození důvěryhodnosti významné demokratické instituce (Česká televize, Policie ČR aj.)
- Vznik českojazyčného plošného média prosazujícího zájmy cizí moci odlišné od ČR.
- Nárůst významu/zisk podílu na moci antisystémových, extremistických a jinak radikálních uskupení oslabujících demokratický systém.
- Úspěch ve volbách politického uskupení prosazujícího zájmy odlišné od zájmů ČR.
- Existence paramilitárních uskupení s přímou nebo nepřímou podporou cizí moci.
- Ovlivňování rozhodování na všech úrovních veřejné správy v rozporu se zájmy ČR
- Aktivity subjektů s významným podílem na výkonné, zákonodárné a soudní moci.
- Aktivity jednotlivých představitelů s významným vlivem na rozhodování v oblasti bezpečnosti.
- Aktivity politických subjektů a politických představitelů prosazujících zájmy, které jsou v rozporu se zájmy ČR.
- Scénář politického a společenského vývoje naplňujícího cíle cizí moci.
- Získávání zákonem chráněných informací nebo jiných veřejně nepřístupných informací, jejichž získání může vést k ohrožení nebo poškození zájmů státu
- Vědomé prozrazení informací ze strany politických představitelů nebo představitelů veřejné správy.
- Neúmyslné prozrazení informací ze strany politických představitelů nebo představitelů veřejné správy.
- Porušení důvěrnosti informací prostřednictvím porušení kybernetické bezpečnosti.

D. Doporučení k posílení odolnosti

1. Nastavení mechanismu vyhodnocování poznatků o působení cizí moci v rámci vzájemné spolupráce a koordinace navrhovaných opatření.
2. Zřízení pracovišť na příslušných úřadech pro hodnocení dezinformačních kampaní a jiných projevů vlivu cizí moci.
3. Vytvoření systému školení úředníků veřejné správy zaměřeného na zodolnění vůči pokusům o ovlivnění ze strany cizí moci.
4. Vytvoření nabídky takového školení na dobrovolné bázi pro další osoby, které z hlediska své činnosti mohou být předmětem zájmu cizí moci.
5. Prověření efektivity školení zásad bezpečného chování na internetu ve státních institucích a stanovení minimálního standardu pro taková školení.
6. Návrhy do oblasti trestního práva hmotného i procesního: (možnosti využití zpravodajských poznatků v trestním řízení aj.).
7. Vytvoření aktivních mediálních strategií důležitých demokratických institucí vůči působení cizí moci.
8. Zajištění podmínek pro uplatňování personální politiky zpravodajských služeb tak, aby byly schopné nabrat potřebný počet uchazečů, vychovat z nich kvalitní experty a ty ve službě pro stát udržet.
9. Zajištění rychlosti předávání zpravodajských informací zákonným adresátům a efektivní zpětné vazby.
10. Opatření v mediálním právu posilující schopnost příslušného orgánu státní správy získávat informace potřebné pro uplatnění zákonných kompetencí zejména ve vztahu k vlastnické struktuře provozovatelů vysílání, kteří jsou právnickou osobou.
11. Analýza efektivity stávajícím právních nástrojů v případě nutnosti reagovat na závažnou dezinformační vlnu.
12. Analýza výjimek k zohlednění bezpečnostních zájmů státu při sdělování informací podle zákona o svobodném přístupu k informacím.
13. Začlenění témat výzkum metod a kategorií propagandy, fact-check projekty a další mezi dotační tituly bezpečnostního výzkumu.
14. Úprava učebních plánů základních a středních škol (posílená výuka občanské gramotnosti a zavedení výuky mediální gramotnosti).

BEZPEČNOSTNÍ ASPEKTY MIGRACE

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Migrace[42] je přirozeným a trvalým historickým jevem a příležitostí. Pro imigranta, pro přijímací zemi i zemi původu. Mezinárodní obchod, zahraniční investice, zahraniční studium, odborné mezinárodní stáže, vysoce kvalifikovaní zahraniční pracovníci, či naopak nízko kvalifikovaná pracovní síla, manažeři nadnárodních korporací, ale i kulturní či vědecká mezinárodní spolupráce, to vše je velmi úzce spojeno s migrací. Výrazné restrikce či snad dokonce vyloučení imigrace by bylo samo hrozbou ekonomickou a vedlo by nejen ke ztrátě konkurenceschopnosti, ale v rámci reciprocity by se velmi pravděpodobně tato imigrační politika dotkla svobody pohybu samotných občanů ČR.

S migrací jsou však spojené i bezpečnostní aspekty. Hrozbu mohou ve specifických případech představovat konkrétní imigranti anebo jejich masy. Tato dílčí hrozba může mít podobu terorismu, organizovaného zločinu, ale i šíření infekční nákazy, kulturních zvyklostí neslučitelných s naším právním pořádkem nebo snížené ochoty k integraci. Vedle typu imigrace, resp. imigrantů, může svou roli v podobě migrační hrozby sehrát i objem migračních toků a bezpečnost může ohrozit masová neřízená imigrace, která by mohla vyústit ve společenské nepokoje či radikalismus, a to jak na straně minority, tak majority.

Problematiku migrace nelze chápat odděleně od vývoje mezinárodní situace v nejbližším sousedství i zemích původu. Z tohoto důvodu je třeba zaměřit se primárně na zdroje migrace – politické řešení konfliktů v zemích původu migrace, boj proti terorismu, boj proti převaděčům, zajišťování podmínek pro návrat migrantů a jejich zapojení do rekonstrukce země. V této souvislosti je rovněž nutné poskytnout pomoc a asistenci zemím bezprostředně sousedícím s ohnisky konfliktů.

Pracovní skupina v rámci analýzy bezpečnostních aspektů migrace identifikovala v souladu s **BS 2015** hrozbu nelegální migrace jako důsledek zvýšeného počtu lokálních ozbrojených konfliktů a také hrozbu nedostatečné integrace legálních migrantů, která může představovat zdroj sociálního napětí. Problematice možné radikalizace[43] členů přistěhovaleckých skupin či většinové společnosti se věnuje kapitola „Extremismus“, problematice terorismu a možnosti výskytu zahraničních bojovníků se věnuje kapitola „Terorismus“. Zejména hrozba neřízené migrace pak může být za určitých okolností jedním z prvků hybridní hrozby, řešené ve stejnojmenné kapitole.

---

[42] Migrace je definována jako přeshraniční fenomén, který je úzce spojen s kontrolou přeshraničního provozu, fungováním hraničních přechodů a překračováním státních hranic. Oproti tomu je nutno vymezit volný pohyb osob, který je základní zásadou evropské legislativy, upravuje ho směrnice 2004/38/ES o právu občanů EU a jejich rodinných příslušníků svobodně se pohybovat a pobývat na území členských států.

[43] Radikalizací jsou v této kapitole (v souladu s kapitolou Extremismus) rozuměny změny ideologických postojů člověka směrem k postojům vyhraněným, které vybočují z ústavních norem, vyznačují se prvky netolerance a útočí proti základním demokratickým ústavním principům. Tyto extremistické postoje jsou způsobilé přejít v aktivity, které působí destruktivně na stávající demokratický systém, včetně aktivit násilného charakteru. Radikalismem rozumíme zastávání těchto vyhraněných ideologických postojů, islámským radikalismem pak zastávání vyhraněných ideologických postojů, které splňují výše uvedenou definici, a které zároveň vycházejí z některých radikálních směrů v rámci islámu (případně se na toto náboženství odvolávají). V případě této kapitoly se soustředíme zejména na postoje vyzývající k různým formám násilí.

Dlouhodobým cílem imigrační politiky je tyto hrozby v rámci ČR eliminovat **nástroji řízené migrace**, kdy jsou bezpečnostní rizika snižována prostřednictvím regulačních, zejména legislativních nástrojů a následných procesů. Státem řízený migrační proces musí být bezpečným a vyváženým. V daném ohledu lze pak za skutečnou bezpečnostní hrozbu v kontextu celého migračního procesu označit právě migraci neřízenou. Míra vlastního a suverénního vlivu v procesu řízené migrace výrazně ovlivňuje míru rizika narušení rovnováhy migrací neřízenou.

Proces řízené imigrace je velmi úzce spjat s **procesem integrace**, neboť i řízená migrace může být dlouhodobě efektivní a funkční pouze v případě, že je spojena s úspěšnou integrací na území cílového státu. Právě schopnost a míra integrace do majoritní společnosti definuje možnosti a objem řízené imigrace.

Z hlediska značné provázanosti a obtížné oddělitelnosti identifikovaných hrozeb nevyužila pracovní skupina konkrétní metodu pro jejich identifikaci. Vycházela z dostupných koncepčních a strategických materiálů, které jí byly k dispozici[44]. U obou identifikovaných hrozeb – hrozba neřízené migrace a hrozba neúspěšné integrace - bylo posouzeno kritérium závažnosti dopadu vzniklých skutečností. Dále byla v rámci vnitřních faktorů uvažována otázka zranitelnosti a nastavení systému a v rámci vnějších faktorů otázka motivace, které ovlivňují úspěšnost systému.

2. Bezpečnostní prostředí a východiska pro ČR – kontext EU

Klíčové, jak pro správnou identifikaci všech hrozeb, tak pro analýzu rizik, je bezpečnostní prostředí, ve kterém se ČR nachází. Toto prostředí prochází dynamickými změnami, stále komplikovanější předvídatelností a skutečností, že na situaci v ČR mají stále častější a větší vliv i relativně vzdálené regionální či lokální konflikty. Pro hodnocení migračních jevů, nastavení souvisejících politik a řešení možných hrozeb je **určující účast ČR v EU a schengenském prostoru**. Zrušení kontrol na vnitřních hranicích států schengenského prostoru významným způsobem ovlivňuje způsob ochrany území ČR i ve vztahu k potírání nelegální migrace, a klade zvýšené nároky na spolupráci členských států EU. Ze členství ČR v EU vyplývají i další souvislosti. Předně se týkají významného vlivu evropského práva v oblasti ochrany hranic, migrace, azylu či vízové a návratové politiky. Díky principu volného pohybu osob v rámci EU se pak samotní občané EU a jejich rodinní příslušníci dostali téměř mimo možnost regulace ze strany národních států. Mobilita občanů EU představuje více než 50% podíl všech cizinců přechodně či trvale pobývajících na území ČR. Vedle evropského práva mají zásadní vliv v oblasti migrace i mezinárodněprávní závazky ČR, zejména závazky v oblasti ochrany lidských práv.

V případě, že své hodnoty a bezpečnost sdílíme v rámci určitého společenství, pak je nutné mít na paměti, že „řetěz je vždy tak silný, jak silný je jeho nejslabší článek.“ Závazkem pro ČR tak je, aby se nestala nejslabším článkem, a tedy zvýšeným bezpečnostním rizikem pro ostatní členy. Stejně musí tento závazek přijmout země ostatní. Ze zkušenosti posledních deseti let vyplývá, že rozhodnutí v oblasti migrace učiněná v národní kompetenci jedním státem EU mohou mít zásadní vliv na migrační realitu v jiných státech EU.

ČR přijala od vstupu do EU i po zrušení kontrol na vnitřních hranicích řadu kompenzačních opatření, která v rámci své přidělené kompetence naplňuje. V rámci své působnosti reaguje na nové trendy důsledným dodržováním přijatých norem, případně návrhy na změnu legislativy v souladu s evropským a schengenským aquis.

[44] Viz část B: Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje pro eliminaci hrozeb a rizik.

I) Hrozba neřízené migrace – neřízené příchody, nedodržování pravidel pobytu, neschopnost realizace návratů v případě porušení pravidel

Hrozba ztráty vlivu na řízenou migraci má dva faktory, vnitřní a vnější. **Vnitřní faktory** jsou dány zejména nemožností či neschopností nastavit imigrační systém či proces. Tento systém se pak stává zranitelným a při vyšším zatížení nedůvěryhodným. Této zranitelnosti lze předcházet kvalitní legislativou a kapacitním zajištěním celého systému. Větší rizika jsou však spojena s **vnějšími faktory**, které ovlivňují naplnění této hrozby, a tou jsou zejména objektivní skutečnosti (konflikty, přírodní vlivy a katastrofy, ale také vliv organizovaného zločinu v podobě převaděčských sítí), subjektivní motivace a psychologické faktory (např. ochota migrantů podstupovat rizika, nereálné představy o příležitostech v cílové zemi, ochota vynaložit finanční prostředky na cestu do cílové země za využití služeb převaděčů, subjektivní ekonomický motiv migrantů atd.). Schopnost předcházet těmto rizikům je výrazně složitější a závisí na míře ovlivnitelnosti rizika.

a) Otázka zranitelnosti (faktory vnitřní)

Při hodnocení zranitelnosti současného systému je nutné brát v úvahu bezpečnostní prostředí, tedy neexistenci vnitřních hranic mezi členskými státy schengenského prostoru a **omezenou možnost využít legislativní regulace z důvodu existujícího právního rámce EU**. Nástroje vízové politiky (zejména vydávání krátkodobých víz) jsou dnes téměř kompletně řešené na celoevropské úrovni, stejně tak standardy vnější ochrany hranic. Oblast mezinárodní ochrany je regulována na eurounijní úrovni, z valné většiny ve formě nařízení a směrnic. V oblasti legální migrace vznikla za posledních deset let celá řada směrnic, i když zde si členské státy stále zachovávají vyšší míru diskrece a lze některých národních regulačních mechanismů využít. Poměrně omezená možnost jednotlivých států zasahovat a utvářet migrační politiku jak na evropské, tak na národní úrovni, je patrná z vysokého procenta centrálně upravovaných dílčích politik. Stěžejní pro efektivní řízení migrace je **možnost a schopnost nastavit legislativou podmínky vstupu a pobytu cizinců tak, aby imigrace na území byla dlouhodobě přínosná, a aby byly minimalizovány případné negativní dopady.**

Vedle právního rámce je, z důvodu snížení rizika, nutné mít zajištěno **dostatečné kapacitní, kvantitativní i kvalitativní zajištění** (technické i personální), schopnost efektivního vízového procesu, kontroly na mezinárodních letištích, odhalování padělaných či pozměněných dokladů, ale také vymahatelnost práva – např. boj s nelegálním zaměstnáváním, prováděním pobytových kontrol a kontrol zaměstnavatelů apod. Neméně důležité je **sdílení zpravodajských informací v rámci národních států**, stav propojení informačních systémů a databází, a to jak na úrovni mezinárodní, tak na úrovni meziresortní v rámci státních orgánů a orgánů samosprávy, které na jedné straně snižuje administrativní náročnost procesu a na druhé straně efektivně odhaluje obcházení legislativy. Naprosto nezbytné se v dnešní době jeví nasazení moderních technologií, které nacházejí uplatnění v oblasti zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací. S tím souvisí i nutnost zajištění komunikačního prostředí, které je těmito technologiemi využíváno. Za zásadní lze též považovat nastavení **protikorupčních opatření** státní správy, protože oblast povolování vstupu a pobytu patří k rizikovým segmentům státní správy z hlediska korupce.

Zásadní pro efektivní řízení migrace jsou pak procesní funkční pravidla. Regulační nastavení musí být dostatečně odolné případnému zneužití (např. fiktivní zaměstnání, fiktivní studium, fiktivní rodinné vazby apod.) a musí poskytnout dostatečný nástroj pro řízení migrace. Tento proces musí být schopen v relativně krátkém časovém horizontu vyhodnotit, zda konkrétní cizinec je na území žádoucí či nikoliv, tedy zda představuje nějakou hrozbu. Přitom však tento proces nesmí bránit žádoucí legální migraci. Pokud jsou dobře nastaveny podmínky vstupu a pobytu, ale nefunguje procesní nastavení, dochází k vysoké míře obcházení zákona a narušení konceptu řízené migrace.

Klíčovou roli pro snížení individuálních rizik hrají **bezpečnostní složky, které musí být nedílnou součástí celého imigračního procesu.**

Podstatné z hlediska důvěryhodnosti celého imigračního procesu je schopnost státu zajistit **efektivně a účinně návrat** cizinců, kteří na území vstoupili neoprávněně, nebo oprávnění k pobytu na území ztratili. Na úspěchu či neúspěchu návratové politiky závisí míra rizika eskalace a účinnosti hrozby. I zde je kladen důraz na efektivitu a skutečnou proveditelnost návratu cizince do domovské země či do země svého posledního pobytu.

b) Otázka motivace (push a pull faktory)

Faktorem ovlivňujícím možné riziko ztráty či omezení vlivu na řízení migrace je motivace migranta, často podporována organizovanými či převaděčskými skupinami. Na motivaci k neřízené migraci působí zejména tzv. push a pull faktory.

Mezi **push faktory** patří vše, co působí na cizince v zemi, ze které odchází a podporuje jeho rozhodnutí odejít. Nejčastěji jde o bezpečnostní a ekonomickou situaci (konflikty, ohrožení specifických skupin) či přírodní faktory (katastrofy nebo nedostatek zdrojů). Nezanedbatelným faktorem je špatné vládnutí, korupce, nezaměstnanost, perzekuce, ztráta perspektivy. Nutné je udržení vysoké aktivity v rámci EU, a to jak ČR samotné, tak i společně v rámci regionálních uskupení typu Visegrádské skupiny.

Klíčový vliv na otázku migrace má socioekonomická situace, bezpečnost a životní úroveň obyvatel ve zdrojových a tranzitních zemích. Je proto nutné na úrovni EU i na národní úrovni posilovat využívání nástrojů k prevenci migrace ze zdrojových zemí prostřednictvím rozmanitých specializovaných programů na podporu. V tomto smyslu Evropská komise ve spolupráci s Evropskou službou vnější akce (ESVA) představila v červnu 2016 nový rámec pro partnerství se třetími zeměmi, který má přinést komplexní a koordinovaný přístup EU zacílený v dlouhodobém horizontu na kořeny migrace. Tento přístup se promítne do tzv. migračních kompaktů - na míru šitých dohod se třetími státy obsahujících jak pozitivní, tak i negativní pobídky, čerpajících z celé škály nástrojů komplexního přístupu EU. Z krátkodobého hlediska má být klíčovým prvkem partnerství účinná návratová politika. Příprava kompaktů s prioritními zeměmi Afriky a blízkého východu byla zahájena a ČR se do přípravy kompaktů aktivně zapojuje.

V rámci EU ČR také aktivně přispívá např. do Svěřeneckého fondu EU pro region Blízkého východu a západního Balkánu (MADAD) nebo do Svěřeneckého fondu pro Afriku. Finanční podpora ČR mimo jiné směřuje na podporu Světového potravinového programu (WFP) a také Úřadu Vysokého komisaře OSN pro uprchlíky (UNHCR). Mezi nástroje na národní úrovni patří zahraniční rozvojová spolupráce, humanitární pomoc a specializované programy, jako je Program MV na asistenci uprchlíkům v regionech původu a prevenci migračních pohybů v roce 2015a také Program humanitárních evakuací zdravotně postižených obyvatel MEDEVAC.

Mezi **pull faktory** se počítá vše, co přitahuje migranta do cílové země (dostupnost sociálního systému, úroveň zdravotní péče, postoj společnosti k migraci, míra ochoty společnosti tolerovat nelegální migraci, velikost usídlené komunity, snadná zneužitelnost správních řízení). Právě velikost diaspory v kombinaci s možným ekonomickým uplatněním, a to i v šedé ekonomice, je významným pull faktorem celé řady nelegálních migrantů. Významnou roli hrají také případné postihy za organizování nelegální migrace. Motivací k danému činu je vysoká odměna a minimální trestnost. Posouzen by tak měl být stav trestněprávní legislativy a současná míra společenské škodlivosti, organizování nelegální migrace a zprostředkování nelegálního pobytu včetně nelegálního zaměstnávání, ale i formy účelových prohlášení otcovství, formálních sňatků apod.

Nelegální migrace jako taková není v České republice trestným činem, nelegální migrant je tak postižen zejména vydáním rozhodnutí o správním vyhoštění se zákazem vstupu na celé území Evropské unie. Jednotlivé skutkové podstaty (uvedené v zákoně o pobytu cizinců) související s nelegální migrací nejsou zařazeny ve stejné kategorii pro určení délky zákazu vstupu. Toto nastavení délky zákazu vstupu by mělo odpovídat závažnosti uvedeného jednání.

Hrozba neřízení migrace spočívá v nedostatečném nastavení funkčnosti systému, jeho omezené důvěryhodnosti a omezené schopnosti realizovat stanovené postupy (návraty) z hlediska vnitřních faktorů. Pokud tento legislativní rámec nebude dostatečně nastaven a dodržován, může dojít ke vzniku pull faktorů a dalších motivací systém obejít či zneužít. Zde je nutné zdůraznit význam prevence a bdělosti, které by měly být zajištěny dostatečným sdílením informací a kooperací mezi dotčenými vládními orgány. Je nutné zmínit, že význam této hrozby je klíčový na národní úrovni, nicméně pracovní skupina zde poukazuje na omezenou možnost členských států EU využít národní legislativní regulace z důvodu existujícího právního rámce EU.

II) Hrozba neúspěšné integrace

Integrace je dlouhodobý dvoustranný[45] proces začleňování cizinců do společnosti s důrazem na nezbytnost zapojení jak cizinců, tak i majoritní společnosti. **Cílem integrační politiky je bezproblémové a oboustranně prospěšné soužití cizinců a majoritní společnosti**. Úspěšná integrace na území je zásadním faktorem pro eliminaci mnoha negativních jevů, které ve svém důsledku mohou vést i k bezpečnostním hrozbám.

Neintegrovaný cizinec na území představuje hrozbu ve vztahu k běžnému soužití s majoritní společností a ve vztahu k sociálnímu smíru. Nedostatečná integrace přináší **riziko vytváření uzavřených komunit cizinců**. Jejich společenská izolace či sociální vyloučení vedou nejen k osobní frustraci, ale i ke vzniku konfliktů mezi cizinci a majoritou či komunitami cizinců navzájem. Nedostatečná či neúspěšná integrace přináší riziko nárůstu xenofobie, netolerance a extremismu ve společnosti.

Nezvládnutá integrace je však **rizikem i pro život migrantů** – nesamostatnost a neinformovanost migrantů může být příčinou manipulovatelnosti, vydírání a ztráty legálního pobytu. Příčinou závislosti migrantů je zejména omezená znalost češtiny, která jim neumožňuje orientovat se ve společnosti, v místních zvyklostech a pravidlech soužití, a která neumožňuje navazovat vztahy s majoritou.

Úspěšná integrace cizince naopak snižuje míru ohrožení imigranta samotného, umožňuje mu vést důstojný a samostatný život, umožňuje jeho další rozvoj a zvyšuje pravděpodobnost osobního úspěchu či prosperity jeho rodiny. Úspěšná integrace tak přispívá i k prosperitě celé společnosti. Klíčovou roli v integraci sehrává schopnost osamostatnit se, nebýt závislý na pomoci druhých – zprostředkovatelích, tlumočníkovi, zaměstnavateli, státu (sociálních dávkách) apod. Cestou k samostatnosti je dostatečná informovanost, znalost práv a povinností, respekt k hodnotám ČR i EU a jejich přijetí, zejména však schopnost komunikace v českém jazyce.

a) Otázka zranitelnosti (faktory vnitřní)

Pro zajištění funkčnosti systému je nutná existence strategických a koncepčních dokumentů, které spolu s dostatečným kapacitním zajištěním a úspěšnou praktickou implementací umožní funkčnost a flexibilitu systému. Z tohoto hlediska ČR disponuje vyváženou integrační politikou, která není významněji harmonizována společnými nástroji EU a udržuje si tak vysokou míru národní diskrece.

[45] Případně je možné uvažovat proces integrace jako trojstranný, neboť na průběh integrace má do jisté míry vliv i působení země původu.

b) Otázka motivace (faktory vnější)

Integraci, která je primárně **zaměřena na migranty** s plánem trvalého usídlení na území, proto nelze nadále vnímat jen jako záležitost volby. Jako nezbytné se jeví podmínit pobyt této skupiny imigrantů na území jejich akceptací **účasti na alespoň základních integračních opatřeních**, a to jak v zájmu migrantů samých, tak celé společnosti. Zcela oprávněný je požadavek na zvýšenou míru znalosti českého jazyka - samozřejmě podpořený rozšířenou nabídkou výuky. Stejně tak je efektivní vyžadovat účast migrantů na výuce, která jim zprostředkuje seznámení s hodnotovým systémem a pravidly soužití v ČR i EU, stejně tak i s jejich právy a povinnostmi. Zde je třeba zvolit diferencovaný přístup podle toho, z jaké kulturní oblasti, ale zejména sociální skupiny migranti přicházejí. Faktickým završením integračního procesu je získání občanství, které implikuje získání a možnost uplatňování politických práv.

Významná role v integraci připadá **majoritní společnosti**. Pozitivní zkušenost v soužití s cizinci a nekonfliktní vztahy vedou u většinové společnosti k podpoře soužití s migranty a k odmítání a nesouhlasu s radikálními postoji některých členů majority, jejichž politické a sociální názory jsou tak následně tlumeny. Ochota či schopnost imigrantů se integrovat, ve svém důsledku zvyšuje vstřícnost majority a její ochotu podporovat soužití s migranty. Z bezpečnostního hlediska a z pohledu bezproblémového soužití majoritní společnosti a migrantů je to zejména schopnost integrace migrantů, která přímo ovlivňuje míru imigrace. Eliminace hrozby neintegrovaných imigrantů tak snižuje riziko vytváření sociálních nepokojů a radikalizace společnosti.

Hrozba neúspěšné integrace spočívá zejména na vnějších faktorech, které lze složitým způsobem ovlivnit. Motivace migrantů aktivně se podílet na integračním procesu a z druhé strany ochota majoritní společnosti tuto integraci umožnit a podpořit, jsou vzájemně provázané a neoddělitelné faktory ovlivňující výsledný bezproblémový charakter soužití.

Migrační politika musí v tomto ohledu minimalizovat riziko neúspěšné integrace již od samého počátku imigračního procesu (radikální cizinci, riziko závislosti na sociálním systému). Je snadnější předcházet problémům, než **čelit následkům neřízené migrace a nezvládnuté integrace**.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Mezinárodní kontext a legislativní rámec

Migrační politika ČR je značně ovlivněna mezinárodně-právními závazky a členstvím v EU. Zásadní vliv na migrační politiku ČR má právo EU, zejména pak Smlouva o fungování EU (SFEU), která zavedla společné politiky v oblastech migrace, mezinárodní ochrany a hranic. Společné politiky jsou prováděny prostřednictvím právních nástrojů EU ve formě konkrétních směrnic a nařízení (např. schengenský hraniční kodex, vízový kodex, dublinské nařízení, atd.), praktická spolupráce na eurounijní úrovni je prováděna mimo jiné prostřednictvím agentur EU (EASO, Frontex, Europol). V oblasti mezinárodního práva lze zmínit Úmluvu OSN o právním postavení uprchlíků.

Migrace je komplexní fenomén, který spadá podle kompetenčního zákona č. 2/1969 Sb.[46] do gesce MV. ČR disponuje v rámci migrační politiky uceleným legislativním rámcem, který pokrývá rozsáhlou problematiku migrace a který je v případě potřeby podrobován dílčím úpravám. Kromě obecných norem je jedním z nejvýznamnějších zákonů v oblasti migrace zákon č. 326/1999 Sb., o pobytu cizinců na území ČR; zákon č. 216/2002 Sb., o ochraně státních hranic; čl. 43 Listiny základních práv a svobod[47]; zákon č. 325/1999 Sb., o azylu; zákon č. 221/2003 Sb., o dočasné ochraně cizinců.

Základní dokumenty

Základním strategickým rámcem migrační politiky je **Strategie migrační politiky ČR**[48] z roku 2015, která definuje sedm prioritních oblastí – integrace; nelegální a návratová politika; azyl; vnější dimenze migrační politiky; volný pohyb osob v EU a schengenská spolupráce; legální migrace; mezinárodní a evropské závazky ČR v oblasti migrace. Aktualizovaná strategie postihuje všechny klíčové aspekty problematiky migrace a je vhodným nástrojem upravujícím migrační politiku v ČR.

Bezpečnostní aspekty migrace ovlivňují kromě soužití na území i sociální a ekonomický charakter společnosti. V této souvislosti vznikla **BS 2015**[49], která definuje jako jednu z bezpečnostních hrozeb zvýšenou míru nelegální migrace a nedostatečné integrace legálních migrantů. Závěry pracovní skupiny potvrzují platnost vymezených hrozeb bezpečnostní strategií, které jsou pracovní skupinou dále rozvedeny. Dokument **Analýza hrozeb pro ČR**[50] z roku 2015 identifikoval jako jednu ze sociogenních hrozeb „Migrační vlnu velkého rozsahu“. Můžeme konstatovat, že pro řešení zmíněného nebezpečí byl MV v roce 2014 aktualizován typový plán krizového řízení **Migrační vlna velkého rozsahu.**[51]

Z hlediska integrace ČR disponuje aktualizovanou **Koncepcí integrace cizinců** (KIC) z roku 2016[52], která reflektuje aktuální situaci a potřeby v rámci integračního procesu zahrnující integraci všech cizinců na území ČR. Dále byl v roce 2015 schválen nový **Státní integrační program** (SIP), který je zaměřen na pomoc osobám s udělenou mezinárodní ochranou při jejich začleňování do společnosti.[53]

Odpovědné instituce a orgány

Multidimenzionální charakter migrace se projevuje v počtu útvarů a organizačních složek státu, které se tímto fenoménem zabývají a které navazují meziresortní spolupráci. V této souvislosti je nutné zmínit činnost meziresortního **Koordinačního orgánu pro řízení ochrany státních hranic a migrací**[54], který byl ustaven dne 13. prosince 2006, v gesci MV. Členy Koordinačního orgánu pro řízení ochrany státních hranici a migraci jsou vedoucí pracovníci na úrovni náměstků ministrů resortů MZV; MPO; MPSV; MŠMT; MO; MMR; MF; MSp; MD a MZdr. Dále mezi další členy patří i policejní prezident; náměstek ministra pro lidská práva, rovné příležitosti a legislativu; místopředseda vlády pro vědu, výzkum a inovace a státní tajemník pro evropské záležitosti Úřadu vlády ČR.

[46] Zákon České národní rady ze dne 8. ledna 1969 o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky.
[47] Ústavní zákon č. 2/1993 Sb., ve znění pozdějších předpisů.
[48] Usnesení vlády ČR ze dne 29. července 2015 č. 621 o Strategii migrační politiky ČR a o Komunikační strategii ČR k migraci.
[49] Usnesení vlády ČR ze dne 4. února 2015 č. 79 o BS 2015.
[50] Usnesení vlády ČR ze dne 27. dubna 2016 č. 369 k Analýze hrozeb pro ČR.
[51] Původní typový plán Migrační vlna velkého rozsahu byl z roku 2010.
[52] Usnesení č. 26 ze dne 18. ledna 2016 aktualizovaná Koncepce integrace cizinců „Ve vzájemném respektu“.
[53] Usnesení č. 954 ze dne 20. listopadu 2015 „Státní integrační program pro osoby s udělenou mezinárodní ochranou v roce 2016 a v letech následujících“.
[54] Usnesení vlády ČR ze dne 18. dubna 2007 č. 394 k Národnímu plánu řízení ochrany státních hranic ČR.

V souvislosti s přijetím Strategie migrační politiky ČR a Komunikační strategie ČR k migraci dne 29. července 2015[55] a s přijetím usnesení vlády ČR ze dne 12. října 2015 č. 824 o změně předchozího usnesení[56] se **Koordinační orgán pro řízení ochrany státních hranic a migraci schází i na vládní úrovni**. Rozdělení jednotlivých kompetencí popisuje **Zpráva o situaci v oblasti migrace a integrace cizinců na území ČR**[57]. Do bezpečnostního rámce migrační politiky jsou v užší či širší míře zapojena jednotlivá ministerstva, případně jejich podřízené složky, do jejichž agendy spadají zejména následující kompetence[58]: Úřad vlády ČR (koordinace veřejné správy, lidská práva, evropské záležitosti), MV (koordinace azylové a migrační politiky a ochrana hranic, koordinace integrace, krizové řízení), MZV (rozvojová spolupráce a humanitární pomoc, vydávání krátkodobých schengenských víz, vízová a konzulární agenda), MPO (podnikání cizinců), MPSV (zaměstnávání a sociální zabezpečení cizinců, integrace cizinců na pracovním trhu), MŠMT (vzdělávání a integrace cizinců v rámci předškolního, základního, středního, vyššího odborného i vysokoškolského studia), MF (finanční zajištění, celní správa, postihy nelegálního zaměstnávání), MO (zabezpečení obrany ČR a součinnost s armádami jiných států), MSp (trestněprávní legislativa, soudní vyhošťování a extradice), MD (civilní letectví), MZdr (zajištění ochrany veřejného zdraví), MMR (regionální politika).

Z hlediska bezpečnostních aspektů hrají zásadní roli i zpravodajské služby, které na problematice participují v rámci své působnosti, stanovené právními předpisy (ust. § 5 zákona č. 153/1994 Sb., o zpravodajských službách ČR) a v souladu s každoročně stanovovanými prioritami činnosti, které schvaluje vláda.

C. SWOT analýza

Silné stránky

Systémové

- Existence Strategie migrační politiky a koordinace migrační politiky skrze Koordinační orgán pro ochranu hranic a migraci, od července 2015 na vládní úrovni.
- Stabilní a trvalý postoj ČR k migraci na národní i eurounijní úrovni.
- Významná a dlouhodobá zkušenost s migranty, pro které se ČR stává cílovou zemí (více než 50 % cizinců s povoleným pobytem na území dosáhlo trvalého pobytu).
- Existence Národního schengenského plánu a jeho pravidelného vyhodnocování s cílem zajistit plnění závazků ČR v oblasti schengenské spolupráce.
- Pravidelný monitoring a analýza migrační situace v ČR i v EU a schopnost přijímání rychlých rozhodnutí v reakci na aktuální vývoj, včetně schopnosti vyhodnotit individuální migrační rizika v průběhu vízového procesu.

[55] Usnesení vlády ČR ze dne 29. července 2015 č. 621 o Strategii migrační politiky ČR a o Komunikační strategii ČR k migraci.
[56] Usnesení vlády ČR ze dne 12. října 2015 č. 824 o změně usnesení vlády ze dne 29. července 2015 č. 621, o Strategii migrační politiky ČR a o Komunikační strategii ČR k migraci.
[57] Zpráva o situaci v oblasti migrace a integrace cizinců na území ČR je každoročně zpracovávána v souladu s usnesením vlády č. 467/1993 a usnesením Poslanecké sněmovny Parlamentu ČR č. 225 ze dne 12. října 1993 a navazujícím usnesením Poslanecké sněmovny Parlamentu ČR č. 716 ze dne 28. června 1995.
[58] Uvedený výčet kompetencí jednotlivých ministerstev a jejich podřízených složek není taxativní, kompetence jsou uvedeny s ohledem na oblast zájmu.

- Dlouhodobá a pravidelně aktualizovaná Koncepce integrace cizinců, která je postavená na schopnosti cílené integrace na lokální úrovni i zasíťováním na regionální úrovni a flexibilita používání nástrojů.
- Zavádění povinných prvků integrace (zkouška z českého jazyka, zkoušky při žádosti o občanství).
- Vysoká míra angažovanosti a cílené bezpečnostní, rozvojové a humanitární intervence v zemích původu, zemích tranzitu i cílových zemí imigrace s cílem prevence velkých migračních toků (Program MV na asistenci uprchlíkům v regionech původu a prevenci migračních pohybů v roce 2015, Program MEDEVAC).
- Existence programů humanitární a rozvojové asistence, mimořádných humanitárních programů (např. Ukrajina, Sýrie, Jordánsko), aktivní zapojení ČR do iniciativ EU - příspěvky ČR do svěřeneckých fondů EU.
- Aktivní zapojení do procesů společné zahraniční a bezpečnostní politiky EU a operací v rámci společné bezpečnostní a obranné politiky EU.
- Existence typových plánů krizového řízení – Migrační vlna velkého rozsahu a Znovuzavedení ochrany na vnitřních hranicích, včetně existence Operačních plánů Policie ČR, Armády ČR a Celní správy ČR.
- Schopnost rychlého zavedení kontrol na vnitřních hranicích v souladu se Schengenským kodexem.
- Schopnost reagovat na aktuální ekonomické požadavky zaváděním zrychlené a zjednodušené procedury pro specifické skupiny migrantů (migrační projekty).

Legislativní

- Ucelený právní rámec.
- Úzké propojení mezi legislativou, politikou a praxí.

Materiálně – technické a personální kapacity

- Vysoká úroveň expertizy a odbornosti.
- Flexibilita v rámci Policie ČR.
- Centralizované informační systémy.
- Schopnost využít dočasně kapacit některých bezpečnostních sborů k plnění úkolů Policie ČR v případě potřeby.
- Finanční zajištění systému a schopnost v případě potřeby uvolnit finanční prostředky na cílená opatření.
- Schopnost vysílat záchranářskou a materiální humanitární pomoc do zahraničí.

Slabé stránky

Systémové

- Omezená schopnost efektivního vymáhání práva (rychlost návratových operací, efektivita a rychlost rušení pobytů z bezpečnostních důvodů, zahraniční bojovníci).

- Zranitelnost správního procesu legální migrace a souvisejících oblastí (snížená schopnost efektivní identifikace migranta bez dokladů popř. s padělanými doklady) – otázka možnosti vyloučení individuálních žádostí s ohledem na bezpečnostní důvody.
- Omezená schopnost zajistit integraci cizinců pobývajících na území (vymahatelnost a monitoring povinné školní docházky…).
- Zneužívání a zneužitelnost azylového systému pro nelegální migraci do ČR/EU.
- Nízká politická podpora v rámci EU některým názorům prosazovaným ČR.
- Stírání bariéry mezi pomocí poskytovanou do zahraničí skrze Mechanismus civilní ochrany EU určenou na řešení krizové situace, tj. neodkladnou, a pomocí návaznou.
- Nejednotné a nesystematické ukládání trestu vyhoštění soudy; nedůsledné navrhování uložení trestu vyhoštění státními zástupci.

Legislativní

- Legislativně stanovená nižší míra společenské nebezpečnosti nelegální migrace a převaděčství.
- Vágní a nedostatečné mantinely v trestním zákoníku pro hodnocení možnosti uložit trest vyhoštění.
- Neefektivní správní proces řízení migrace.
- Překotný vývoj legislativy EU, která znamená nutnost pravidelných novelizací národních předpisů a vede k jejich nepřehlednosti.
- Snížená schopnost ovlivňování evropské legislativy v migrační oblasti.

Materiálně – technické a personální kapacity

- Nedostatečná schopnost státních složek rychle a efektivně reagovat na nutnost navýšení personální kapacity (nabírání nových zaměstnanců, školení) a udržení odborného personálu (finanční zajištění).
- Nedostatek jazykově vybavených odborníků, kteří by mohli působit v terénu, zejména v mimoevropských zemích.
- Nutnost kontinuální obnovy a rozvoje materiálního vybavení bezpečnostních sborů.
- Nedostatečné propojení informačních systémů veřejné správy.
- Nedostatečné komunikační prostředí pro využití moderních technologií při zajišťování vnitřního pořádku, bezpečnosti státu a prevence v oblasti národní bezpečnosti.
- Nedostatečná schopnost účinného a efektivního rozvoje kritických informačních systémů.

Příležitosti

- Mobilita pracovních sil a s ní spojený ekonomický rozvoj.
- Bezvízový režim i pro občany ČR v rámci reciprocity.
- Volný pohyb osob, zboží, služeb a kapitálu jako základních prvků existence EU.
- Příliv zahraničních investorů a tedy investic.

- Efektivní využití finančních prostředků z EU.
- Pozitivní dopady do demografické bilance.
- Dlouhodobá koncepce bezpečnostního výzkumu.
- Využití finančních prostředků ze Svěřeneckých fondů MADAD a pro Afriku nejen k zamezení migrace, ale i k posílení zapojení českých subjektů do jejich čerpání.

Hrozby

Neřízená migrace

- V důsledku konfliktů ve třetích zemích – zdroje migrace způsobené tzv. push faktory.
- V důsledku přírodních vlivů a katastrof.
- V důsledku nerovnoměrného plnění společných pravidel v rámci EU Schengenu (ochrana vnějších hranic, azylové aquis).
- V důsledku fenoménu tzv. zahraničních bojovníků.
- V důsledku organizovaného zločinu (obchodování s lidmi a výnosy z něj investované zpět do ilegálního systému, kriminální činnost zaměřená na nelegální migraci – padělané doklady, převaděčství a nelegální překročení hranice - úkryty, účelově uzavírané manželství, tzv. bílí koně, nelegální zaměstnávání apod.).
- V důsledku neregulovatelných přelivů občanů EU a sekundárních migračních toků (občané třetích zemí pobývající na území EU).
- V důsledku zrušení vízové povinnosti některým zemím.

Neúspěšná integrace

- V důsledku odmítavého postoje většinové společnosti.
- V důsledku růstu sociálního napětí.
- Projevy a posilování vlivu a aktivit extremistických skupin.
- V důsledku nedostatečné ochoty samotného migranta se integrovat z důvodu výrazných kulturních odlišností a zvyklostí rozdílných od právního pořádku ČR.
- V důsledku existence druhé a následné generace migrantů (naturalizovaní migranti) nezačleněné do společnosti a neztotožněné s hodnotovým žebříčkem ČR a EU.
- V důsledku vzniku ghett a následně vytvoření kriminogenního prostředí.

D. Doporučení k posílení odolnosti

V rámci shrnutí lze konstatovat, že ČR má v rámci možností, které jí jsou dány bezpečnostním prostředím, v němž se díky své geografické poloze a členství v EU a schengenském prostoru nachází, nastaven systém pro řízení migračních toků. Přestože je systém nastaven, je nutné díky vysoké dynamičnosti a nízké předvídatelnosti vývoje neustále systém prověřovat, odhalovat dílčí nedostatky a efektivně reagovat na nové vývojové trendy.

Návrhy opatření vyplývají ze SWOT analýzy části C materiálu:

Systémová opatření

1. Zajištění strategické komunikace, transparentního a otevřeného informování veřejnosti a všech dalších zainteresovaných subjektů.
2. Včasná identifikace a vyhodnocení hrozby neřízené migrace týkající se ČR.
3. Efektivní spolupráce bezpečnostních složek na národní i mezinárodní úrovni, se zajištěním včasného předávání informací.
4. Výměna relevantních informací s vládami partnerských zemí ohledně migrace, mezinárodní ochrany a současného bezpečnostního stavu v regionech zasažených krizí (např. v regionu Blízkého východu a severní a subsaharské Afriky).
5. Prevence radikalizace většinové společnosti a prevence radikalizace a rekrutování cizinců za využití informačních a osvětových kampaní.
6. Optimalizace nastavení a postihů trestných činů souvisejících s nelegální migrací.Spolupráce v oblasti vnějších vztahů formou posilování kapacit ve třetích zemích zasažených krizí.
7. Posílení humanitární, rozvojové a rekonstrukční asistence zdrojovým zemím migrace.
8. Příprava dlouhodobých strategií a vládních materiálů.
9. Posílení asistence tranzitním a cílovým zemím, které čelí zesíleným migračním tokům.

Legislativní opatření

1. Novela zákona č. 326/1999 Sb. o pobytu cizinců z hlediska posílení bezpečnostních prvků imigračního procesu.
2. Novela zákona č. 326/1999 Sb. o pobytu cizinců s ohledem na posílení povinných prvků integrace.
3. Novela zákona č. 325/1999 Sb. o azylu s cílem zavedení možného zrychlení azylové procedury ve specifických případech.
4. Novela zákona č. 150/2002 Sb., soudního řádu správního s cílem zrychlení správního soudnictví.
5. Novela zákona č. 234/2014 Sb. o státní službě s cílem zajištění vyšší flexibility státní správy v personálních otázkách a efektivního nastavení systému ohodnocování s cílem udržet odborný personál.
6. Úsilí o ovlivnění unijní legislativy a koordinačních procesů s cílem zefektivnit správní procesy v oblastech již regulovaných eurounijním právem, se zaměřením na důkladné zvážení následných kroků v problematice vízové liberalizace.

Materiálně – technické a personální kapacity

1. Zajištění elektronizace řízení o žádosti jako efektivního protikorupčního i bezpečnostního aspektu řízení, které zároveň zvyšuje rychlost a komfort pro klienty, a to včetně žádoucího propojení informačních systémů státní správy.
2. Podpora nastavení nadresortních principů dlouhodobého rozvoje pevné a mobilní komunikační infrastruktury a technologií veřejné správy a eGovernmentu pro využití při

zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a prevence v oblasti národní bezpečnosti.

3. Naplnění konceptu rozvoje současných kritických informačních, identifikačních a evidenčních systémů (CIS[59], VIS[60]) dále i AFIS[61] s cílem zavádět nové technologie v oblasti identifikace osob, včetně funkčního a efektivního propojení těchto národních informačních systémů s centrálními nadnárodními informačními systémy EU.
4. Provedení inventury na hraničních přechodech dle schválené Analýzy situace v oblasti infrastruktury na hraničních přechodech ČR[62].
5. Opatření v personální oblasti k zajištění dostatečně jazykově i odborně vyškolených specialistů ve všech resortech.
6. Pravidelná obnova materiálního vybavení bezpečnostních sborů a konzulárních úseků.
7. Institucionální podpora dlouhodobé koncepce bezpečnostního výzkumu.
8. Podpora rozvoje Národního centra pro kontrolu dokladů.
9. Podpora rozvoje Národního situačního centra ochrany hranic.

[59] Cizinecký informační systém.
[60] Vízový informační systém.
[61] Daktyloskopický identifikační systém (Automatic Fingerprint Identification System).
[62] Usnesení BRS ze dne 18. ledna 2016 č. 5, k Analýze situace v oblasti infrastruktury na hraničních přechodech ČR.

PŘÍRODNÍ HROZBY

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

S ohledem na trendy změny klimatu neustále roste počet mimořádných událostí či krizových situací způsobených přírodními hrozbami i závažnost jejich dopadů. Ve většině případů nelze zásadním způsobem omezit riziko jejich vzniku, ale můžeme je monitorovat, s určitým předstihem předpovídat a činit opatření k zajištění připravenosti na jejich řešení. Důležitá je také adaptace na změnu klimatu, která vzniku ztrát a škod předchází a zmírňuje tak ekonomické, sociální a další dopady změny klimatu.

Pro identifikaci a rozdělení typů nebezpečí, které se může vyskytnout na území ČR, byl zpracován dokument Analýza hrozeb pro ČR, který dne 27. dubna 2016 usnesením č. 369 schválila vláda. Touto analýzou bylo identifikováno 72 typů nebezpečí, které byly následně podrobeny multikriteriální analýze[63], zohledňující jak četnost výskytu, tak závažnost dopadu na chráněné zájmy (dopady na životy a zdraví, dopady na životní prostředí, ekonomické a sociální dopady). Posledním krokem analýzy bylo hodnocení rizik, které rizika prioritizovalo a jasně definovalo, kterým je nutné věnovat zvýšenou pozornost. V oblasti přírodních - živelních hrozeb byly zohledněny jak hrozby abiotické (způsobené neživou přírodou), tak hrozby biotické (způsobené živou přírodou).

Jako výstup pro účely Auditu budou zohledněny tyto hrozby[64]:

I) Povodeň, přívalová povodeň, vydatné srážky

II) Dlouhodobé sucho

III) Požár v přírodě

IV) Extrémně vysoké teploty

V) Extrémní vítr

VI) Epidemie - hromadné nákazy osob

VII) Epifytie - hromadné nákazy polních kultur

VIII) Epizootie - hromadné nákazy zvířat

[63] Podrobné informace o provedené analýze, včetně posuzovaných parametrů/kritérií a úrovni rizika pro jednotlivé nebezpečí (hrozby) jsou uvedeny v materiálu Analýza hrozeb pro ČR.

[64] Jedná se o všechna nebezpečí přírodního původu (identifikované analýzou hrozeb) s nepřijatelnou úrovní rizika. Dále s ohledem na předpokládaný výskyt sucha v následujících obdobích (a v souladu s Koncepcí environmentální bezpečnosti) byla zahrnuta i problematika přírodních požárů.

2. Popis jednotlivých hrozeb:

I) Povodeň, přívalová povodeň, vydatné srážky

Povodně jsou zapříčiněny přívalovými (přívalové povodně) nebo vytrvalými dešti, táním sněhu na větším území v kombinaci s nepříznivým fyzikálním stavem půdy a sníženou retenční schopností krajiny. Přívalové povodně charakterizuje velmi silná intenzita deště a jsou spojené s rychlým vzestupem hladiny vody ve vodních tocích a jejím následným rychlým poklesem.

Důsledkem jsou ztráty na životech, zdraví a majetku a životním prostředí, zejména při nerespektování přirozených limitů území. Povodně mohou vyvolat další krizové jevy, např. kontaminaci území (půda, voda) způsobenou únikem nebezpečných látek.

Míra a druh znečištění (biologické, chemické) mohou způsobit, že vodu po určité období nebude možné upravit na požadovanou kvalitu. Průvodním jevem povodní je i poškození zemědělských kultur na rozsáhlých plochách.

Vydatnými srážkami a jejich následky se rozumí výskyt intenzivních srážek v zastavěných plochách obcí, kde v jejich důsledku dochází k překročení kapacity stokové sítě, zaplavení níže ležících prostor objektů a technické infrastruktury povrchově odtékající srážkovou vodou.

Dopady na kritickou infrastrukturu se mohou vyskytovat zejména v odvětvích energetiky, vodního hospodářství, potravinářství a zemědělství a dopravy.

II) Dlouhodobé sucho

Z klimatologického hlediska je sucho normální, opakující se projev, který souvisí s fluktuací klimatu. Sucho vzniká v důsledku déletrvajícího srážkově deficitního období, které bývá ještě umocněno nadnormálním průběhem teplot a tím zvýšeným výparem. Stávajícími metodami hospodaření na zemědělské půdě, ale také zástavbou s rychlým odvodem vod došlo ke snížení infiltračních schopností krajiny a tím byla významně snížena její retenční kapacita.

Zásadním problémem při výskytu dlouhodobého sucha je nedostatek vody ve zdrojích saturujících potřeby obyvatel, kritických infrastruktur a ekosystémů a s tím související omezení jejich schopnosti zajišťovat klíčové ekosystémové služby. V konečném důsledku může nedostatek vody vést k ohrožení zdraví a životů obyvatel, snížení hospodářské produkce, spolupůsobit při vzniku a šíření požárů vegetace a způsobovat poškození lesních porostů a porostů zemědělských kultur.

III) Požár v přírodě

Požáry v přírodním prostředí, tj. především lesní požáry a požáry travních porostů, ploch zemědělských kultur a rašelinišť představují zejména v souvislosti s dlouhodobým suchem aktuální problém. Vyšší pravděpodobnost požárů přírodního prostředí nastává při nižší vlhkosti organické hmoty (travní porost, lesní porost, hrabanka apod.), dlouhotrvajícím suchu, nižší vlhkosti prostředí (vzduchu, půdy), vyšší teplotě vzduchu a vyšší délce a intenzitě slunečního svitu.

Kromě ohrožení majetku, zdraví a života občanů mají požáry přírodního prostředí značně devastující vliv na životní prostředí. Mezi velmi závažné patří požáry hraničních lesů s přesahem přes hranice ČR a požáry zvláště cenných biotopů s ohrožením jejich ekologické stability či přímo bezprostřední existence. V případě požárů ve zvláště chráněných územích a územích soustavy Natura 2000 je potom problémem případná újma a riziko jejich poškození při hasebním zásahu. Rozsáhlé požáry také mohou způsobit významnou kontaminaci ovzduší a vod.

IV) Extrémně vysoké teploty

Extrémně vysoké teploty (vlny veder) ohrožují zdraví a životy obyvatel, ale také funkčnost kritické infrastruktury, zejména v odvětvích jako je energetika, doprava, vodní hospodářství, potravinářství a zemědělství. Mezi následky extrémně vysokých teplot patří především ohrožení zdraví a životů obyvatel. Dalšími dopady jsou poškození lesních porostů, zemědělských kultur a zvýšené riziko vzniku požárů. Vysoké teploty ovlivňují výpar vody z krajiny a mohou být jednou z příčin vzniku sucha. V oblasti kritické infrastruktury je vysokými teplotami ohrožena zejména energetika, a to nejen kvůli zvýšení spotřeby energie na klimatizaci, ale také kvůli omezené možnosti chlazení (např. pro odvod odpadního tepla, snížení hladiny vody k chlazení). Tepelným namáháním mohou být ohroženy i dopravní konstrukce, např. železnice.

V) Extrémní vítr

Nebezpečné rychlosti větru se v ČR vyskytují v zimní polovině roku při postupu hlubokých tlakových níží k východu, v letní polovině roku pak při intenzivní bouřkové činnosti. Extrémní vítr se závažnými následky zpravidla postihuje pouze určitou část území. Následky silného větru spočívají především ve vlivu na dopravu, komunikace a sídla a na lesní porosty, které může komplexně poškodit nebo zničit. Dopady na kritickou infrastrukturu se projevují zejména v odvětví energetiky (ohrožena je energetická rozvodná síť) a dopravy.

VI) Epidemie - hromadné nákazy osob

Epidemií se rozumí výskyt infekčního onemocnění, který výrazně převyšuje obvykle očekávané hodnoty incidence v daném čase a místě. V ČR je možný výskyt epidemií buď u infekcí, které se běžně v ČR vyskytují anebo se může jednat o zcela nový typ infekčního onemocnění (případně onemocnění, které bylo vymýceno). Incidence infekčních onemocnění (tj. míra frekvence nových onemocnění v populaci specifikovaná místně a časově) je ovlivněna zejména vnímavostí populace k infekci, virulencí původce, toxicitou, efektivitou stanovených protiepidemických opatření a možnostmi kauzální léčby.

U epidemií velkého rozsahu nelze jednoznačně stanovit dopady na kritickou infrastrukturu, neboť se budou odvíjet od možnosti přenosu infekční nemoci, virulentnosti, možnostech léčby, dostupnosti očkovacích látek atd. (zvýšená nemocnost a s ní související absence v zaměstnání může mít dopady průřezově na všechna odvětví kritické infrastruktury).

VII) Epifytie - hromadné nákazy polních kultur

Epifytie je označení pro hromadné nákazy zemědělských plodin a lesních kultur. Jsou závislé na vývoji klimatických podmínek v období vegetace. Doba trvání je závislá na rychlosti provedení rostlinolékařských opatření, či případné likvidaci kultur.

VIII) Epizootie – hromadné nákazy zvířat

Epizootie je nakažlivé onemocnění zvířat postihující velké skupiny zvířat (velký počet) na velkém území (kraje, celý stát) v určitém časovém období. Charakteristickými rysy epizootie je rychlý nástup, rychlé šíření a vysoká nemocnost. Extrémní formou epizootie je panzootie, kdy infekční nemoc zasáhne celé kontinenty. Formou epizootie nebo panzootie probíhají vysoce virulentní (nakažlivá) onemocnění virového původu. V Evropě se nejčastěji vyskytuje slintavka a kulhavka, mor prasat nebo

vysoce patogenní forma ptačí chřipky H5N1. Tato onemocnění se velmi rychle šíří a při nedodržení veterinárních opatření se často během několika dní mohou rozšířit do více států.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Základní dokumenty

Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 – materiál v širším pohledu stanoví další postup rozvoje významných oblastí ochrany obyvatelstva, jako je výchova a vzdělávání, síly, věcné zdroje, úkoly ochrany obyvatelstva, krizové řízení, věda a výzkum. Dále obsahuje základní úkoly pro realizaci stanovených priorit ochrany obyvatelstva na celé období její platnosti, včetně výhledu do roku 2030.

Koncepce environmentální bezpečnosti, a to na období 2016-2020 s výhledem do roku 2030 - cílem tohoto dokumentu je omezit vznik krizové situace vyvolané interakcí životního prostředí a společnosti, snížit dopady již nastalých krizových situací a zvýšit environmentální bezpečnost, přičemž dosažení těchto cílů je postaveno na premise dopracování systému konkrétních legislativních, technických, institucionálních a informačních opatření. Koncepce zahrnuje návrhy rozšíření stávajících opatření, jež povedou ke zvýšení environmentální bezpečnosti, a to z hlediska jak zdrojů rizik antropogenního původu (chemické látky, zdroje ionizujícího záření a biologická agens), tak i nebezpečí přírodního původu (extrémní meteorologické jevy, povodně, dlouhodobé sucho, svahové nestability a další).**Strategie přizpůsobení se změně klimatu v podmínkách ČR** představuje národní adaptační strategii ČR, která kromě zhodnocení pravděpodobných dopadů změny klimatu obsahuje návrhy konkrétních adaptačních opatření, legislativní a částečnou ekonomickou analýzu.

Legislativa

Základními právními předpisy, které se vztahují na všechny typy přírodních hrozeb, jsou:

- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů,
- zákon č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon),
- zákon č. 241/2000 Sb., zákon o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů,

Legislativa a základní plánovací dokumenty vztahující se k jednotlivým hrozbám:

I) Povodeň, přívalová povodeň, vydatné srážky

- zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon)
- Směrnice Evropského parlamentu a Rady 2000/60/ES ze dne 23. října 2000, kterou se stanoví rámec pro činnost Společenství v oblasti vodní politiky
- Směrnice Evropského parlamentu a Rady 2007/60/ES ze dne 23. října 2007 o vyhodnocování a zvládání povodňových rizik

Související dokumenty: plány pro zvládání povodňových rizik, plány dílčích povodí, povodňové plány obcí, ORP, krajů, Povodňový plán ČR, havarijní plán kraje, krizový plán kraje a ORP

II) Dlouhodobé sucho

- zákon č. 254/2001 Sb., zákon o vodách (vodní zákon, ve znění pozdějších předpisů)
- **Stávající legislativa není v oblasti ochrany před suchem dostatečná**. V rámci meziresortní pracovní skupiny VODA-SUCHO jsou připravovány také návrhy na úpravu jednotlivých právních předpisů s předpokládaným termínem do konce roku 2018.

Související dokumenty: havarijní plán kraje*,* krizový plán kraje a ORP

III) Požár v přírodě

- zákon č. 133/1985 Sb., o požární ochraně
- vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)
- vyhláška č. 247/2001 Sb., o organizaci a činnosti jednotek požární ochrany
- nařízení jednotlivých krajů, kterými se stanoví podmínky k zabezpečení požární ochrany v době zvýšeného nebezpečí vzniku požáru či zabezpečení zdrojů vody k hašení požárů
- plány péče o zvláště chráněná území (zpracovávané dle § 38 zákona č. 114/1992 Sb., o ochraně přírody a krajiny, ve znění pozdějších předpisů

Související dokumenty: dokumentace požární ochrany, havarijní plán kraje

IV) Extrémně vysoké teploty

- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů
- zákon č. 133/1985 Sb., o požární ochraně

Související dokumenty: dokumentace požární ochrany, havarijní plán kraje

V) Extrémní vítr

Pro tuto hrozbu nejsou specifické předpisy, důvodem je relativně nízký výskyt tohoto jevu na našem území, avšak v souvislosti se změnou klimatu se zvyšuje pravděpodobnost výskytu. V souvislosti s tím je nutno zajistit pro danou oblast právní zakotvení a současně je nezbytné modifikovat právní úpravu varovné, hlásné a předpovědní služby a SIVS tak, aby právní stav odpovídal aktuálním potřebám a byla zajištěna činnost a další rozvoj meteorologické služby v ČR.

Související dokumenty: havarijní plán kraje, krizový plán kraje a ORP

VI) Epidemie - hromadné nákazy osob

- Mezinárodní zdravotnické předpisy (2005)
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů
- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě

- zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech)
- Rozhodnutí Evropského parlamentu a Rady o vážných přeshraničních zdravotních hrozbách (1082/2013)
- vyhláška č. 252/2004 Sb., kterou se stanoví hygienické požadavky na pitnou a teplou vodu četnost a rozsah kontroly pitné vody
- vyhláška č. 537/2006 Sb., o očkování proti infekčním nemocem
- vyhláška č. 306/2012 Sb., o podmínkách předcházení vzniku a šíření infekčních onemocnění a o hygienických požadavcích na provoz zdravotnických zařízení a ústavů sociální péče
- vyhláška č. 137/2004 Sb., o hygienických požadavcích na stravovací služby a o zásadách osobní a provozní hygieny při činnostech epidemiologicky závažných
- vyhláška č. 473/2008 Sb., o systému epidemiologické bdělosti pro vybrané infekce

Související dokumenty: pandemické plány, traumatologické plány, havarijní plán kraje, krizový plán kraje a ORP

VII) Epifytie - hromadné nákazy polních kultur

- zákon č. 326/2004 Sb., o rostlinolékařské péči a změně některých souvisejících zákonů
- vyhláška č. 215/2008 Sb., o opatřeních proti zavlékání a rozšiřování škodlivých organismů rostlin a rostlinných produktů

Související dokumenty: havarijní plán kraje, krizový plán kraje a ORP

VIII) Epizootie - hromadné nákazy zvířat

- zákon č. 166/1999 Sb. o veterinární péči a o změně některých souvisejících zákonů (veterinární zákon)
- vyhláška č. 290/2003 Sb., o veterinárních přípravcích a veterinárních technických prostředcích
- vyhláška č. 299/2003 Sb., o opatřeních pro předcházení a zdolávání nákaz a nemocí přenosných ze zvířat na člověka
- vyhláška č. 372/2003 Sb., o veterinárních kontrolách při obchodování se zvířaty

Související dokumenty: pohotovostní plány SVS ČR určené pro jednotlivé druhy nákaz, koncepce sanace ohnisek hromadných úhynů zvířat, havarijní plán kraje, krizový plán kraje a ORP

Odpovědné instituce a orgány dle jednotlivých posuzovaných hrozeb:

I) Povodeň, přívalová povodeň, vydatné srážky

- působnost ochrany před povodněmi a výkon dozoru – MŽP,
- ochrana obyvatelstva – MV,
- činnost podniků Povodí včetně podílu na budování protipovodňových opatření – MZe,
- kontrolní činnost -povodňové orgány,

- předpovědní povodňová služba – ČHMÚ
- podíl na řešení následků extrémních meteorologických jevů – MD, MPO, MZdr, MZe a SSHR

II) Dlouhodobé sucho

- ochrana přírody, ochrana vod – MŽP,
- vodovody a kanalizace, zdroje vody, podniky povodí – MZe,
- ochrana obyvatelstva – MV,
- regulace průmyslové výroby – MPO,
- lodní doprava – MD,
- SIVS – ČHMÚ ve spolupráci s Odborem hydrometeorologického zabezpečení Vojenského geografického a hydrometeorologického úřadu Armády ČR
- podíl na řešení následků extrémních meteorologických jevů – MD, MPO, MZdr, MZe a SSHR

III) Požár v přírodě

- požární prevence a ochrana života a zdraví občanů a majetku před požáry – HZS ČR,
- SIVS – ČHMÚ ve spolupráci s Odborem hydrometeorologického zabezpečení Vojenského geografického a hydrometeorologického úřadu Armády ČR

IV)Extrémně vysoké teploty

- SIVS – ČHMÚ ve spolupráci s Odborem hydrometeorologického zabezpečení Vojenského geografického a hydrometeorologického úřadu Armády ČR,
- podíl na řešení následků extrémních meteorologických jevů - MD, MPO, MZdr, MZe a SSHR

V) Extrémní vítr

- SIVS – ČHMÚ ve spolupráci s Odborem hydrometeorologického zabezpečení Vojenského geografického a hydrometeorologického úřadu Armády ČR,
- podíl na řešení následků extrémních meteorologických jevů - MD, MPO, MZdr, MZe a SSHR

VI) Epidemie - hromadné nákazy osob

- státní správa – MZdr, orgány ochrany veřejného zdraví, spolupráce správní úřady, poskytovatelé zdravotních služeb

VII) Epifytie - hromadné nákazy polních kultur

- státní správa – MZe, Ústřední kontrolní a zkušební ústav zemědělský

VIII) Epizootie - hromadné nákazy zvířat

- státní správa – MZe, Státní veterinární správa a krajské veterinární správy

Síly a prostředky pro zvládání přírodních hrozeb

Pro zvládání mimořádných událostí a krizových situací jsou stěžejní **složky integrovaného záchranného systému**. Základní složky IZS (HZS ČR a JPO zařazené do plošného pokrytí kraje JPO, poskytovatelé ZZS, Policie ČR) zajišťují nepřetržitou pohotovost pro příjem ohlášení vzniku mimořádné události, její vyhodnocení a neodkladný zásah na místě. Za tímto účelem rozmísťují své síly a prostředky po celém území ČR. Ostatní složky IZS poskytují plánovanou pomoc na vyžádání; jsou jimi vyčleněné síly a prostředky ozbrojených sil, ozbrojené bezpečnostní sbory, ostatní záchranné sbory (např. Báňská záchranná služba), orgány ochrany veřejného zdraví (hygienická služba), havarijní, pohotovostní, odborné a jiné odborné služby, zařízení civilní ochrany, neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím.

V případě krizových situací či rozsáhlých mimořádných událostí, kdy nedostačují standardní zdroje pro jejich zvládání, se využívá **systému hospodářských opatření pro krizové stavy** (zejména systému nouzového hospodářství, použití státních hmotných rezerv a regulačních opatření). Cílem nouzového hospodářství je zajistit za krizového stavu nezbytné dodávky pro uspokojení základních životních potřeb obyvatelstva, pro podporu výkonu státní správy a pro podporu činnosti záchranných sborů, havarijních služeb, zdravotnické záchranné služby a Policie ČR. Pro jejich zajištění jsou na úrovni obcí s rozšířenou působností, krajských úřadů a ústředních správních úřadů zpracovávané plány nezbytných dodávek. Regulační opatření slouží za krizového stavu ke snížení spotřeby nedostatkových surovin a výrobků a dodávek služeb nebo k usměrnění spotřeby a dodávek v souladu s krizovými plány v případech, kdy krizová situace nabývá takového rozsahu, že běžné ekonomické nástroje nejsou při zajišťování nezbytných dodávek účinné.

Neopomenutelný je podíl právnických a podnikajících fyzických osob, které jsou povinny pro řešení mimořádných událostí či krizových situací poskytovat věcnou či osobní pomoc, mohou zajišťovat plnění opatření vyplývajících z krizového plánu a podílet se na zpracování plánovací dokumentace.

Posouzení stávajících právních předpisů a kapacit ke zvládání hrozby

Obecně lze říci, že systém pro zajištění připravenosti i samotné řešení mimořádných událostí a krizových situací, vyvolaných přírodními hrozbami zohledněnými v této kapitole, je funkční a v praxi prověřený. Příslušná legislativa se dostatečně zabývá identifikovanými hrozbami, vyjma problematiky sucha, které v minulosti nebyla věnována pozornost[65] (legislativa neposkytuje dostatečnou oporu pro přijímání účinných opatření na zmírnění dopadů dlouhodobého sucha, s výjimkou omezení užívání pitné vody z veřejných vodovodů a náhradního zásobování a zajištění přídělů pitné vody) a problematiky meteorologických služeb.

[65] Až v Koncepci environmentální bezpečnosti 2012-2015 s výhledem do roku 2020 je dlouhodobé sucho označeno jako priorita k řešení, a v roce 2014 vznikla meziresortní pracovní komise VODA-SUCHO, výsledkem jejíž činnosti je materiál „Příprava realizace opatření pro zmírnění negativních dopadů sucha a nedostatku vody“ (schválený usnesením vlády č. 620 z roku 2015). Cílem je připravit návrh pro realizaci aktivit a adaptačních opatření vedoucích k zabezpečení hlavních cílů uvažovaných plánů pro zvládání sucha a vytvoření informačního základu pro návrh souhrnné koncepce řešení problematiky negativních dopadů výskytu sucha a nedostatku vody. Plány pro zvládání sucha by se měly v blízké budoucnosti stát nedílnou součástí novely vodního zákona.

Dalším nedostatkem v legislativní oblasti je nevyhovující právní úprava zajištění varovné, hlásné a předpovědní služby, dále SIVS a činností ČHMÚ.

Jako hrozba do budoucnosti se jeví omezení financování Letecké hasičské služby, která byla významným nástrojem pro identifikaci a zdolávání požárů (pozornost je věnována pouze problematice hašení požárů nikoliv hlídkové činnosti).

Pro zajištění připravenosti na řešení mimořádných událostí a krizových situací je zpracovávána řada plánovací dokumentace (viz jednotlivé hrozby). Jejich potřebnost byla v rámci konkrétních mimořádných událostí prakticky ověřena.

Na ústřední úrovni a především na úrovni územních samosprávných celků se projevuje nedostatek pracovníků zabývajících se problematikou krizového řízení (pracovníci ÚSC často vykonávají tuto činnost jen na část úvazku).

Personální kapacity IZS pro zvládání přírodních hrozeb jsou uspokojivé, avšak problém představuje zejména personální nestabilita (snižování tabulkových míst a propouštění následované opětovným nabíráním nových sil způsobuje odchod zkušených pracovníků a narušuje stabilitu systému).

Materiální kapacity složek IZS jsou v současnosti na dobré úrovni, avšak je nezbytné zajistit jejich pravidelnou obměnu a modernizaci, tak aby bylo možné efektivně zvládat narůstající počet mimořádných událostí.

Při řešení mimořádných událostí se osvědčila spolupráce s nestátními neziskovými organizacemi, je však nezbytné nastavit efektivní systém jejich zapojení (i jednotlivých dobrovolníků).

Velkou předností je stávající systém hospodářských opatření pro krizové stavy (zejména systém nouzového hospodářství, použití státních hmotných rezerv a regulačních opatření), jehož využitelnost a funkčnost byla ověřena při mnoha mimořádných událostech a krizových situacích. V souladu s novou právní úpravou je možné bezplatně použít státní hmotné rezervy i pro řešení vybraných mimořádných událostí a pro odstraňování následků krizových situací. Problémem zůstává opakovaná disproporce mezi schváleným Plánem nezbytných dodávek a přidělenými finančními prostředky v rozpočtové kapitole SSHR k jeho realizaci.

Jako naprosto nezbytné se v dnešní době jeví nasazení moderních technologií, které nacházejí uplatnění v oblasti řešení mimořádných událostí a krizových situací. S tím souvisí i nutnost zajištění komunikačního prostředí, které je těmito technologiemi využíváno.

C. SWOT analýza

Pro každou hrozbu byly zpracovány dílčí SWOT analýzy, z nichž byly vybrány a v celkové SWOT analýze dále rozpracovány faktory, které se průřezově uplatňují v oblasti zvládání přírodních-živelních hrozeb:

Silné stránky

- Funkční a ověřený systém.
- Existující legislativa, metodické pokyny, doporučení.
- Odborné znalosti a schopnosti.
- Mezinárodní spolupráce.
- Plošné pokrytí.
- Věcné zdroje vytvořené v systému hospodářských opatření pro krizové stavy.

Slabé stránky

- Nedostatečné finanční prostředky.
- Nedostatek lidských zdrojů na ústřední úrovni a úrovni územních samosprávných celků.
- Personální nestabilita u výkonných složek.
- Nedostatečná podpora rozvoje systému.
- Zdlouhavý proces schvalování strategických materiálů.

Příležitosti

- Povinné vzdělávání obyvatelstva.
- Bezpečnostní výzkum.
- Sdílení zkušeností na mezinárodní úrovni.
- Technologický rozvoj.
- Širší zapojení nestátních neziskových organizací a dobrovolníků.

Hrozby

- Změny klimatu.
- Personální restrikce.
- Finanční restrikce.
- Nepřipravenost občanů k sebeochraně.
- Věnování přílišné pozornosti „aktuálním“ bezpečnostním tématům a zanedbávání ostatních témat.

D. Doporučení pro posílení odolnosti

1. Připravit úpravu systému ochrany obyvatelstva, tak aby odpovídal současným bezpečnostním trendům[66].
2. Zajistit personální stabilitu složek IZS.
3. Posílit personální kapacity (pracovníků v oblasti krizového řízení) na ústřední úrovni i úrovni územně samosprávných celků, tak by se tito pracovníci mohli dostatečně věnovat problematice krizového řízení (nejen na část úvazku).
4. Zajistit dostatečnou výši finančních prostředků na přípravu a řešení mimořádných událostí a krizových situací.
5. Formou povinného vzdělávání obyvatelstva zvýšit spoluodpovědnost občanů za své bezpečí.
6. Zakotvit problematiku sucha do právních předpisů.
7. Přizpůsobit právní úpravu zajištění varovné, hlásné a předpovědní služby a SIVS činností ČHMÚ současným potřebám.

[66] V souladu s aktuální koncepcí ochrany obyvatelstva.

8. Zabývat se problematikou PR, prezentování událostí v médiích, komunikací s veřejností.
9. Věnovat zvýšenou pozornost bezpečnostnímu výzkumu včetně systému sdílení informací mezi aktéry a uživateli výsledků.
10. Nastavit efektivní systém koordinace a spolupráce s nestátními neziskovými organizacemi v rámci ochrany obyvatelstva.
11. Podporovat dlouhodobý rozvoj komunikační infrastruktury a technologií pro využití při přípravě na mimořádné události a krizové situace a jejich řešení.
12. Zvyšovat odolnost implementací Strategie přizpůsobení změně klimatu v podmínkách ČR.

ANTROPOGENNÍ HROZBY

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Počet mimořádných událostí či krizových situací a závažnost jejich dopadů neustále roste. Vhodně nastavenými preventivními opatřeními lze mnoha antropogenním hrozbám předcházet, pro ostatní případy je nezbytný dobře nastavený systém opatření k zajištění připravenost na řešení a samotné řešení mimořádných událostí a krizových situací vzniklých v souvislosti s lidskou činností.

Pro identifikaci a rozdělení typů nebezpečí, které se může vyskytnout na území ČR, byl zpracován dokument Analýza hrozeb pro ČR, který dne 27. dubna 2016 usnesením č. 369 schválila vláda. Touto analýzou bylo identifikováno 72 typů nebezpečí, které byly následně podrobeny multikriteriální analýze[67], zohledňující jak četnost výskytu, tak závažnost dopadu na chráněné zájmy (dopady na životy a zdraví, dopady na životní prostředí, ekonomické a sociální dopady). Posledním krokem analýzy bylo hodnocení rizik, které rizika prioritizovalo a jasně definovalo, kterým je nutné věnovat zvýšenou pozornost.

Jako výstup pro účely Auditu budou zohledněny následující hrozby, pro které byla identifikována nepřijatelná úroveň rizika, a které zároveň nejsou rozpracovány v jiných kapitolách Auditu:

I) Zvláštní povodeň

II) Únik nebezpečné chemické látky ze stacionárního zařízení

III) Radiační havárie

IV) Narušení dodávek pitné vody velkého rozsahu

V) Narušení dodávek potravin velkého rozsahu

2. Popis jednotlivých hrozeb:

I) Zvláštní povodeň

Zvláštní povodeň je způsobená poruchou či havárií vodního díla vzdouvajícího nebo akumulujícího vodu, nebo nouzovým řešením kritické situace na vodním díle (úmyslné poškození, terorismus) vyvolávající vznik mimořádné události pod vodním dílem. Pro účely dohledu jsou vodní díla zařazena do I. až IV. kategorie podle výše možných škod v území pod vodním dílem při případné havárii. Vlastníci (uživatelé) nebo správci vodních děl jsou povinni zajišťovat na nich odborný technickobezpečnostní dohled, zvláště na vodních dílech I. – III. kategorie, jehož účelem je průběžné

[67] Podrobné informace o provedené analýze, včetně posuzovaných parametrů/kritérií a úrovni rizika pro jednotlivé nebezpečí (hrozby) jsou uvedeny v materiálu Analýze hrozeb pro ČR.

zjišťování technického stavu vodního díla z hlediska jeho stability, bezpečnosti a možných poruch i navrhování vhodných opatření k nápravě.

Zvláštní povodeň může mít dopady jak na samotné obyvatelstvo žijící pod vodním dílem, tak na veškeré objekty nacházející se v území ohroženém vodním dílem. Analýza možností vzniku a průběhu zvláštních povodní, stanovení jejich účinků v profilu vodního díla a stanovení směrodatných limitů pro stupně povodňové aktivity při nebezpečí vzniku zvláštní povodně je stanovena v Plánech ochrany území pod vodním dílem před zvláštní povodní.

II) Únik nebezpečné chemické látky ze stacionárního zařízení

Nebezpečné chemické látky jsou v současné době vyráběny a dováženy pro široké užití. Při všech činnostech spojených s nakládáním s nebezpečnými látkami vzniká riziko jak ohrožení zdraví člověka, tak životního prostředí. Bezpečnostní riziko je spojené se vznikem závažných havárií způsobených technickou závadou nebo selháním lidského faktoru, ať již neúmyslného nebo úmyslného, s cílem vyvolat závažné škody na zdraví člověka, na životním prostředí, na majetku nebo na fungování společnosti.

Podmínkou pro efektivní ochranu společnosti před důsledky závažných havárií je stanovení jednotných pravidel pro všechny činnosti spojené s nakládáním s nebezpečnými látkami.

Oblast prevence závažných havárií způsobených nebezpečnými chemickými látkami a směsmi je založena na přístupu stupňování povinností v závislosti na zvyšující se míře rizika a implementaci nástrojů kontroly a prosazování práva v této oblasti. Při dosažení kritických množství vybraných látek a bezpečného nakládání s nimi musí odpovědný subjekt plnit přísnější, náročnější a také finančně nákladnější povinnosti.

III) Radiační havárie

Požadavky na bezpečné nakládání se zdroji ionizujícího záření, s jadernými materiály, na jadernou bezpečnost a havarijní připravenost jsou stanoveny atomovým zákonem a jeho prováděcími předpisy.

Atomový zákon a mezinárodní úmluvy stanovují, mimo jiné, podmínky vykonávání činností, které souvisejí s využíváním jaderné energie a ionizujícího záření. Dále také stanoví pravidla radiační ochrany osob a životního prostředí. V červenci 2016 byl schválen nový atomový zákon č. 263/2016 Sb., který nabyde účinnosti dnem 1. 1. 2017. Nový atomový zákon oblast havarijní připravenosti (nově „zvládání radiačních mimořádných událostí“) řeší mnohem explicitněji než stávající právní předpisy. Mimo jiné je požadováno zpracování Národního programu monitorování (do 2 let od nabytí účinnosti nového atomového zákona) a Národního radiačního havarijního plánu (do 4 let od nabytí účinnosti nového atomového zákona).

Výkon státní správy a dozoru v oblasti jaderné bezpečnosti, radiační ochrany, havarijní připravenosti, respektive zvládání radiačních mimořádných událostí a monitorování radiační situace, je v působnosti SÚJB, který vydává příslušná povolení, schvaluje dokumentaci a provádí pravidelné kontroly na pracovištích se zdroji ionizujícího záření. Nový atomový zákon řeší nově také oblast monitorování radiační situace na území ČR, které kromě SÚJB zajišťují ministerstva, jiné správní orgány stanovené tímto zákonem a držitelé povolení stanovení zákonem. Řízením tohoto monitorování je pověřen SÚJB. Získaná data slouží pro hodnocení radiační situace, pro potřeby sledování a posuzování a stavu ozáření a v případě radiační havárie pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření.

IV) Narušení dodávek pitné vody velkého rozsahu

Narušení dodávek pitné vody může mít vliv nejen na obyvatelstvo, ale i na činnost řady subjektů, které např. pitnou vodu využívají k výrobě potravin, v zemědělství (živočišná výroba) či ve zdravotnických zařízeních. K narušení dodávek pitné vody může dojít zejména v důsledku jiných mimořádných událostí či krizových situací. Pokud je příčinou přerušení dodávky pitné vody běžná porucha vodovodní sítě, řeší tuto situaci vlastník či provozovatel vodovodů a kanalizací náhradním zásobováním. V případech narušení dodávek pitné vody velkého rozsahu, je nezbytné realizovat opatření nouzového zásobování pitnou vodou, která jsou stanovena v příslušných havarijních či krizových plánech. Tato situace se může dotýkat i ohrožení úmyslného narušení systému zásobování vodou.

V) Narušení dodávek potravin velkého rozsahu

Vzhledem k množství výrobců, distributorů a skladů není vznik samostatné krizové situace narušení dodávek potravin velkého rozsahu příliš pravděpodobný, může však vzniknout sekundárně, jako důsledek jiné události.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Základní dokumenty:

Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 – materiál v širším pohledu stanoví další postup rozvoje významných oblastí ochrany obyvatelstva, jako je výchova a vzdělávání, síly, věcné zdroje, úkoly ochrany obyvatelstva, krizové řízení, věda a výzkum. Dále obsahuje základní úkoly pro realizaci stanovených priorit ochrany obyvatelstva na celé období její platnosti, včetně výhledu do roku 2030.

Koncepce environmentální bezpečnosti, a to na období 2015-2020 s výhledem do roku 2030 -

cílem tohoto dokumentu je navrhnout rozšíření existujících opatření, která povedou k omezení rizik vzniku krizových situací, vyvolaných interakcí životního prostředí a společnosti (zejména závažné havárie, živelní pohromy a teroristické činy).

Legislativa:

Základní právní předpisy, vztahující se na všechny typy antropogenních hrozeb;

- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů;
- zákon č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů (krizový zákon);
- zákon č. 241/2000 Sb., zákon o hospodářských opatřeních pro krizové stavy a o změně souvisejících zákonů.

Legislativa a základní plánovací dokumenty vztahující se k jednotlivým hrozbám:

I) Zvláštní povodeň

- zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon);
- směrnice Evropského parlamentu a Rady 2000/60/ES ze dne 23. října 2000, kterou se stanoví rámec pro činnost Společenství v oblasti vodní politiky;
- směrnice Evropského parlamentu a Rady 2007/60/ES ze dne 23. října 2007 o vyhodnocování a zvládání povodňových rizik;
- vyhláška MZe č. 471/2001 Sb., o technickobezpečnostním dohledu nad vodními díly;
- vyhláška MŽP č. 236/2002 Sb. o způsobu a rozsahu zpracování návrhu a stanovování záplavových území;
- vyhláška MZe č. 24/2011 Sb. o plánech povodí a plánech pro zvládání povodňových rizik.

Související dokumenty - plán ochrany území pod vodním dílem před zvláštní povodní, plán pro zvládání povodňových rizik v povodí, havarijní plán kraje, krizový plán kraje a ORP

II) Únik nebezpečné chemické látky ze stacionárního zařízení

- zákon č. 224/2015 Sb., o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů (zákon o prevenci závažných havárií);
- vyhláška č. 226/2015 Sb., o zásadách pro vymezení zóny havarijního plánování a postupu při jejím vymezení a o náležitostech obsahu vnějšího havarijního plánu a jeho struktuře;
- vyhláška č. 228/2015 Sb., o rozsahu zpracování informace veřejnosti, hlášení o vzniku závažné havárie a konečné zprávy o vzniku a dopadech závažné havárie.

Související dokumenty - bezpečnostní program, bezpečnostní zpráva, vnitřní havarijní plán, vnější havarijní plán, havarijní plán kraje, krizový plán kraje a ORP

III) Radiační havárie

právní předpisy platné do 31. 12. 2016

- zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů;
- nařízení vlády č. 11/1999 Sb., o zóně havarijního plánování;
- vyhláška č. 146/1997 Sb., stanovující činnosti, které mají bezprostřední vliv na jadernou bezpečnost, a činnosti zvláště důležité z hlediska radiační ochrany, požadavky na kvalifikaci a odbornou přípravu, způsob ověřování zvláštní odborné způsobilosti a udělování oprávnění vybraným pracovníkům a způsob provedení schvalované dokumentace pro povolení k přípravě vybraných pracovníků;
- vyhláška č. 106/1998 Sb., o zajištění jaderné bezpečnosti a radiační ochrany jaderných zařízení při jejich uvádění do provozu a při jejich provozu;
- vyhláška č. 195/1999 Sb., o požadavcích na jaderná zařízení k zajištění jaderné bezpečnosti, radiační ochrany a havarijní připravenosti;
- vyhláška č. 307/2002 Sb., o radiační ochraně;

- vyhláška č. 318/2002 Sb., o podrobnostech k zajištění havarijní připravenosti jaderných zařízení a pracovišť se zdroji ionizujícího záření a o požadavcích na obsah vnitřního havarijního plánu a havarijního řádu;
- vyhláška č. 319/2002 Sb., o funkci a organizaci celostátní radiační monitorovací sítě.

právní předpisy platné od 1. 1. 2017

- zákon č. 263/2016 Sb., atomový zákon a jeho prováděcí vyhlášky (o podrobnostech k zajištění zvládání radiačních mimořádných událostí, o monitorování radiační situace, o radiační ochraně a zabezpečení radionuklidového zdroje)

Související dokumenty - vnitřní havarijní plán, vnější havarijní plán, havarijní plán kraje, krizový plán kraje a ORP.

IV) Narušení dodávek pitné vody velkého rozsahu

- zákon č. 274/2001 Sb., o vodovodech a kanalizacích pro veřejnou potřebu a o změně některých zákonů (zákon o vodovodech a kanalizacích), ve znění pozdějších předpisů;
- zákon č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon), ve znění pozdějších předpisů;
- plán rozvoje vodovodů a kanalizací na území ČR (PRVKÚ ČR);
- plán rozvoje vodovodů a kanalizací na území kraje (PRVKÚK);
- metodický pokyn MZe k zajištění jednotného postupu orgánů krajů, hlavního města Prahy, orgánů obcí a městských částí v hlavním městě Praze k zajištění nouzového zásobování obyvatelstva pitnou vodou při mimořádných událostech a za krizových stavů Službou nouzového zásobování vodou.

Související dokumenty- havarijní plán kraje, krizový plán kraje a ORP

V) Narušení dodávek potravin velkého rozsahu

- zákon č. 110/1997 Sb., o potravinách a tabákových výrobcích a o změně a doplnění některých souvisejících zákonů.

Související dokumenty - havarijní plán kraje, krizový plán kraje a ORP

Odpovědné instituce a orgány dle jednotlivých posuzovaných hrozeb:

I) Zvláštní povodeň

- státní správa - MZe ve spolupráci s MV, MŽP
- technickobezpečnostní dohled

II) Únik nebezpečné chemické látky ze stacionárního zařízení

- oblast chemických látek a směsí a prevence závažných havárií – MŽP
- vliv nebezpečných chemických látek na zdraví člověka – MZdr
- vliv nebezpečných chemických látek na oblast zemědělství – MZe
- oblast havarijního plánování – MV

III) Radiační havárie

- oblast jaderné bezpečností, radiační ochrany, havarijní připravenosti – SÚJB
- monitorování radiační situace na území ČR – RMS (SÚJB, MF, MO, MV, MZe a MŽP)
- oblast havarijního plánování - MV, SÚJB

IV) Narušení dodávek pitné vody velkého rozsahu

oblast vodního hospodářství – MZe

V) Narušení dodávek potravin velkého rozsahu

- státní správa – MZe

Síly a prostředky pro zvládání antropogenních hrozeb

Pro zvládání mimořádných událostí a krizových situací jsou stěžejní **složky integrovaného záchranného systému** (IZS). Základní složky IZS (HZS ČR a JPO zařazené do plošného pokrytí kraje JPO, poskytovatelé ZZS, Policie ČR) zajišťují nepřetržitou pohotovost pro příjem ohlášení vzniku mimořádné události, její vyhodnocení a neodkladný zásah na místě. Za tímto účelem rozmísťují své síly a prostředky po celém území ČR. Ostatní složky IZS poskytují plánovanou pomoc na vyžádání; jsou jimi vyčleněné síly a prostředky ozbrojených sil, ozbrojené bezpečnostní sbory, ostatní záchranné sbory (např. Báňská záchranná služba), orgány ochrany veřejného zdraví (hygienická služba), havarijní, pohotovostní, odborné a jiné odborné služby, zařízení civilní ochrany, neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím.

V oblasti antropogenních hrozeb je třeba také zmínit existenci Radiační monitorovací sítě. Data získávaná RMS slouží pro hodnocení radiační situace, pro potřeby sledování a posuzování stavu ozáření a pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření v případě radiační havárie.

V případě krizových situací či rozsáhlých mimořádných událostí, kdy nedostačují standardní zdroje pro jejich zvládání, se využívá **systému hospodářských opatření pro krizové stavy** (zejména systému nouzového hospodářství, použití státních hmotných rezerv a regulačních opatření). Cílem nouzového hospodářství je zajistit za krizového stavu nezbytné dodávky pro uspokojení základních životních potřeb obyvatelstva, pro podporu výkonu státní správy a pro podporu činnosti záchranných sborů, havarijních služeb, zdravotnické záchranné služby a Policie ČR. Pro jejich zajištění jsou na úrovni obcí s rozšířenou působností, krajských úřadů a ústředních správních úřadů zpracovávané Plány nezbytných dodávek. Regulační opatření slouží za krizového stavu ke snížení spotřeby nedostatkových surovin a výrobků a dodávek služeb nebo k usměrnění spotřeby a dodávek v souladu s krizovými plány v případech, kdy krizová situace nabývá takového rozsahu, že běžné ekonomické nástroje nejsou při zajišťování nezbytných dodávek účinné.

Právnické a podnikající fyzické osoby se samozřejmě také podílí na zvládání antropogenních hrozeb, jedná se zejména o ty subjekty, které pro své okolí mohou představovat ohrožení. Avšak všechny právnické a podnikající fyzické osoby jsou povinny pro řešení mimořádných událostí či krizových situací poskytovat věcnou či osobní pomoc, mohou zajišťovat plnění opatření vyplývajících z krizového plánu a podílet se na zpracování plánovací dokumentace.

V oblasti zvládání antropogenních hrozeb za zmínku stojí i Transportní informační a nehodový systém (TRINS), který poskytuje prostřednictvím svých středisek nepřetržitou pomoc při řešení mimořádných událostí spojených s přepravou či skladováním nebezpečných látek.

Posouzení stávajících právních předpisů a kapacit ke zvládání hrozby

Obecně lze říci, že systém pro zajištění připravenosti i samotné řešení mimořádných událostí a krizových situací, vyvolaných antropogenními hrozbami zohledněnými v této kapitole, je funkční a v praxi prověřený. Příslušná legislativa se dostatečně věnuje všem identifikovaným hrozbám (v roce 2015 byl novelizován zákon o prevenci závažných havárií a od 1. 1. 2017 nabývá účinnosti nový atomový zákon č. 263/2016 Sb.

Pro zajištění připravenosti na řešení mimořádných událostí a krizových situací je zpracovávána řada plánovací dokumentace (viz jednotlivé hrozby), které byly v rámci konkrétních mimořádných událostí prakticky ověřeny.

Na ústřední úrovni a především úrovni územních samosprávných celků se projevuje nedostatek pracovníků zabývajících se problematikou krizového řízení (pracovníci ÚSC často vykonávají tuto činnost jen na část úvazku).

Personální kapacity IZS pro zvládání antropogenních hrozeb jsou uspokojivé, avšak problém přestavuje zejména personální nestabilita (snižování tabulkových míst a propouštění následované opětovným nabíráním nových sil způsobuje odchod zkušených pracovníků a narušuje stabilitu systému).

Materiální kapacity složek IZS jsou v současnosti na dobré úrovni, avšak je nezbytné zajistit jejich pravidelnou obměnu a modernizaci, tak aby bylo možné efektivně zvládat narůstající počet mimořádných událostí.

Velkou předností je stávající systém hospodářských opatření pro krizové stavy (zejména systém nouzového hospodářství, použití státních hmotných rezerv a regulačních opatření), jehož využitelnost a funkčnost byla ověřena při mnoha mimořádných událostech a krizových situacích. V souladu s novou právní úpravou je možné bezplatně použít státní hmotné rezervy i pro řešení vybraných mimořádných událostí a pro odstraňování následků krizových situací. Problémem zůstává opakovaná disproporce mezi schváleným Plánem nezbytných dodávek a přidělenými finančními prostředky v rozpočtové kapitole SSHR k jeho realizaci.

Naopak je nedostatečné zapojení právnických a podnikajících fyzických osob (zejména těch, které představují pro své okolí zvýšené riziko) do přípravy na mimořádné události a krizové situace a jejich řešení.

Naprosto nezbytné se v dnešní době jeví nasazení moderních technologií, které nacházejí uplatnění v oblasti řešení mimořádných událostí a krizových situací. S tím souvisí i nutnost zajištění komunikačního prostředí, které je těmito technologiemi využíváno.

C. SWOT analýza

Pro každou hrozbu byly zpracovány dílčí SWOT analýzy, z nichž byly vybrány a v celkové SWOT analýze dále rozpracovány faktory, které se průřezově uplatňují v oblasti zvládání antropogenních hrozeb:

Silné stránky

- Funkční a ověřený systém.
- Existující legislativa, metodické pokyny, doporučení na národní a evropské úrovni.
- Existující plánovací dokumentace.

- Odborné znalosti a schopnosti.
- Věcné zdroje vytvořené v systému HOPKS.

Slabé stránky

- Nedostatečné finanční prostředky.
- Personální nestabilita a nedostatečné personální kapacity na ústřední úrovni a úrovni územních samosprávných celků.
- Zdlouhavé administrativní a právní postupy při realizaci některých preventivních opatření (např. budování poldrů).
- Nedostatečná vazba na územní plánování a stavební řízení.
- Roztříštěnost gescí v oblasti CBRN.

Příležitosti

- Povinné vzdělávání obyvatelstva.
- Bezpečnostní výzkum.
- Technologický rozvoj.
- Sdílení zkušeností a závěrů z konkrétních událostí v zahraničí.

Hrozby

- Personální restrikce.
- Finanční restrikce.
- Nedostatečné zapojení vybraných právnických a podnikajících fyzických osob.
- Vznik velkých aglomerací zahrnujících průmyslové zóny s nebezpečnými objekty.
- Možnost teroristických útoků.

D. Závěrečná doporučení

1. Zajistit aktualizaci systému ochrany obyvatelstva z pohledu antropogenních hrozeb[68].
2. Zajistit personální stabilitu složek IZS.
3. Posílit personální kapacity (pracovníků v oblasti krizového řízení) na ústřední úrovni i na úrovni územních samosprávných celků, tak, aby se tito pracovníci mohli dostatečně věnovat problematice krizového řízení (nejen na část úvazku).
4. Zajistit dostatečnou výši finančních prostředků na přípravu a řešení mimořádných událostí a krizových situací.

[68] V souladu s aktuální koncepcí ochrany obyvatelstva.

5. Zvýšit odpovědnost vybraných právnických a podnikajících fyzických osob provozující objekty, které mohou představovat zvýšené riziko pro své okolí (např. provozovatelé zařízení kategorie IV. podle atomového zákona, provozovatelé zařazení do skupiny B podle zákona o prevenci závažných havárií a provozovatelé vodních děl I. kategorie podle vodního zákona) a zajistit jejich širší zapojení do přípravy na mimořádné události a krizové situace a jejich řešení cestou užší spolupráce s odpovědnými orgány veřejné správy a zvýšeným podílem na realizaci konkrétních úkolů.
6. Formou povinného vzdělávání obyvatelstva zvýšit spoluodpovědnost občanů za své bezpečí.
7. Věnovat zvýšenou pozornost bezpečnostnímu výzkumu včetně systému sdílení informací mezi aktéry a uživateli výsledků.
8. Zajistit provázanost potřeb ochrany obyvatelstva s procesy územního plánování a stavebního řízení.
9. Podporovat dlouhodobý rozvoj komunikační infrastruktury a technologií pro využití při přípravě na mimořádné události a krizové situace a jejich řešení.

HROZBY V KYBERPROSTORU

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Před hrozbami v kyberprostoru není v dnešní době plně chráněn žádný stát, ČR nevyjímaje. Zhoršující se bezpečnostní situace nejen v oblastech bezprostředně sousedících s členskými státy NATO a EU pak umocňuje zvyšující se nároky na schopnost ČR samostatně reagovat na bezpečnostní hrozby v kyberprostoru. Můžeme pozorovat rostoucí snahy státních i nestátních aktérů v budování a používání kybernetických ofenzivních prostředků, které cílí zejména na kritickou infrastrukturu (KI), respektive její část vystavenou v kyberprostoru – kritickou informační infrastrukturu (KII)[69] a významné informační systémy (VIS)[70]. Právě ty totiž představují v ČR klíčový systém prvků, jejichž narušení nebo nefunkčnost by měla závažný dopad na bezpečnost ČR, zabezpečení základních životních potřeb obyvatelstva nebo ekonomickou situaci.

Následující text rozděluje kapitolu Hrozby v kyberprostoru do celkem pěti konkrétních hrozeb, které významně ohrožují národní bezpečnost[71]:

I) Kybernetická špionáž

II) Narušení nebo snížení odolnosti IT infrastruktury

III) Nepřátelské kampaně

IV) Narušení nebo snížení bezpečnosti eGovernmentu

V) Kyberterorismus

Za kybernetickou špionáží či nepřátelskými kampaněmi v kyberprostoru stojí stále častěji přímo cizí státy, potažmo jejich bezpečnostní struktury. Dále nabývá na významu působení kriminálních, teroristických či jiných extremistických skupin a jednotlivců v kyberprostoru, které mohou v dohledné době eskalovat až k prvním případům kyberterorismu, majícího dopady na životy a zdraví osob.

ČR proto musí kontinuálně usilovat o navyšování odolnosti IT infrastruktury za účelem minimalizace dopadů kybernetických útoků a uvedení této infrastruktury rychle zpět do funkčního stavu. Zároveň musí ČR prosazovat důsledné dodržování bezpečnostních standardů u informačních a komunikačních systémů (IS; KS) provozovaných orgány veřejné správy a správci KII a VIS a v rámci této snahy se pak zaměřit i na projekt elektronizace veřejné správy – eGovernment. Závažné narušení jeho bezpečnosti by totiž mohlo zastavit digitalizaci veřejné správy, vést k nedůvěře občanů v tento koncept a tím dokonce narušit či zpomalit fungování státu.

[69] KII se rozumí prvek nebo systém prvků kritické infrastruktury (podle § 2 písm. g) a písm. i) zákona č. 240/2000 Sb.) v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (§ 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů).

[70] VIS se rozumí informační systém spravovaný orgánem veřejné moci, který není KII a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

[71] Těchto pět hrozeb bylo určeno zadáním Auditu.

Výše zmíněné hrozby ohrožující národní bezpečnost umocňuje především fenomén kybernetické kriminality. Stále ve větší míře je pachateli využíváno anonymity a prostorové neuchopitelnosti kyberprostoru, což přináší rychlý účinek při výrazně sníženém riziku postihu.

Návaznost na jiné kapitoly Auditu: tato kapitola se v částech o kybernetické špionáži a nepřátelských kampaních prolíná s kapitolou „Hybridní hrozby" a „Působení cizí moci". Dále se prolíná s kapitolou „Energetická, surovinová a průmyslová bezpečnost" a obsahuje také hrozbu kyberterorismu, která doplňuje kapitolu „Terorismus".

Při hodnocení relevance hrozby pro ČR v tomto materiálu byla použita kritéria pravděpodobnosti a závažnosti dopadu, jejichž kombinací je relevance následně hodnocena na škále nízká-střední-vysoká[72].

2. Třídění hrozeb

Text je rozdělen do několika částí. Kvůli komplikovanosti a vysoké heterogenitě faktorů a proměnných u jednotlivých hrozeb, je v části A. každá hrozba nejprve popsána v obecné rovině a následně je uveden výčet nejvýznamnějších rizik a problémů spjatých s touto hrozbou. Popis hrozby i jednotlivá rizika a problémy vycházejí z expertního zhodnocení a konsensu na úrovni pracovní skupiny[73]. Dále v části B. následuje výčet (nikoliv vyčerpávající) odpovědných institucí a základních nástrojů pro eliminaci hrozeb v kyberprostoru. V části C. jsou do SWOT analýzy souhrnně integrovány v bodové struktuře zásadní silné stránky, slabé stránky, příležitosti a hrozby. Závěrem jsou uvedeny v části D. zásadní doporučení ke zvýšení národní bezpečnosti a odolnosti proti hrozbám v kyberprostoru.

I) Kybernetická špionáž

Zhodnocení relevance hrozby pro ČR: **Vysoká**

Kybernetická špionáž, jakožto snaha o získání strategicky citlivých či důležitých informací a dat osobní, citlivé nebo utajované povahy, a to bez souhlasu jejich držitele, je jedním z projevů nepřátelského chování. Útočníci cílí na jednotlivce, skupiny či organizace působící jak v soukromém, tak i veřejném sektoru. Zájmem útočníků je získání osobní, ekonomické, politické či vojenské výhody za použití kyberprostoru, respektive internetu, sociálních sítí a informačních a komunikačních technologií (ICT) obecně. Za případy kybernetické špionáže stojí jak jednotlivci, tak i skupiny a celé organizace. V jistých případech útoky přímo organizují, podporují, využívají či minimálně tolerují

[72] Při hodnocení závažnosti dopadu byly brány v úvahu především životní, strategické a další významné zájmy ČR, tak jak je definuje BS 2015. V případě hrozeb v kyberprostoru se jedná zejména o: zajištění suverenity, územní celistvosti a politické nezávislosti ČR, zachování všech náležitostí demokratického právního státu včetně záruky a ochrany základních lidských práv a svobod obyvatel. Dále zajištění vnitřní bezpečnosti a ochrany obyvatelstva, zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky skrze zabezpečený kyberprostor, a především zajištění kybernetické bezpečnosti a obrany ČR, spolu s prevencí a potlačováním bezpečnostních hrozeb z kyberprostoru ovlivňujících bezpečnost ČR a jejích spojenců. V případě kritéria pravděpodobnosti byly posuzovány zkušenosti ze zahraničí, i analýza a dosavadní poznatky z praxe působení národních aktérů v kyberprostoru, spolu se zkušenostmi s četností a způsoby provádění kybernetických útoků, jejich příčin a motivů. V úvahu byl brán i faktor zranitelnosti některých cílů a snadnost provedení případného útoku na tyto cíle. Pracovní skupina se shodla na faktu, že tyto faktory nelze přesně matematicky kvantifikovat, takže výsledné hodnocení je výsledkem expertního zhodnocení a konsensu na úrovni pracovní skupiny.

[73] Určitým limitem textu se jeví překryv či částečná duplicita některých rizik a problémů mezi hrozbami, což je dáno komplexností problematiky kybernetické bezpečnosti, kdy jednotlivé problémy a rizika zákonitě ovlivňují hned několik zkoumaných hrozeb.

někteří státní aktéři. Hranice mezi útočníky, kteří se zabývají kybernetickou kriminalitou a kybernetickou špionáží, je mnohdy velmi nejasná a často se jedná o stejné subjekty.

Fenomén kybernetické špionáže je spojen s „advanced persistent threat“ (APT), tedy pokročilou přetrvávající hrozbou, která je oproti tradičním kybernetickým útokům mnohem sofistikovanější a důmyslnější. APT využívá takových technik útoku a takových zranitelností, které jsou pro běžně používané detekční metody a nástroje obtížně rozpoznatelné. Tyto aktivity tak bývají po dlouhou dobu neodhaleny a v konkrétních případech je velmi složité dohledat a identifikovat jejich reálného původce. K exfiltraci informací a dat proto může kontinuálně docházet i po dobu několika let, respektive do té doby, dokud nedojde k odhalení a eliminaci této hrozby.

Význam hrozby kybernetické špionáže se odráží na počtu případů i nárůstu rizika užití kybernetických nástrojů k útokům na veřejný i soukromý sektor. Za růstem tohoto trendu stojí snadnější dostupnost sofistikovaných nástrojů pro provádění kybernetické špionáže, profesionalizace útočníků, budování ofenzivních kapacit u státních a nestátních aktérů na poli kybernetické bezpečnosti, elektronizace mnoha činností ve společnosti i celková politická situace ve světě.

Kybernetická špionáž může být jedním z prvotních znaků přípravy na kybernetický či kinetický útok, konflikt nebo také součást nepřátelské kampaně, kdy dochází mimo shromažďování strategických a citlivých informací také k mapování důležité infrastruktury, na kterou může být později útočeno. Reakce na kybernetickou špionáž si vyžaduje nasazení zvláštních prostředků a postupů, aby došlo k minimalizaci vzniklých a dalších potenciálních škod. Řešení těchto typů incidentů vyžaduje součinnost napříč rezorty zabývajícími se kybernetickou bezpečností i podporu a spolupráci jednotlivých subjektů.

ČR a její instituce se opakovaně stávají cílem kybernetické špionáže a lze předpokládat, že v českém prostředí působí doposud nedetekované APT, které škodí národním zájmům. Vzhledem k četnosti kybernetické špionáže a jejím potenciálně závažným důsledkům pro národní bezpečnost pak lze tuto hrozbu hodnotit jako vysokou. Oběťmi se zpravidla stávají exponované státní úřady a jejich představitelé, ale také instituce zabývající se vzděláváním, výzkumem a vývojem, provozovatelé IS a KS KII, správci VIS, bezpečnostní složky a řada dalších organizací. Obdobně se kybernetická špionáž týká soukromého sektoru, kde slouží především jako prostředek konkurenčního boje a dochází při ní k závažným krádežím duševního vlastnictví a k průmyslové špionáži.

Jednotlivá rizika a problémy:

- V mnoha organizacích dochází k nedostatečné alokaci finančních prostředků na problematiku kybernetické bezpečnosti a k podceňování kybernetických hrozeb.
- Někteří ICT výrobci či distributoři mající vazby na vlády a bezpečnostní složky jiných států se podílejí přímo i nepřímo na kybernetické špionáži.
- Dochází k outsourcingu řešení kybernetické bezpečnosti v mnoha organizacích, který rozšiřuje okruh potenciálních nositelů hrozeb.
- V mnoha organizacích je kybernetická bezpečnost řešena pouze z provozní úrovně, nikoliv komplexně, systémově.
- S nástupem internetu věcí se nedostatečně řeší kybernetická bezpečnost netradičních zařízení, nyní nově připojených ke kyberprostoru.
- Mnoho organizací nemá vytvořené nebo vhodně nastavené a reálně aplikovatelné politiky kybernetické bezpečnosti.
- Skrze nedostatečně prověřené zaměstnance nebo odborně znalé pracovníky, působící vědomě či nevědomě ve prospěch třetích stran, může docházet k infiltraci organizací a vystavení citlivých informací riziku zneužití.

- Mnoho organizací se dostatečně nevěnuje edukaci a osvětě zaměstnanců v oblasti kybernetické bezpečnosti, respektive lze identifikovat nedostatečnou IT gramotnost relevantních pracovníků.
- Nákup ICT probíhá přes nedostatečně prověřené prostředníky a bez znalosti produktového řetězce, které mohou obsahovat zadní vrátka (software i hardware) pro exfiltraci informací.
- Citlivé informace jsou vystaveny riziku neoprávněného užití v důsledku používání soukromých prostředků (především PC, mobilní zařízení, email) pro pracovní účely či při nevhodném a neuváženém zacházení s pracovními prostředky (především datové nosiče a mobilní zařízení).

II) Narušení nebo snížení odolnosti IT infrastruktury

Zhodnocení relevance hrozby pro ČR: **Vysoká**

V prostředí neustále se měnících kybernetických hrozeb, které mohou z dynamicky se vyvíjejícího kyberprostoru přicházet, musí ČR vytvářet zabezpečený a důvěryhodný kyberprostor a odolnou IT infrastrukturu. Stát proto musí soustavně budovat a navyšovat národní kapacity v této oblasti, avšak bez kooperace se soukromým sektorem a akademickou sférou, dále bez intenzivní mezinárodní spolupráce a zejména bez zapojení samotných obyvatel, nemůže být zajištěna potřebná účinnost těchto aktivit.

Odolnost IT infrastruktury znamená schopnost entity udržet přijatelnou úroveň služeb, rychle se adaptovat a reagovat bez ohledu na to, jaké problémy a komplikace vznikají. Vzhledem k množství eventualit a faktorů, které mohou způsobit narušení IT infrastruktury (technické selhání, selhání lidského faktoru při obsluze, přírodní katastrofy, kybernetické útoky a další), je pak podstatné vytvářet i efektivní systém zotavení IT infrastruktury po havárii či útoku.

Vzhledem ke vzrůstající četnosti a sofistikovanosti kybernetických útoků je zapotřebí neustále navyšovat své kapacity směrem ke komplexnímu řešení kybernetické bezpečnosti a kontinuálně navyšovat odolnost české IT infrastruktury, především pak u KII a VIS. Kvůli množství eventualit a faktorů, které mohou způsobit narušení nejen kritické části IT infrastruktury v ČR, a kvůli vzrůstající robustnosti a komplexnosti celkové IT infrastruktury v ČR je nutné hodnotit hrozbu narušení odolnosti IT infrastruktury jako vysokou. Je tak zapotřebí neustále navyšovat jak organizační, tak i procesní a technické schopnosti a kapacity, a tudíž posilovat celkovou odolnost IT infrastruktury v ČR.

Jednotlivá rizika a problémy:

- Riziko napadení KII a VIS kybernetickými útoky prostřednictvím kybernetické špionáže, kyberterorismu, kriminálními organizacemi, hacktivisty a dalšími.
- Nedostatek finančních prostředků na zajištění potřebných technických kurzů a najmutí bezpečnostně prověřených odborníků na ICT a kybernetickou bezpečnost.
- Chemický průmysl a jiná strategická odvětví nejsou zahrnuta do kritické infrastruktury a jejich vybrané IS a KS tak nemohou být zahrnuty do KII. U zdravotnických zařízení není v příslušném nařízení vlády obsaženo odvětvové kritérium, které by umožnilo pokrytí některých IS a KS ve zdravotnických zařízeních.
- Zaměstnanci státní a veřejné správy nemají dostatečné povědomí o kybernetické bezpečnosti, chybí jim edukace a nedodržují základy digitální hygieny.
- Nesystematicky prováděná bezpečnostní testování.

- Útoky na IT infrastrukturu prostřednictvím výrobního, dodavatelského a subdodavatelského řetězce. Z hlediska akvizičního procesu omezené možnosti zadání zakázky IT a bezpečnostních řešení prověřeným dodavatelům a subdodavatelům či nemožnost odmítnutí podezřelých dodavatelů a subdodavatelů.
- Špatná prioritizace některých rezortů a institucí při plánování investic do bezpečnostních technologií a ostatních ICT.
- Nedostatečná legislativní úprava kybernetické kriminality, respektive problém při odhalování pachatelů a následné dokazování spojené s nedostatečnými legislativními prostředky k zajištění, zadokumentování a důkaznímu využití elektronických důkazů.
- Zdravotnická zařízení, chemický průmysl a jiná strategická odvětví nejsou zahrnuta do kritické infrastruktury a jejich vybrané IS a KS tak nemohou být zahrnuty do KII.
- V mnoha případech bývají udržovány zastaralé systémy, přičemž náklady spojené s provozem a údržbou mnohdy převyšují investice do nových, lépe zabezpečených technologií.
- Dochází k outsourcingu řešení kybernetické bezpečnosti, respektive zabezpečení a celkové údržby ICT, ve kterém převažuje model „locked in“ bez „exit“ plánu a souvisejícího náhradního plánu, s čímž souvisí i problém neznalosti správců a operátorů úrovně zabezpečení.
- Roztříštěné systémy komunikačních prostředků ve státní správě nedovolující adekvátní efektivní „in-time“ údržbu, zabezpečení a kontrolu.
- Neexistence centrálních metodik pro používání prostředků výpočetní techniky, zejména mobilních zařízení, které v současné době představují stále se zvyšující riziko.
- Absence povinnosti zabezpečené (komerčně šifrované) emailové a jiné elektronické komunikace mezi státními institucemi a pracovníky státní správy.
- Současná právní úprava (zákon č. 234/2014 Sb., o státní službě) ztěžuje některým institucím přijímání kvalitních odborníků do IT.

III) Nepřátelské kampaně

Zhodnocení relevance hrozby pro ČR: **Vysoká**

Kybernetická nepřátelská kampaň představuje řadu různých, souvisejících kybernetických operací zaměřených na jeden konkrétní strategický cíl nebo výsledek. Jedná se o období, kdy dochází k sérii plánovaných a koordinovaných (kybernetických) útoků nebo dalších operací v kyberprostoru. Kampaně mohou provádět jednotlivci, nebo může jít o společné úsilí více aktérů (většinou státních či státem podporovaných či organizovaných). Definovat a ohraničit nepřátelskou kampaň v kyberprostoru je možno podle jejího účelu, tj. dosažení určitého předem stanoveného cíle v kyberprostoru, podle jejích vymezených zdrojů (technologie, aktéři, lokalita) nebo jejího průběhu v čase. V reálných podmínkách často dochází k „recyklaci“ kampaní či jejich částí, protože vývoj stále nových nástrojů a postupů pro útoky a další působení v kyberprostoru je relativně velmi nákladný a časově náročný proces.

Kyberprostor a ICT hrají v rámci nepřátelských kampaní významnou roli. Již nyní můžeme pozorovat systematické působení cizí moci, respektive nepřátelských kampaní v kyberprostoru na území ČR. Prostředky a způsob boje proti nim nejsou v současné době dostatečně účinné. Tuto hrozbu lze kvůli reálným rizikům a potenciálním dopadům hodnotit jako vysokou.

Jednotlivá rizika a problémy:

- Vlivové a dezinformační mediální kampaně na internetu mohou mít velký vliv na formování nálad obyvatelstva, což představuje vysoké riziko vyvolání společenského neklidu.
- Vlivové a dezinformační mediální kampaně prováděné prostřednictvím internetu a organizované zájmovými skupinami, zločineckými strukturami, případně zpravodajskými službami jiných států. K šíření takových informací jsou v současné době využívány jak v ČR dlouhodobě působící zpravodajské servery, tak i servery nové.
- Využíváno je hojně prostředí sociálních sítí kvůli aspektu jejich mezinárodnosti a odlišného přístupu ke svobodě slova. Z tohoto důvodu je možné je ještě ve vyšší míře využívat k šíření nenávistných či dezinformačních kampaní, jak vůči určitým skupinám obyvatel, tak i státním orgánům, anebo samotnému zahraničněpolitickému směřování ČR za účelem dosažení vojenských, politických nebo ekonomických cílů.
- Mezi problematické faktory patří struktura vlastnictví jednotlivých českých internetových médií, jež mohou ve svých zprávách sledovat rozličné soukromé zájmy, případně zájmy jiných států.
- Uvedených možností kyberprostoru využívá organizovaný zločin k podrývání důvěryhodnosti bezpečnostních složek.
- Nedostatečně prověření zaměstnanci nebo odborně znalí zaměstnanci pracující (byť nevědomě) ve prospěch třetích stran, kteří mají přístup ke strategickým aktivům, mohou exfiltrací citlivých a jinak důležitých informací a dat vážně ohrožovat národní bezpečnost.
- Současná právní úprava o svobodném přístupu k informacím (č. 106/1999 Sb.) může ohrozit kybernetickou bezpečnost ČR, respektive je zneužitelná v rámci nepřátelských kampaní. Konkrétně lze na jejím základě žádat o informace o subjektech KII či informace o komunikaci mezi NBÚ a příslušnými subjekty, ve které se řeší i aspekty mající dopad na bezpečnost předmětných systémů.

IV) Narušení nebo snížení bezpečnosti eGovernmentu

Zhodnocení relevance hrozby pro ČR: **Střední**

Myšlenkou eGovernmentu je správa věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa občanům dostupnější, efektivnější, rychlejší a levnější. Stěžejním projektem českého eGovernmentu je síť kontaktních míst veřejné správy Czech POINT, která jsou dnes téměř v každé obci. Díky nim mohou občané na jednom místě získat řadu dokumentů a využít služby několika různých úřadů. Byl také spuštěn systém datových schránek – nástroj pro zaručenou elektronickou komunikaci se státem. V neposlední řadě vznikl i systém základních registrů, v nichž jsou uloženy aktuálně platné údaje, které už ve většině případů nemusí úředníci opakovaně žádat od občanů.

Využívání eGovernmentu nabývá na významu. Pro fungování takto složitých a náročných systémů je však nutné vytvořit robustní a především bezpečnou infrastrukturu. Pokračující digitalizace veřejné správy v ČR slouží k zlepšení fungování veřejné správy a jejího vztahu k veřejnosti. Avšak služby a aplikace poskytované občanům a soukromým podnikům prostřednictvím eGovernmentu s sebou nesou značná kybernetická bezpečnostní rizika. Jednotlivé systémy eGovernmentu pracují s

obrovským objemem spravovaných a zpracovávaných důležitých dat[74]. Bezpečnost eGovernmentu může být ohrožena nejen neadekvátním zacházením s informacemi a daty, ale také vnější hrozbou, tedy kybernetickými útoky. Rozsáhlejší narušení kybernetické bezpečnosti jednotlivých projektů eGovernmentu, respektive jejich dat a informací, by mohlo vést k nedůvěře občanů v celý koncept eGovernmentu a zastavení využívání jeho služeb veřejností. Selhání systémů eGovernmentu by tedy bylo kritické.

I přes atraktivnost tohoto cíle a možné závažné důsledky selhání některého ze systémů eGovernmentu či narušení jeho dat a informací, většina kybernetických útoků spjatá s tímto konceptem není závažného charakteru a v nejbližší době nelze s jistotou predikovat změnu. Hrozbu tedy lze zejména pro možné závažné důsledky selhání systémů eGovernmentu hodnotit jako střední.

Jednotlivá rizika a problémy:

- Nedostatečné financování kybernetické bezpečnosti, nedostatečné finanční ohodnocení pracovníků a personální kapacity v oblasti kybernetické bezpečnosti a podceňování kybernetických hrozeb ve státní správě.
- Nedostatečné zabezpečení IS a KS státní správy sloužících pro komunikaci občanů se státem. Jedná se zejména o systémy, které zajišťují výkon státní správy vůči občanům státu a EU.
- Špatně nastavené politiky kybernetické bezpečnosti a nedostatečná edukace zaměstnanců ve státní správě ohledně kybernetické bezpečnosti.
- Slabé povědomí a edukace obyvatelstva o kybernetické bezpečnosti a projektu eGovernmentu jako takovém.

V) Kyberterorismus

Zhodnocení relevance hrozby pro ČR: **Střední**

NBÚ / Národní centrum kybernetické bezpečnosti definuje kyberterorismus takto: *„Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.“*[75]

V užším pojetí lze za kyberterorismus považovat pouze takové teroristické aktivity v kyberprostoru, které způsobí rozsáhlé narušení počítačových sítí či zařízení se závažnými až fatálními dopady. Při těchto útocích může docházet ke ztrátám na životech či v případě kompromitace finančního systému k velmi závažným ekonomickým ztrátám s těžko předvídatelnými důsledky. Stát se však v kyberprostoru musí bránit i před dalšími teroristickými aktivitami jakými jsou např. podněcování k nenávisti či tvorba a šíření propagandy. Významnou roli zde hrají tzv. nová média.

Kyberterorismus již nelze považovat za hypotetický fenomén a lze predikovat, že v blízké budoucnosti ke kyberteroristickým útokům bude docházet. V současnosti však nemalou část kybernetických útoků a incidentů, často mediálně prezentovaných a popisovaných jako kyberterorismus, lze označit spíše za využívání kyberprostoru, respektive internetu, teroristy.

[74] CZECH Point, datové schránky, EiDAS, SIS, VIS, ISZR, STC, eSbírka a eLegislativa.
[75] Vzhledem k absenci definice kyberterorismu v českém prostředí vytvořil NBÚ pro potřeby Auditu zcela novou definici.

Teroristické organizace prozatím nejspíše nedisponují dostatečnými kapacitami a schopnostmi k uskutečnění kybernetických útoků se závažnými až fatálními dopady. Na druhou stranu není obtížné tyto kapacity nakoupit jako službu, což lze podložit zvýšenou aktivitou a zájmem o tuto formu terorismu především z pozice tzv. Islámského státu. Tato organizace v poslední době dokázala provést takové kybernetické útoky (avšak nikterak sofistikované), které ostatní teroristické organizace nedokázaly dlouhou dobu vůbec uskutečnit.

Co se týče ČR, hrozbu kyberterorismu lze hodnotit jako střední, nikoliv nízkou. ČR je stejně jako u terorismu plynoucího z islámského fundamentalismu a radikalismu v odlišném postavení, než země západní Evropy či Spojené státy americké. Na druhou stranu je v ČR využíváno prostředí tzv. darknetu k ilegálním činnostem mířeným na vrcholné představitele státu či zneužíváno odcizených obsahů e-mailové komunikace k dehonestaci některých představitelů a následnému pokusu o ovlivnění veřejného mínění. Rovněž byly zjištěny zčásti úspěšné pokusy o znepřístupnění webových stránek nebo služeb, případně sociálních profilů politických subjektů nebo sdělovacích prostředků. Takové situace se v budoucnu budou s největší pravděpodobností opakovat či dokonce stupňovat z hlediska závažnosti.

Jednotlivá rizika a problémy:

- Možnost koordinovaného kybernetického útoku:
    - za účelem vydírání státních orgánů, obchodních korporací, či vystrašení společnosti;
    - na složky IZS a komunikační sítě operátorů;
    - za účelem zničení konkrétní technologie/systému (obvykle ve spojitosti s KII a ICS či SCADA[76] systémy);
    - na distributory energií či služeb za účelem vyřazení služby (typicky energetický blackout) a další.
- Kybernetické útoky se snahou získat citlivé informace zpravodajského charakteru za účelem jejich využití při kinetickém teroristickém útoku, např. jako informace pro výběr cílů nebo přípravu pro napadení subjektu nebo přímou podporu k jeho dezorientaci či likvidaci, která může být v přímé součinnosti s chystanými vojenskými nebo teroristickými kinetickými akcemi.
- Teroristé hojně využívají kyberprostor a ICT k šíření propagandy, materiálů k podpoře radikalizace stoupenců a jejich náboru. Jako strategické informační platformy využívají především různé sociální sítě a komunikační platformy (včetně takových, které jsou zabezpečené šifrováním).
- Teroristé skrze kyberprostor řídí samotné sympatizanty, a to zejména svoláváním proti možným cílům, plánováním operací, poskytováním zpětné vazby a poučením z provedených akcí či připisováním zásluh na provedených operacích.
- Teroristé zveřejňují soukromé údaje (získané online vyhledáváním či odcizením) zájmových osob (pro teroristické a extremistické organizace) na internetu a podněcují proti nim nenávist tak, aby se mohly stát cílem útoku nejen pro tzv. vlky samotáře.
- Nízká připravenost příslušníků bezpečnostních složek na specifické digitální prostředí a působení v něm. Existuje nedostatek ICT expertů v bezpečnostních složkách a v mnoha případech i jazyková bariéra.

[76] ICS – průmyslové řídící systémy; SCADA – systémy pro průmyslové řízení a sběr dat.

- Nízká připravenost a působení příslušníků bezpečnostních složek v prostředí tzv. darknetu (či deep webu, tedy skrytého internetu), které je ve stále větší míře využíváno organizovanými zločineckými strukturami a teroristy.
- V nízké míře je doposud využíváno přebírání zkušeností, zejména v oblasti vzdělávání, od zahraničních partnerů, kteří mají s prostředím darknetu dlouhodobé praktické zkušenosti.
- Nedostatečně prověření zaměstnanci, nebo odborně znalí zaměstnanci pracující ve prospěch třetích stran, kteří mají přístup ke strategickým aktivům, mohou exfiltrací citlivých a jinak důležitých informací a dat vážně ohrožovat kybernetickou bezpečnost ČR.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Základní dokumenty

Základním dokumentem pro zajišťování kybernetické bezpečnosti v ČR je BS 2015, na kterou navazuje Národní strategie kybernetické bezpečnosti na období let 2015 až 2020 (Strategie), jakožto stěžejní dokument upravující strategický rámec zajišťování kybernetické bezpečnosti v ČR. Ze Strategie vychází Akční plán kybernetické bezpečnosti ČR na období let 2015 až 2020 (Akční plán), který definuje konkrétní úkoly, stanovuje u nich zodpovědnost, termíny jejich plnění a kontrolu. NBÚ průběžně sleduje, diskutuje a hodnotí plnění Strategie a Akčního plánu ve spolupráci se všemi ostatními zainteresovanými subjekty. V rámci každoroční Zprávy o stavu kybernetické bezpečnosti v ČR, která informuje vládu ČR o stavu zajišťování kybernetické bezpečnosti, zpracovává hlášení vládě ČR o stavu naplňování Akčního plánu ve formě přílohy.

V oblasti kybernetické kriminality jsou postupně naplňovány nejen úkoly vyplývající ze Strategie a Akčního plánu, ale i opatření obsažená v Koncepci rozvoje schopností Policie ČR vyšetřovat informační kriminalitu s cílovým stavem v roce 2020.

Na základě Strategie a Akčního plánu jsou také nově vytvářeny i kapacity v oblasti kybernetické obrany v rámci VZ. V neposlední řadě s ohledem na problematiku eGovernmentu lze zmínit také Strategii rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ITC služeb.

Legislativa

V oblasti kybernetické bezpečnosti ČR disponuje unikátním zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB), a jeho prováděcími právní předpisy – vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (tzv. vyhláška o kybernetické bezpečnosti). Dále bylo v tomto směru novelizováno nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (novela zveřejněna ve Sbírce zákonů pod číslem 315/2014 Sb.).

Veškeré trestné činy, včetně těch páchaných v kybernetické oblasti, jsou upraveny zákonem č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. U kybernetické kriminality je většina trestných činů proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů upravena v hlavě

V. o trestných činech proti majetku. Trestné činy páchané ve vztahu k datům (uloženým informacím) jsou pak zejména tyto:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
- Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).

Odposlech dat je upraven v § 182 mezi trestnými činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.

Co se týče kybernetické obrany, v současné době probíhá mezirezortní připomínkové řízení návrhu legislativních změn, které jsou nezbytné pro výkon kybernetické obrany ze strany VZ. Do doby schválení těchto legislativních změn tak VZ plní úkoly v souladu se stanovenou působností a prioritami stanovenými vládou spočívající pouze v zabezpečování relevantních informací důležitých pro obranu a bezpečnost státu.

Odpovědné instituce a orgány

Národní bezpečnostní úřad

V ČR je zodpovědným vládním tělesem za kybernetickou bezpečnost NBÚ. Od roku 2011 působí jako gestor kybernetické bezpečnosti a národní autorita v této oblasti (dle usnesení vlády ČR č. 781/2011). V roce 2014 byl také skrze ZKB pověřen výkonem státní správy v oblasti kybernetické bezpečnosti. Na základě přijatého usnesení vzniklo v jeho struktuře Národní centrum kybernetické bezpečnosti (NCKB) se sídlem v Brně. Úlohou NCKB je především koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům. V rámci NCKB je provozován vládní CERT (GovCERT.CZ), který hraje klíčovou roli při ochraně KII a VIS dle ZKB. Tento zákon zavedl i institut národního CERT[77], jehož provozovatelem je na základě veřejnoprávní smlouvy s NBÚ v současnosti CZ.NIC.

Ministerstvo vnitra

MV plní úkoly v oblasti vnitřní bezpečnosti a veřejného pořádku. Z hlediska kybernetické bezpečnosti má klíčovou roli především jako hlavní gestor elektronizace výkonu veřejné správy (eGovernmentu) a je zodpovědné za provoz celé řady důležitých informačních a komunikačních systémů, důležitých pro fungování státní správy (základní registry, datové schránky, systém Czech Point, CMS, atd.) i integrovaného záchranného systému (např. linka 112, systém PEGAS). Do budoucna budou všechny systémy postupně napojovány na dohledové centrum eGovernmentu (DCeGOV), které v současné době již monitoruje některé VIS a KII.

Policie ČR

Policie ČR jako největší bezpečnostní sbor je jedním ze základních pilířů vnitřní bezpečnosti ČR. V boji s hrozbami v kyberprostoru jí patří nezastupitelná role orgánu činného v trestním řízení, jehož úkolem je vyhledávat, odhalovat a vyšetřovat kybernetickou trestnou činnost. Zásadní pro splnění tohoto cíle je efektivní působení odborně připravených policistů v prostředí internetových sociálních

[77] Orgány a osoby uvedené v § 3 písm. a) a b) ZKB, plní povinnosti k národnímu CERT.

sítí, ve skrytých částech internetu a při identifikaci původců hrozeb. Základními předpoklady k zajištění takové činnosti jsou odpovídající personální a materiální zdroje, cílený systém vzdělávání a služební přípravy, jakož i legislativní prostředí umožňující rychle a efektivně reagovat na kybernetickou trestnou činnost, včetně důkazního zajištění informací nacházejících se v kybernetickém prostoru. Zodpovědným pracovištěm Policie ČR v rámci vyšetřování kybernetické kriminality je Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování (NCOZ SKPV), potažmo krajská ředitelství Policie ČR.

Ministerstvo obrany

Rezort MO odpovídá za zajištění kybernetické bezpečnosti rezortních komunikačních a informačních systémů a vojenských sítí.

MO je odpovědné za minimalizaci dopadů kybernetických hrozeb v případech, kdy tyto hrozby mohou ohrozit působení ozbrojených sil ČR:

- použití kybernetických útoků v rámci vojenských nebo hybridních operací;
- kybernetická špionáž zaměřená na získání informací vojenského charakteru;
- nepřátelské kampaně a působení cizí moci v kyberprostoru za účelem dosažení vojenských cílů.

MO také odpovídá za plnění závazků v oblasti Cyber Defence vyplývajících z členství v NATO a EU při plánování, výstavbě a rozvoji schopností ozbrojených sil ČR.

Ministerstvo zahraničních věcí

MZV se v součinnosti a spolupráci s NBÚ a některými dalšími rezorty podílí na realizaci či úspěšném naplňování konkrétních úkolů stanovených v Akčním Plánu k Strategii především ve vztahu k mezinárodním organizacím a vybraným státům. MZV zároveň pojímá kybernetickou problematiku jako téma zahraniční politiky ČR.

Zpravodajské služby ČR

Základním posláním BIS, ÚZSI a VZ je získávání informací a jejich vyhodnocování s cílem odhalit ohrožení zájmů a bezpečnosti státu a obyvatelstva ČR. Zpravodajské služby tak provádí dle své zákonné působnosti i sběr a analýzu informací o hrozbách a rizicích v kyberprostoru. Na zajišťování kybernetické bezpečnosti v ČR se podílí především poskytováním zpravodajských informací příslušným orgánům státní správy.

VZ jako součást MO je zároveň gestorem kybernetické obrany ČR a na základě schválené Strategie a Akčního plánu v současnosti vytváří Národní centrum kybernetických sil (NCKS), které bude v budoucnu provádět široké spektrum operací v kyberprostoru a další aktivity nutné pro zajištění kybernetické obrany ČR.

C. SWOT analýza

Silné stránky

- Fungující, základní právně-legislativní rámec pro řešení kybernetické bezpečnosti.
- Kapacity NCKB, respektive vládního CERT (GovCERT.CZ) na dobré úrovni.
- Velmi dobrá mezinárodní spolupráce v oblasti kybernetické bezpečnosti, především mezi CERT/CSIRT pracovišti.
- Velké množství CSIRT/CERT týmů v ČR a efektivní spolupráce v rámci komunity.
- Budování NCKS pro zvládání a řešení závažných kybernetických útoků v rámci konceptu kybernetické obrany.
- Aktuální a prosazovaný strategický rámec kybernetické bezpečnosti ČR.
- Efektivní implementace a každoroční evaluace Strategie, respektive jejího Akčního plánu.
- Efektivní model spolupráce v kybernetické bezpečnosti mezi bezpečnostními institucemi, zpravodajskými službami a dalšími vrcholovými národními aktéry.

Slabé stránky

- Omezené finanční prostředky jednotlivých organizací vynaložitelné na prevenci a zvládání kybernetických hrozeb.
- Nedostatek kvalifikovaných specialistů na problematiku ICT a kybernetické bezpečnosti a neschopnost tyto odborníky řádně finančně ohodnotit.
- Špatně nastavené politiky kybernetické bezpečnosti, přehlížení a podceňování kybernetických hrozeb ve státní správě. Dlouhodobé podceňování edukace zaměstnanců v oblasti kybernetické bezpečnosti a nedostatečná IT gramotnost relevantních pracovníků státní správy.
- Některá strategická odvětví nejsou a nemohou být dle současné právní úpravy zahrnuta do soustavy KII.
- Právní úprava problematiky veřejných zakázek nereflektuje požadavky na kybernetickou bezpečnost a naopak může vytvářet či posilovat kybernetická bezpečnostní rizika.
- Právní úprava zajišťující občanům ČR svobodný přístup k informacím nereflektuje požadavky na kybernetickou bezpečnost a naopak může vytvářet či posilovat kybernetická bezpečnostní rizika.
- Nedostatky právní úpravy v problematice vyšetřování kybernetické kriminality.
- Absence mechanismu systematického komplexního vyhodnocování událostí a aktivit, které by vedlo k rozpoznání potenciální hybridní kampaně[78].

[78] Podrobněji se této problematice věnuje kapitola „Hybridní hrozby“.

- Nízká připravenost bezpečnostních složek na fenomén kyberterorismu a dalších teroristických aktivit v kyberprostoru.
- Nedostatečná úprava vztahů mezi správci KII či VIS na straně jedné a dodavateli či subdodavateli ICT služeb na straně druhé.
- Nedostatečné působení pracovníků bezpečnostních složek v darknetu, jakož i nízká znalost tohoto prostředí.
- Slabé bezpečnostní povědomí obyvatelstva ČR o službách eGovernmentu zneužitelné pachateli kybernetických útoků.
- Rozdílné personální zajištění agendy kybernetické bezpečnosti v orgánech státní a veřejné správy, kdy zaměstnanci ICT vykonávají svou činnost v rámci tří různých pracovně-právních poměrů (dle zákona č. 234/2014 Sb. o státní službě, zákona č. 262/2006 Sb., zákoník práce a zákona č. 361/2003 Sb. o služebním poměru příslušníků bezpečnostních sborů).

Příležitosti

- Motivovat odborníky na ICT a kybernetickou bezpečnost k práci ve státní správě vytvořením adekvátních, nejen finančních, podmínek.
- Prohlubovat a rozvíjet dosavadní mezinárodní spolupráci v oblasti kybernetické bezpečnosti založenou na nadstandardní pověsti ČR a její expertizy v této oblasti.
- Zapojovat se intenzivněji do mezinárodních projektů a aktivit v oblasti kybernetické bezpečnosti, kybernetické kriminality a kybernetické obrany.
- Standardizovat vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti a digitální hygieny státních orgánů na všech úrovních.
- Vytvořit centrální školící pracoviště pro kvalitní technické školení expertů ICT a kybernetické bezpečnosti.
- Možnost učit se ze zkušeností západních zemí s přípravami na příchod éry kyberterorismu, aniž bychom byli v tuto chvíli kyberterorismem bezprostředně ohroženi.
- Řešit situaci bezpečnosti dodavatelského řetězce s ohledem na výrobce a dodavatele, kteří dodávají nezabezpečený hardware a software.
- Novelizovat příslušné zákony vztahujících se ke kybernetické bezpečnosti, kybernetické kriminalitě a kybernetické obraně.
- Vybudovat v ČR na nadresortní úrovni (při koordinaci Úřadu vlády ČR) mechanismus k vyhodnocování potenciální hybridní kampaně[79].
- Stanovit orgány plnící roli národních partnerů „Hybrid Fusion Cell“ Evropské služby vnější akce (EEAS), pro účinnou spolupráci nejen v oblasti kybernetické bezpečnosti[80].
- Personálně i technologicky posílit NCKB a ve větší míře tak provádět audity kybernetické bezpečnosti, testování zabezpečení IS a KS (respektive odolnosti IT infrastruktury) u

[79] Konkrétní podoba řešení bude formulována až na základě závěrů jednání pracovní skupiny vytvořené v rámci systému BRS u ÚV ČR k implementaci závěrů Auditu v oblasti hybridních hrozeb, jejímž cílem je především nalezení konsensu o konkrétní podobě nadresortní platformy pro výměnu informací týkajících se hybridních hrozeb a pro koordinaci komunikace zainteresovaných subjektů

[80] Podrobněji se této problematice věnuje kapitola „Hybridní hrozby“.

relevantních subjektů, a zároveň poskytovat metodickou i jinou podporu všem (i nekritickým) entitám v ČR.

- Vytvořit platformu sdružující špičkové odborníky na ICT a kybernetickou bezpečnost z řad veřejného, akademického i soukromého sektoru na podporu odolnosti IT infrastruktury v ČR.
- Posílit (personálně i finančně) bezpečnostní složky o další specialisty zabývající se přímo problematikou kybernetické bezpečnosti, kybernetické kriminality a kybernetické obrany a kontinuálně je školit s ohledem na specifika jevů souvisejících s těmito oblastmi.
- Vytvořit zabezpečenou komunikační platformu mezi veřejnou a státní správou.

Hrozby

- Exponenciální nárůst množství kybernetických útoků a jejich potenciálních cílů, včetně vektorů útoků a bezpečnostních zranitelností.
- Působení cizí moci skrze kyberprostor na území ČR a kybernetické útoky jako jedna z metod hybridního válčení.
- Snadnější dostupnost sofistikovaných nástrojů pro provádění kybernetické špionáže, profesionalizace útočníků a budování ofenzivních kapacit u státních a nestátních aktérů na poli kybernetické bezpečnosti.
- Nedostatek kvalifikovaných pracovníků v oboru kybernetické bezpečnosti a ICT jako hrozba sui generis.
- Outsourcing řešení kybernetické bezpečnosti, respektive zabezpečení a celkové údržby ICT, rozšiřuje okruh potenciálních nositelů hrozeb.
- Nedostatečně prověření zaměstnanci, nebo odborně znalí pracovníci v ICT pracující ve prospěch třetích stran (insider hrozba) a nedostatečně prověření dodavatelé a subdodavatelé ICT produktů.
- Nepřátelské kampaně sponzorované státními aktéry prostřednictvím vlivových a dezinformačních mediálních kampaní prováděných v kyberprostoru.
- Zneužívání kyberprostoru zájmovými skupinami a teroristy pro účely získání vlastního prospěchu, nebo výhody, propagandy, podněcování nespokojenosti, či nenávisti ve společnosti a radikalizaci osob.
- Zadní vrátka (implementovaná v software i hardware) pro exfiltraci informací a dat.
- Hrozba závažného narušení bezpečnosti projektu eGovernment.

D. Doporučení k posílení odolnosti

1. Provést personální posílení bezpečnostních složek o další specialisty zabývající se přímo problematikou kybernetické bezpečnosti, kybernetické kriminality a kybernetické obrany.
2. Provést finanční posílení bezpečnostních složek jednak na podporu nových bezpečnostních projektů, technologického rozvoje a prohloubení či rozšíření stávajících schopností a kapacit, a jednak na podporu a vytváření osvětových akcí a dalších vzdělávacích projektů.

3. Provést některé novelizace platné právní úpravy v oblasti potírání kybernetické kriminality. Zejména je nutné se zaměřit na otázku anonymity uživatelů internetu a s tím spojené pátrání po pachatelích protiprávních skutků skrze možné doplnění dalších nástrojů do zákona o Policii ČR.
4. Zamezit nedostatku kvalifikovaných pracovníků v oboru kybernetické bezpečnosti skrze:
    a. vypracování opatření ke zvýšení počtu odborníků na kybernetickou bezpečnost v ČR. Ty by měly být následovány zlepšením odměňování klíčových pracovníků a nastavením takových pracovních podmínek, aby byl stát schopen získat uchazeče o takovou odbornou práci a následně byl schopen si takové odborníky udržet.
    b. novelizaci zákona č. 234/2014 Sb. o státní službě takovým způsobem, aby bylo zjednodušeno přijímání kvalitních odborníků na ICT a kybernetickou bezpečnost ve státní správě.
    c. rozšíření výuky kybernetické bezpečnosti na středních a zejména vysokých školách.
5. Zahrnout důležité sektory jako chemický průmysl, zdravotnická zařízení a další strategická odvětví do soustavy KII skrze:
    a. novelizaci krizového zákona a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, jež by umožnilo zahrnutí důležitých sektorů mezi sektory KI, pomocí kterého je KII určována.
6. Dostatečně upravit vztahy mezi správci KII a VIS na straně jedné a dodavateli a subdodavateli ICT služeb na straně druhé.
    a. K řešení tohoto problému již navrhl NBÚ, v rámci mezirezortního připomínkového řízení k návrhu zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a některé další zákony, předkládaný nyní MV (MV-165721/LG-2015) k dalšímu legislativnímu procesu do Legislativní rady vlády, změnu v této oblasti a současně navrhl změnu zákona č. 181/2014 Sb.
7. Ošetřit problematiku zákona o svobodném přístupu k informacím (č. 106/1999 Sb.) ve vztahu ke kybernetické bezpečnosti, buďto:
    a. novelizací rozsahu zákona č. 106/1999 Sb., nebo
    b. rozšířením povinnosti zachovávat mlčenlivost upravenou v ZKB i o vybrané aspekty bezpečnostních opatření, a stanovit tuto povinnost i správcům a provozovatelům informačních systémů a sítí ve věcné působnosti tohoto zákona (nyní se mlčenlivost týká jen evidence incidentů vedené vládním CERT). Tím by bylo dosaženo efektu vynětí bezpečnostně exponovaných informací z rozsahu zákona č. 106/1999 Sb. bez toho, aby bylo třeba zasahovat do jeho struktury.
8. Snížit kybernetická bezpečnostní rizika spojená se zákonem o veřejných zakázkách (zákon č. 134/2016 Sb.), respektive zamezit zpřístupnění zadávací dokumentace třetím osobám a umožnit v některých specifických případech vyloučit uchazeče z důvodu existence bezpečnostních rizik na jeho straně.
    a. Zadávací řízení na dodávky ICT nelze z působnosti zákona vyjmout a priori. Je však nutné legislativně upravit situace, kdy by měla být kybernetická bezpečnost jednotlivých KII a VIS nadřazena co nejotevřenější hospodářské soutěži tak, aby měli správci KII a VIS možnost řídit rizika tak, jak jim přikazuje ZKB. Je také vhodné najít shodu s Ministerstvem pro místní rozvoj a Úřadem pro ochranu

hospodářské soutěže, jakým způsobem zajistit požadavky vyplývající ze ZKB při co nejotevřenější hospodářské soutěži.

ENERGETICKÁ, SUROVINOVÁ A PRŮMYSLOVÁ BEZPEČNOST

ENERGETICKÁ BEZPEČNOST

I) Narušení dodávek elektrické energie velkého rozsahu

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

Nejpravděpodobnější příčinou velkoplošného výpadku dodávek elektrické energie je nepředvídatelný obtížně regulovatelný přebytek elektrické energie, technická závada, živelní pohroma, kybernetický nebo teroristický útok, a to především na úrovni přenosové soustavy. V poslední době zpracované studie a průběžný monitoring situace nasvědčují, že pravděpodobnost výskytu velkoplošného výpadku dodávek elektrické energie je relativně nízká. I přesto však k výpadku v řádu několika málo hodin v minulosti došlo, např. na území hl. m. Prahy. V tomto ohledu je však nutné uvést, že při velkoplošném výpadku na celém území státu by velmi pravděpodobně byla postižena celá střední Evropa a pravděpodobně i určitá část západní Evropy a naopak je nutné uvést, že propojenost elektrizačních soustav jednotlivých států a jejich synchronní provoz umožňuje šíření krizových situací do ČR ze sousedních, resp. z jiných evropských států. Pokud by příčinou výpadku byla „pouze“ disproporce mezi výrobou a spotřebou elektrické energie, pak by bylo velmi pravděpodobně možné obnovit fungování elektrizační soustavy v řádu jednotek hodin. Pokud by však např. z důvodu povětrnostních podmínek došlo k pádu stožáru přenosové soustavy nebo pokud by bylo vedení významně poškozeno nebo dokonce zcela zničeno např. teroristickým útokem, pak by bylo možné očekávat významně delší časový horizont potřebný k obnově provozu. V tomto ohledu by bylo velmi pravděpodobně nutné najít co nejrychleji náhradní trasy pro zajištění dodávky elektrické energie. Subjekty, které jsou důležité pro chod státu a zajišťování základních životních potřeb obyvatelstva a subjekty kritické infrastruktury by ve svých prvcích měly mít instalované náhradní zdroje elektrické energie. Je však nutné konstatovat, že ne všechny je v současné době mají a navíc jsou dimenzovány jen na určitou dobu chodu (cca kolem 6 – 8 hodin). Dieselagregáty jsou sice připraveny dodávat elektrickou energii během několika desítek vteřin, ale zásoby paliva podle zátěže vydrží většinou maximálně 8 hodin. To znamená, pokud by došlo k výpadku např. v délce 4 – 5 hodin, mělo by být vše v pořádku, ale pokud by výpadek trval několik dní, nastal by velký logistický problém jak doplňovat pohonné hmoty. Z uvedeného vyplývá, že cca po 8 hodinách by většina dieselagregátů byla mimo provoz. Řešením by bylo, aby legislativa uložila povinnost mít náhradní zdroje elektrické energie a udržovat dostatečné zásoby pohonných hmot (např. v Rakousku je to 72 hodin).

Kybernetické útoky na energetický sektor jsou prováděny stále častěji. Povaha této hrozby se také mění a energetické společnosti se celosvětově potýkají s mnohem inteligentnějšími a složitějšími kybernetickými útoky. Vzhledem k trendu otevřenosti a propojování důležitých průmyslových řídicích systémů (ICS) a SCADA (Supervisory Control and Data Acquisition – dispečerské řízení a sběr dat) s dalšími IT systémy k zajištění vyšší efektivnosti a snížení nákladů, se riziko neustále zvyšuje. Nejen v energetickém sektoru se přitom používají ICS/SCADA s dlouhou provozní životností, které postupem času přestávají vyhovovat požadavkům na kybernetickou bezpečnost. Důsledky útoků na energetický sektor mohou být katastrofální. Koordinované kybernetické útoky na elektrickou síť na

Ukrajině z prosince 2015, které způsobily několikahodinový výpadek elektřiny desítkám tisíc domácností, jasně demonstrují aktuální ohrožení.

Pokud by byla elektrizační soustava fyzicky napadena, mohlo by to způsobit vážný problém, ale pouze v případě např. vícenásobného teroristického útoku. Z tohoto důvodu byla zpracována Analýza dopadů vícenásobného teroristického útoku na přenosovou soustavu, resp. narušení či vyřazení její funkcionality velkého rozsahu v důsledku úmyslného jednání útočníka. Bylo vytipováno několik nejcitlivějších míst, při jejichž současném napadení v kritický den s maximálním zatížením vedení a v kombinaci s odstávkami v rámci realizace plánovaného investičního programu by mohlo dojít k velkoplošnému výpadku dodávek elektrické energie. Zpracováním analýzy se podařilo posoudit stávající bezpečnostní dokumenty s cílem zkvalitnit podmínky pro rychlý a efektivní zákrok složek Integrovaného záchranného systému (minimalizovat dojezdový čas, a reakci na signál typu „tíseň“, zkvalitnit krizovou komunikaci a standardizaci bezpečnostních postupů a procedur).

1. V současné době je nejpravděpodobnější možnou příčinou výpadku neočekávaný přetok velkého množství elektrické energie zejména ze severních oblastí Německa, kde jsou rozmístěny intermitentní zdroje velkých výkonů. Elektřina z těchto zdrojů je, částečně přes českou přenosovou soustavu, přenášena do míst spotřeby na jihu Německa a v Rakousku (viz např. mimořádná situace v přenosové soustavě ČR vlivem enormní výroby ve větrných parcích v Německu na přelomu roku 2014/2015). Další příčinou neplánovaných toků elektřiny ohrožujících bezpečnost přenosové soustavy ČR je neexistence koordinovaného alokačního mechanismu přeshraničních kapacit na německo-rakouské hranici. Společná německo-rakouská nabídková (obchodní) zóna umožňuje de facto neomezené obchodní výměny, které převyšují fyzické možnosti propojených soustav Německa a Rakouska. Takový výpadek dodávek elektrické energie by byl zvládnutelný v řádu hodin, protože by zapracovaly elektrické ochrany a zařízení přenosové soustavy by zůstalo nepoškozené.

V případě kumulace poruch či útoků na více místech a následné dezintegrace přenosové sítě musí být garantována včasná obnova dodávky elektřiny pro všechny velké aglomerace. Jeden z nástrojů vymezený ve Státní energetické koncepci ČR proto ukládá zpracování národního programu se zaměřením na zvýšení energetické odolnosti a schopnost ostrovních provozů velkých aglomerací. Mezi priority stanovené Státní energetickou koncepcí ČR potom patří také doplnění územních energetických koncepcí krajů o problematiku zabezpečení ostrovních provozů v nouzových stavech, které v současné době postupně probíhá podle zákona o hospodaření energií.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Odpovědné instituce: MPO, ERÚ, SEI, NBÚ

Základní nástroje (legislativa): zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích (energetický zákon), vyhláška č. 79/2010 Sb., o dispečerském řízení elektrizační soustavy a o předávání údajů pro dispečerské řízení, vyhláška č. 80/2010 Sb., o stavu nouze v elektroenergetice a o obsahových náležitostech havarijního plánu, vyhláška č. 401/2010 Sb., o obsahových náležitostech Pravidel provozování přenosové soustavy a Pravidel pro provozování distribuční soustavy, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Základní nástroje (strategie, koncepce EU): Směrnice Evropského parlamentu a Rady 2005/89/ES, o opatřeních pro zabezpečení dodávek elektřiny a investic do infrastruktury a nařízení Evropského parlamentu a Rady (EU) č. 347/2013, kterým se stanoví hlavní směry pro transevropské energetické sítě a sdělení Komise Evropského parlamentu, Radě, Evropskému hospodářskému a sociálnímu

výboru, Výboru regionů a Evropské investiční bance – Rámcová strategie k vytvoření odolné energetické unie s pomocí progresivní politiky v oblasti změny klimatu (2015).

Základní nástroje (strategie, koncepce ČR): Státní energetická koncepce ČR, Typový plán narušení dodávek elektrické energie velkého rozsahu, Národní strategie kybernetické bezpečnosti na období let 2015 až 2020, Akční plán kybernetické bezpečnosti ČR na období let 2015 až 2020.

C. SWOT analýza

Silné stránky

- Vysoká kvalita a spolehlivost dodávek elektrické energie.
- Relativně příznivý ukazatel dovozní energetické závislosti.
- Plná soběstačnost ve výrobě elektřiny a tepla.
- Právní regulace kybernetické bezpečnosti ICS/SCADA[81] v energetickém sektoru.
- Výroba elektřiny/tepla je dosud postavena prioritně /významně na domácích zásobách.

Slabé stránky

- Stárnoucí zdrojová základna i síťová infrastruktura.
- Vnímání samozřejmosti vysokého standardu kvality a spolehlivosti.
- Používání zastaralých ICS/SCADA systémů nevyhovujících požadavkům na kybernetickou bezpečnost.
- Nedostatečně rozpracované legislativní pokrytí, technické a technologické předpisy zajišťující kybernetickou bezpečnost v oblasti chytrých sítí (smart grids).

Příležitosti

- Pokračující propojování evropských trhů s elektřinou.
- Uvedení do provozu transformátorů s regulací fáze na českém území k předcházení krizových stavů na úrovni přenosové soustavy.
- Vytvořit moderní legislativu zajišťující kybernetickou bezpečnost v oblasti chytrých sítí (smart grids).
- Podílet se na mezinárodní spolupráci při standardizaci a vytváření technických předpisů a technologických manuálů pro zajištění kybernetické bezpečnosti v oblasti chytrých sítí (smart grids).
- Zavedení koordinovaného alokačního mechanismu přeshraničních kapacit na německo-rakouské hranici, tj. rozdělení společné německo-rakouské obchodní zóny.

[81] ICS – informační a komunikační systémy, SCADA – dispečerské řízení a sběr dat (software, který z centrálního pracoviště monitoruje průmyslová a jiná technická zařízení a procesy a umožňuje jejich ovládání.

Hrozby

- Nucené ukončení provozu jaderné elektrárny Dukovany z technických či politických důvodů.
- Pokračující rozvoj výroby elektřiny z intermitentních zdrojů v severní části Německa s pokračujícím trendem úbytku stabilních zdrojů v místech vysoké spotřeby na jihu při současném zpožďování dostatečného propojení těchto oblastí.
- Ohrožení funkce chytrých sítí (smart grids) a tím energetické infrastruktury.

D. Doporučení k posílení odolnosti

1. V rámci zpracování Národního programu energetické odolnosti definovat společensko-technické standardy (stupně bezpečnosti dodávek elektrické energie) pro normální stav a stav nouze v elektroenergetice.
2. Prověřovat připravenost odvětví elektroenergetiky na řešení případných stavů nouze formou pravidelných cvičení jak na úrovni přenosové soustavy, tak na úrovni distribučních soustav, za účasti regionálních orgánů krizového řízení a složek Integrovaného záchranného systému.
3. Aktualizovat plány krizové připravenosti subjektů kritické infrastruktury k zajištění fyzické ochrany prvků kritické infrastruktury.
4. Aktualizovat územní energetické koncepce se zaměřením na energetickou odolnost a schopnost dodávek elektrické energie v ostrovních provozech.
5. Stanovit povinnost disponovat náhradním zdrojem elektrické energie a udržovat dostatečné zásoby pohonných hmot pro případ déletrvajícího výpadku.
6. Zajistit bezpečné a dostupné komunikační prostředí pro řešení krizových situací zapříčiněných rozsáhlými výpadky dodávek elektrické energie a jeho využití v oblasti preventivního monitoringu.
7. Připravit studii nejvhodnějšího postupu zajištění zásob jaderného paliva v rozsahu stanoveném pro pokrytí jednoho palivového cyklu všech jaderných elektráren.

II) Narušení dodávek plynu velkého rozsahu

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

Nejpravděpodobnější příčinou výpadku dodávek plynu jsou přírodní pohromy, technologické havárie, terorismus nebo obchodně-politické spory. V závislosti na územním rozsahu a intenzitě působení přírodních pohrom může být narušen mezinárodní tranzit plynu. Jedná se o ohrožení především vrchních přechodů vodních toků záplavami v místech, kde dochází k odplavení nebo sesunutí zeminy. Důsledné zajištění těchto kritických míst toto riziko významným způsobem snižuje. Technologické havárie mohou být rovněž příčinou podstatných změn provozního režimu plynárenské soustavy. Při běžném provozu lze míru těchto rizik eliminovat důsledným dodržováním údržbářských a opravárenských činností dle plánu údržby a stanovených technologických postupů, bezpečnostních předpisů, prováděním inspekcí, kontrol, revizí a zkoušek plynového zařízení včetně periodických školení obsluhy a montážních pracovníků plynových zařízení. Destrukce provozních objektů

plynárenské soustavy teroristickým činem by měla přímý vliv na spolehlivost zásobování ČR zemním plynem. Čím vyšší tlakový stupeň plynovodů by byl zasažen, tím větší plošné dopady by havárie měla. Havárie zásobníků plynu by měla podstatný dopad na zásobování zákazníků především v zimních měsících. Míra ohrožení dlouhodobým přerušením dodávek plynu od jednoho zahraničního dodavatele je z pohledu prakticky plné závislosti na dovozu značná. Tuto míru je možné snižovat zajišťováním diverzifikace zdrojů a uzavíráním dlouhodobých smluv s producenty plynu. Zajištění dodávek plynu z více zdrojů a zajištění více než jedné dopravní cesty a také možnosti reverzních toků je i obranou vůči případnému politickému zneužívání a řešením při jakékoli mimořádné situaci. Evropský systém dálkové přepravy plynu se v posledních desetiletích rozvinul do zcela propojené podoby, což je významným předpokladem zajištění spolehlivosti a bezpečnosti dodávek.

Přepravní soustava ČR je robustní, vysoce kvalitní a pečlivě udržovaná a zajišťuje bez problému splnění standardu N-1. Tento standard je dokonce podstatně vyšší než je požadavek nařízení Evropského parlamentu a Rady EU č. 994/2010, o opatřeních na zajištění dodávek zemního plynu a o zrušení směrnice Rady 2004/67/ES .

Skladování plynu, které představuje cca 37 % roční spotřeby, významně pomáhá zajištění dodávek plynu koncovým zákazníkům. Skladovací kapacity se v současné době dále rozšiřují a po jejich dokončení bude celková skladovací kapacita odpovídat 40 % roční spotřeby.

ČR využívá diverzifikace dodávek. Přibližně 63,44 % plynu přichází z Ruské federace, 2,95 % z Norského království a 33,59 % z EU.

Dokončena byla i diverzifikace nové trasy, kde zprovozněním plynovodu Nord Stream, návazného plynovodu OPAL a plynovodu Gazelle (HPS Brandov) je možné dodávat plyn do ČR touto novou trasou která je však primárně určena na tranzit plynu do Německa (tedy z HPS Brandov a HPS Waidhaus). Byly také provedeny investice umožňující reverzní tok plynu ve směru západ – východ, částečně sever – jih (STORK I), i když ne v plném rozsahu. Z analýzy rizik vyplývá, že kumulace poruch, jako je souběžný výpadek dodávek plynu ve dvou hraničních předávacích stanicích je vysoce nepravděpodobný, stejně jako výpadek možnosti čerpání plynu z několika podzemních zásobníků plynu současně.

Výpadkem plynu není ani ohrožena výroba elektřiny, protože výroba elektřiny v plynových elektrárnách představuje pouze 2,5 % celkové výroby elektřiny. Není však do budoucna vyloučeno, že tento podíl bude dosahovat významně vyšších hodnot v závislosti na vývoji v oblasti výstavby nových elektroenergetických zdrojů. Zemní plyn je však významně využíván zejména ve vytápění a ohřevu teplé vody v sektoru domácností, kdy v roce 2015 bylo podle zprávy Energetického regulačního úřadu registrováno celkem 2 636 189 odběratelů na úrovni domácností. Zemní plyn také hraje významnou roli v průmyslovém sektoru.

Identifikovaná rizika, pokud nastane vždy jen jedno z nich, nezpůsobí ohrožení ani omezení dodávek plynu do ČR. Aby uvedená rizika měla dopad na zásobování zákazníků, musela by nastat alespoň dvě z nich současně, což je vysoce nepravděpodobné, zejména u výpadku HPS Lanžhot a HPS Hora Svaté Kateřiny. Z analýzy rizik vyplývá, že by musely nastat současně nejméně tři nepříznivé okolnosti, tj. výpadek největší infrastruktury, podstatné snížení těžby ze zásobníku plynu, a to vše za nepříznivých klimatických podmínek, které by trvaly delší období.

Nejzávažnější neočekávané neplnění dodávkových povinností ze strany společnosti Gazprom Export bylo zaznamenáno s ohledem na rusko-ukrajinské spory v období leden – únor 2006 a zejména v lednu 2009. V tomto období byly chybějící dodávky kompenzovány dodávkami z podzemních zásobníků plynu a dodávkami realizovanými jinými přepravními trasami, takže žádný ze zákazníků v ČR nebyl ve svých požadavcích na odběr zemního plynu krácen. U norských dodavatelů plynu nebyly zaznamenány žádné podobné případy, neboť mimořádné události (např. z důvodu údržby) jsou hlášeny s dostatečným časovým předstihem, aby bylo možno nakoupit plyn na trhu a tím předejít jeho nedostatku.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Odpovědné instituce: MPO, ERÚ

Základní nástroje (legislativa): zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích (energetický zákon), vyhláška č. 344/2012, o stavu nouze v plynárenství a o způsobu zajištění bezpečnostního standardu dodávky plynu ve znění pozdějších předpisů, vyhláška č. 401/2010 Sb., o obsahových náležitostech Pravidel přepravní soustavy, Řádu provozovatele přepravní a distribučních soustav a Řádu provozovatele podzemního zásobníku plynu a obchodních podmínek operátora trhu.

Základní nástroje (strategie, koncepce EU): Nařízení Evropského parlamentu a Rady č. 994/2010, o opatřeních na zajištění bezpečnosti dodávek zemního plynu a sdělení Komise Evropského parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru, Výboru regionů a Evropské investiční bance – Rámcová strategie k vytvoření odolné energetické unie s pomocí progresivní politiky v oblasti změny klimatu (2015).

Základní nástroje (strategie, koncepce ČR): Státní energetická koncepce ČR, každoročně aktualizovaný Havarijní plán plynárenské soustavy ČR, Plán opatření pro stav nouze ke zmírnění dopadu narušení dodávek plynu a jeho odstranění v ČR, Plán preventivních opatření nezbytných k odstranění nebo ke zmírnění zjištěných rizik pro zajištění dodávek zemního plynu v ČR, Plán posouzení rizik ovlivňujících bezpečnost dodávek zemního plynu v ČR.

C. SWOT analýza

Silné stránky

- Robustní, vysoce kvalitní a pečlivě udržovaná přepravní soustava.
- Diverzifikace přepravních tras.
- Vysoký standard plnění kritéria N-1.
- Umožnění reverzního toku v tranzitní přepravní soustavě.
- Vysoká kapacita zásobníků plynu vzhledem ke spotřebě zemního plynu i vysoký parametr jejich maximálního denního těžebního výkonu.

Slabé stránky

- Relativně nízká diverzifikace zdrojů zemního plynu.
- Komerční provoz zásobníků plynu – vtláčení ovlivněno vývojem spotových cen na evropských burzách.
- Kontrola GTS soukromou společností orientovanou na zisk.
- Aplikace pravidel evropské legislativy a důsledný unbundling.
- Naprostý nedostatek vlastních zdrojů zemního plynu.
- Nedostatečné propojení přepravních tras zemního plynu ve směru sever – jih.
- Stát nemá kontrolu nad přepravou plynu.

Příležitosti

- Výstavba nových zásobníků plynu v lokalitách s ukončenou těžbou uhlovodíků či hlubinnou těžbou uranu.
- Další rozvojové plány s ohledem na posilování infrastruktury.
- Možnost přístupu ke zdrojům zkapalněného plynu.
- Vybudování a posílení plynovodů ve směru sever – jih (propojení CZ-AT a CZ-PL).

Hrozby

- Růst podílu zemního plynu na výrobě elektřiny vlivem nepříznivého vývoje v oblasti výstavby jaderných elektráren.
- Privátní subjekty v plynárenství budou rozvojové investice realizovat pouze v případě zajištění relativně rychlé ekonomické návratnosti investic.

D. Doporučení k posílení odolnosti:

1. Navýšení provozního objemu a těžebních kapacit podzemních zásobníků plynu na území ČR.
2. Posílení severo-jižního propojení (Stork II, BACI).
3. Výstavba plynovodu „Moravia“ směrem na severní Moravu pro případ současného výpadku podzemních zásobníků plynu Lobodice, Štramberk a Třenovice.

III) Narušení dodávek ropy velkého rozsahu

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

ČR je závislá na dodávkách ropy ropovody Družba a IKL (trasa Ingolstadt - Kralupy nad Vltavou – Litvínov). Výroba pohonných hmot a dalších ropných produktů v českých rafinériích tedy bezprostředně souvisí s dodávkami ropy ropovody ze zahraničí, a to jak v množství, tak i kvalitě ropy, která je v rafinériích zpracovávána.

V tomto ohledu je nutné zmínit, že ropa dopravována do ČR z různých regionů má do určité míry odlišné vlastnosti. Z Ruské federace je ropovodem Družba přepravována tzv. středně těžká relativně sirnatá ropy. Ropovodem IKL je pak do Česka dopravována ropa zejména z Ázerbájdžánu a Kazachstánu. Z těchto zemí pochází ropa takzvaně lehká a sladká, tedy ropa s vyšším zastoupením méně složitých uhlovodíků a relativně menší sirnatostí. Zatímco rafinérie v Litvínově je nastavena na zpracování ruské ropy, rafinérie v Kralupech nad Vltavou zpracovává zejména ropu z oblasti Kaspického moře.

Tato závislost vytváří riziko vzniku situace, kdy dojde k přerušení dodávek ropy do ČR. Přerušení může být krátkodobé či dlouhodobé. Krátkodobé přerušení zřejmě nebude mít vliv na výraznější snížení produkce ropných produktů. Tento nedostatek ropy potřebné pro výrobu ropných produktů by byl vykrýván rezervami především rafinérií a dalších petrochemických společností a distributorů pohonných hmot, případně státních hmotných rezerv. Při déletrvajícím nedostatku ropy by mohlo

dojít k vyčerpání uvedených rezerv. Dlouhodobější nedostatek především pohonných hmot na trhu a předpoklad další eskalace by vytvořil již situaci, kterou by nebylo možné řešit bez zásahu státu a jeho správních úřadů, eventuálně orgánů územní samosprávy. V tomto okamžiku by bylo možné uvedenou situaci klasifikovat jako mimořádnou, která je definována v ustanovení zákona o nouzových zásobách ropy jako situace, kdy nastane nebo hrozí, že nastane ohrožení zásobování trhu ropou nebo ropnými produkty v ČR nebo v jiných členských státech EU nebo v členských státech Mezinárodní energetické agentury.

V situaci další eskalace nedostatku ropy a ropných produktů, zejména pohonných hmot, by vláda mohla vyhlásit stav ropné nouze. V rámci tohoto stavu může vláda stanovit opatření k omezení spotřeby ropy a ropných produktů. Pokud by byly dopady nedostatku pohonných hmot na trhu takového rozsahu, že by uvedené mělo mít vliv i na fungování další infrastruktury, mohlo by být vyhlášení stavu ropné nouze doprovázeno i vyhlášením krizového stavu.

Nejpravděpodobnější příčinou narušení dodávek ropy a ropných produktů by mohlo být zhoršení mezinárodně politické situace, dlouhodobý výpadek těžby a zpracování ropných produktů a distribuce ropných produktů ke spotřebiteli, přerušení provozu ropovodů Družba a/nebo IKL.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Odpovědné instituce: MPO, SSHR, NESO

Základní nástroje (legislativa): Zákon č. 189/1999 Sb., o nouzových zásobách ropy, o řešení stavů ropné nouze (zákon o nouzových zásobách ropy), zákon č. 97/1993 Sb., o působnosti Správy státních hmotných rezerv, vyhláška č. 165/2013 Sb., o druzích ropy a skladbě ropných produktů pro skladování v nouzových zásobách ropy, výpočtu nouzových zásob ropy, o skladovacích zařízeních a vykazování nouzových zásob ropy.

Základní nástroje (strategie, koncepce EU): Směrnice Rady 2009/119 ES, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy nebo ropných produktů, Nařízení Evropského parlamentu a Rady 1099/2006 ES o energetické statistice, Sdělení Komise Evropskému parlamentu a Radě – Evropská strategie energetické bezpečnosti, hloubková studie EU k evropské energetické bezpečnosti (2014) a sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru, Výboru regionů a Evropské investiční bance – Rámcová strategie k vytvoření odolné energetické unie s pomocí progresivní politiky v oblasti změny klimatu (2015).

Základní nástroje (strategie, koncepce ČR): Státní energetická koncepce ČR, Typový plán narušení dodávek ropy a ropných produktů velkého rozsahu, Plán opatření při ropné nouzi, Opatření k zavedení přídělového systému při stavu ropné nouze.

C. SWOT analýza

Silné stránky

- Diverzifikace dodavatelů a přepravních tras ropy.
- Dostatečné nouzové zásoby ropy a ropných produktů.
- Odpovídající legislativa ropné bezpečnosti a systém reakcí na nouzové stavy.

- Aktivní zapojení ČR do mezinárodního systému ropné bezpečnosti (IEA, EU).
- Hustá vnitrostátní produktovodní síť.
- Ochraňování nouzových zásob státem kontrolovanými subjekty.
- Skladování a distribuce pohonných hmot ve významném objemu pod kontrolou státu.

Slabé stránky

- Absence vlastních zdrojů ropy.
- Omezený vliv státu na rafinérie a jejich nejistá budoucnost.
- Stát nemá ve svých zásobách nízkosirnou neruskou, tzv. sladkou ropu.
- Potřeba relativně vysokých investic do rafinérií, u kterých je riziko, že prostředky nemusí být vyčleněny kvůli jiným investičním prioritám soukromého subjektu.

Příležitosti

- Možnost navýšení nouzových zásob při relativně nízkých cenách ropy.
- Výstavba dalších skladovacích kapacit na ropu nebo pohonné hmoty.

Hrozby

- Pokles státem držených nouzových zásob ropy a ropných produktů k hranici povinných 90 dnů z důvodu růstu domácí spotřeby.
- Dlouhodobé výpadky výroby ropných produktů v rafinériích.

D. Doporučení k posílení odolnosti:

1. Postupné zvyšování nouzových zásob až na 120 dnů průměrného denního čistého dovozu referenčního roku.
2. Zařazení lehké ropy do struktury nouzových zásob.
3. Další diverzifikace přepravních tras (např. projekt společného zájmu EU Litvínov – Leuna).
4. Posílení role státu v českém rafinérském průmyslu (podpora tuzemského zpracování ropy).
5. Pravidelné prověrky plánů a opatření pro stavy ropné nouze.
6. Zajištění dosažitelnosti nouzových zásob ropy skladováním na území ČR.

SUROVINOVÁ BEZPEČNOST

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

Nerostné suroviny reprezentují zcela zásadní vstup pro naprostou většinu průmyslových odvětví a tím i pro celou ekonomiku země a jejich nepřerušované dodávky jsou klíčem k udržení ekonomiky v chodu. Zajištění nediskriminačního přístupu k nerostným zdrojům ať již z domácích zdrojů nebo

z dovozu je zásadním parametrem surovinové bezpečnosti státu. Tuto skutečnost si globální hráči velmi dobře uvědomují a státy uvažující strategicky kladou na zajištění dostatku vstupních nerostných zdrojů pro své ekonomiky mimořádný důraz.

V první dekádě 21. století došlo vlivem rozsáhlé modernizace části někdejších rozvojových, zpravidla velmi lidnatých, zemí k překlopení dosavadních principů, na kterých po desetiletí fungoval světový trh s nerostnými surovinami. V důsledku toho se z typických producentů a vývozců nerostných surovin stali postupně v řadě případů jejich spotřebitelé, nebo dokonce dovozci. Tento fakt dodal tradičnímu soupeření o nerostné zdroje mezi globálními hráči novou kvalitu i dynamiku. Tradičně mimořádnou pozornost věnují zabezpečení národních ekonomik nerostnými surovinami asijské státy (Japonsko, Jižní Korea, později i Čínská lidová republika). Evropa jako kontinent se nachází ve velmi nekonformní pozici – je jedním z největších světových spotřebitelů nerostných surovin, současně je však jejich zanedbatelným producentem, takže není schopna ovlivňovat světové trendy v surovinovém průmyslu. Těžební průmysl byl v Evropě v 70., 80. a 90. letech zbytečně rychle utlumen, což se po zásadních změnách na světovém trhu po roce 2003 ukázalo jako strategicky chybné rozhodnutí. V současnosti jsou členské státy EU vysoce závislé na dovozu řady nerostných surovin (včetně strategických komodit) ze zahraničí, což činí EU v této oblasti vydíratelnou. EU tak není schopna jako celek ani svým členům garantovat zajištění odpovídající surovinové a energetické bezpečnosti. V této situaci byla na konci roku 2008 představena integrovaná strategie Raw Materials Initiative, která se snaží tuto situaci řešit. Je postavena na třech vzájemně propojených pilířích:

a) vyšší míra využívání domácích (evropských) nerostných surovin;

b) podpora vzájemně výhodných ekonomických vztahů se zeměmi třetího světa, které mají široký nerostně surovinový potenciál (surovinová diplomacie);

c) podpora materiálově úsporných technologií, např. chytré recyklace.

EU v následujících letech vytipovala seznam tzv. kritických (superstrategických) komodit na jejichž dovozu je EU extrémně závislá, které jsou produkovány monopolně jedním či několika málo státy či které jsou do EU importovány z politicky nestabilních oblastí – nejprve se v roce 2011 jednalo o 14 nerostných komodit, později po opětovném vyhodnocení byl tento seznam v roce 2014 rozšířen na celkem 21 komodit. Jedná se o následující komodity: *antimon, beryllium, boráty, fluorit, fosfáty, galium, germanium, hořčík, chrom, indium, kobalt, koksovatelné uhlí, kovy platinové skupiny, křemík, lithium, magnezit, niob, kovy lehkých vzácných zemin, kovy těžkých vzácných zemin, přírodní grafit a wolfram.*

Přerušení dodávek některé strategické nerostné suroviny by vedlo k ohrožení určité strategické výroby či k poškození konkurenceschopnosti české ekonomiky.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Odpovědné instituce: MPO, SSHR.

Základní nástroje (legislativa): zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

Základní nástroje (strategie, koncepce EU): Raw Materials Initiative (2008), Critical Raw Materials (2011; 2014).

Základní nástroje (strategie, koncepce ČR): Surovinová politika ČR v oblasti nerostných surovin a jejich zdrojů (2016), Státní energetická koncepce ČR (2015), Východiska ke koncepci surovinové a energetické bezpečnosti (2011).

C. SWOT analýza

Silné stránky

- Relativně dobrá prozkoumanost území ČR tradičními metodami na tradiční suroviny.
- Solidní zásoby i produkce některých nerudních surovin.
- Solidní zásoby stavebních surovin.
- Dobré jméno české/československé geologie ve světě.
- Vlastní, na evropské poměry solidní zásoby uranové rudy.
- Vlastní, i když časově/administrativně omezené zásoby hnědého uhlí.

Slabé stránky

- Výsledky průzkumné činnosti jsou staré 30 až 50 let, jejich kvalita, zaměření, vypovídající schopnost a tím pádem využití je v mnoha případech problematické zejména s ohledem na moderní, dříve nedostupné technologie těžby a úpravy.
- Minimální znalosti o potenciálu území ČR v oblasti nových moderních high tech surovin.
- Naprostý nedostatek vlastních ekonomicky těžitelných zdrojů rud i specifické části nerudních surovin.
- Dosud málo rozvinutá surovinová diplomacie jakožto nedílná součást české ekonomické diplomacie.
- Preference ekologického pilíře udržitelného rozvoje společností a některými úřady

Příležitosti

- Využití moderních metod průzkumu pro vyhledání nových surovinových zdrojů na našem teritoriu (např. high tech surovin), včetně využití moderních metod těžby a úpravy.
- Odstranění části ekologických zátěží z minulosti jejich znovuvyužitím jakožto druhotných ložisek cenných komodit.
- Zjištění potenciálu ČR v oblasti moderních high tech surovin, např. strategických kovů.
- Udržení cenného know-how v oblasti těžby a úpravy uranových rud a možnost jeho využití v surovinové diplomacii.
- Restrukturalizace existujících strategických zásob surovinových komodit ve státních hmotných rezervách bez potřeby značných finančních prostředků ze státního rozpočtu.
- Předvídavé budování infrastruktury pro dopravu surovin do ČR v časovém předstihu, dopravní kapacitě a s dostatečnou rezervou.

Hrozby

- Ztráta těžební schopnosti některých specifických nerostných komodit – zúžení spektra produkovaných surovin v ČR – zvýšení dovozní závislosti státu.

- Nedostatečná průběžná náhrada dotěžovaných ložisek novými lokalitami.
- Ztráta nezbytného know how v oblasti technických věd.
- Omezování diverzifikace dodávek strategických surovin do ČR.
- Ztráta kontroly nad kritickou infrastrukturou dosud patřící státu.
- Omezování nebo likvidace strategických zpracovatelských kapacit.
- Trvání nepříznivé situace na světovém trhu černého uhlí, které ohrožuje evropský černouhelný průmysl.
- Pokles státem držených nouzových zásob ropy a ropných produktů k hranici povinných 90 dnů z důvodu růstu domácí spotřeby.

D. Doporučení k posílení odolnosti:

1. Restrukturalizace/modernizace struktury státních hmotných rezerv v oblasti neenergetických komodit.

2. Zjištění skutečného potenciálu českého území v oblasti moderních high-tech surovin, které jsou využívány v průmyslových odvětvích s vysokou přidanou hodnotou.

PRŮMYSLOVÁ BEZPEČNOST

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

Průmysl tvoří v ČR významné odvětví ekonomiky. Reprezentuje 35 % českého hospodářství a zaměstnává přes 40 % všech ekonomicky aktivních obyvatel země. Mezi hlavní pilíře českého průmyslu patří průmysl strojírenský, hutnický, chemický a potravinářský. Dalšími významnými složkami jsou průmysl energetický, stavební a spotřební. Strojírenský průmysl patří v ČR k nejtradičnějším odvětvím. Jeho nejdůležitější součástí je automobilový průmysl, který se také výrazně podílí na exportu země. Exportní výkonnost je tažena zejména automobilovým, elektronickým, strojírenským a elektrotechnickým průmyslem. Jejich souhrnný podíl na exportu činí více jak 60 %.

Závislost české ekonomiky na exportu do zemí EU se stále udržuje na vysoké úrovni. Do zemí EU míří více jak 80 procent tuzemského vývozu. Ekonomicky se daří střední a severní zóně EU a poptávka po českém zboží roste. Největší obchodní partneři ČR Německo a Slovensko se stále větší měrou podílejí na odběru zboží. Stát přitom podporuje opačný trend – Exportní strategie ČR na roky 2012 až 2020 stanovuje 12 prioritních zemí pro export a všechny jsou mimo EU. Exportéři se však na evropském trhu dobře orientují. Nenarážejí zde na kulturní problémy a administrativa spojená s exportem zboží a služeb je relativně jednoduchá. Udržování zahraniční obchodní sítě není tak časově a finančně náročné v porovnání se vzdálenějšími trhy.

Hospodářský vývoj v ČR a Německu probíhá paralelně. Jestliže se zvyšuje v ročním srovnání HDP v Německu, dochází k obdobnému vývoji i v ČR. ČR kopíruje i opačný směr – snížení přírůstků či absolutní pokles oproti předcházejícímu roku zaznamená česká ekonomika rovněž v témže roce. Vyvodit z toho ale závěr, že české hospodářství je s německým tak úzce propojeno, že německý růst je zárukou českého růstu, by bylo nebezpečným zjednodušením. Tento vzájemný vztah souvisí především se skutečností, že v ČR působí několik set německých podniků, které jsou přímo napojeny

na mateřské hospodářství a vyvíjejí se s ním téměř souběžně. Pro podstatnou část českých vývozů do Německa platí, že jejich hlavními aktéry jsou zahraniční firmy se sídlem v ČR. Aktivity těchto firem přispívají značnou měrou k vysokém podílu Německa na českých vývozech. Pokud jde o názor, že je nutno závislost na Německu snížit, je nutno si uvědomit, že exporty zahraničních firem jsou z hlediska českého hospodářství tou nejsnazší a nejlacinější cestou, jak se na německý trh dostat. Důležitost těchto firem v českém zahraničním obchodě však zvyšuje riziko negativního vývoje, pokud by tyto firmy ČR opustily, což lze učinit poměrně snadno. Pro české exportéry je důležité, v jaké pozici se v Německu nacházejí. Vedle firem, které se prosadily konkurenceschopnými finálními výrobky, existuje řada podniků, které jsou integrovány do výrobních procesů v roli subdodavatelů. Kvalitní subdodavatel může mít velmi silné postavení. Příkladem jsou vývozci součástí pro motorová vozidla, kteří jsou nepostradatelnou složkou výrobních struktur. Hodnota jejich exportů přesahuje objem vývozu automobilů. Stabilizace jejich pozice na německém trhu by měla být jedním z cílů podpory exportu. Statistické údaje o vývoji exportů v období krize ukazují, že robustní německá ekonomika stabilizovala v době světového hospodářského útlumu české vývozy, a to mnohem účinněji než tomu bylo v případě prioritních a zájmových zemích. Nelze očekávat, že se hospodářské turbulence nebudou opakovat. Pokud by se zahraniční podniky rozhodly zemi opustit, došlo by i ke snížení objemu českého exportu do Německa. Bez zahraničních firem do Německa směřuje pouze desetina celkových exportů.

Automobilový průmysl tvoří téměř čtvrtinu českého exportu a sedm procent HDP. V oboru pracuje kolem 150 tis. osob. Výrazná návaznost na jedno odvětví může představovat vážné ohrožení pro českou ekonomiku. Automobilový průmysl by se podle expertů mohl dostat do problémů v případě, že klesne poptávka. Pokud by v době krize poptávka klesla, český trh zpomalí. Klesne nejen výroba a zaměstnanost, ale následně i spotřeba domácností, což pocítí firmy i z jiných oborů. Obavy jsou především z velké nasycenosti trhu s automobily v eurozóně. Analytici předpokládají, že dříve nebo později nepochybně dojde k útlumu poptávky, což může být cyklický jev, stejně jako vyvolaný nějakou další krizí. Českým výrobcům v automobilovém průmyslu však díky nízkým mzdovým nákladům, vysoké kvalifikaci části zaměstnanců, moderním výrobním provozům, špičkovým vývojovým pracovištím a příznivé geografické poloze zatím nehrozí. Stejně tak nejspíše ze dne na den nepřijde žádný šok. Nutno uvést, že pokud se hovoří o snižování závislosti na automobilovém průmyslu, musí se přijít s nabídkou nějaké jiné alternativy. V současné chvíli však žádná taková, která by mohla kompenzovat sílu automobilového průmyslu, neexistuje. V budoucnu by jí mohlo být např. strojírenství – od energetiky až po výrobu zdravotnických přístrojů.

Přibližně 98 % průmyslových podnikatelských subjektů je pod domácí kontrolou. Je ovšem třeba zmínit, že v celkovém počtu je obrovské množství malých podniků včetně podnikatelů – fyzických osob. Zahraniční investoři jsou významní především ve větších podnicích, jejichž ekonomický význam přesahuje jejich počet. Podle Českého statistického úřadu dosahují podniky pod zahraniční kontrolou v průmyslu cca 60 % celkových tržeb. Přidaná hodnota vytvořená těmito podniky, která signalizuje význam z hlediska ekonomického výkonu, dosahuje 500 mld. Kč, což je zhruba polovina průmyslu celkem. Podniky pod zahraniční kontrolou hrají nejvýznamnější roli ve výrobě motorových vozidel. Vlastnictví některých klíčových průmyslových firem zahraničním majitelem však může rovněž znamenat bezpečnostní riziko, pokud by tyto osoby konaly v zájmu cizí moci.

Významné riziko pro český průmysl pak mohou představovat vlivové a infiltrační operace zpravodajských služeb cizí moci namířené proti strategickým hospodářským zájmům ČR, průmyslová a vědecko-technická špionáž. V případě státem vlastněných či spoluvlastněných společností se obrana proti takovému jednání odvíjí především od náležitého výkonu jeho vlastnických práv. Zejména u akciových společností s podílem soukromých subjektů je však s ohledem na právní rámec často obtížné v jejich rozhodovacích procesech dostatečně zohlednit bezpečnostní zájmy státu. Významnou příležitostí a výzvou související s hledáním oborových příležitostí odbytu průmyslových komodit bude v příštích letech i realizace procesů spojených s rozvojem digitálního trhu včetně Průmyslu 4.0, čtvrté průmyslové revoluce, založené na komplexním systému změn v řadě činností, a

to nejen v průmyslové výrobě. Průmysl 4.0 transformuje výrobu ze samostatných automatizovaných jednotek na plně automatizovaná a průběžně optimalizovaná výrobní prostředí. Vertikální výrobní procesy budou horizontálně propojeny v rámci firemních systémů, které budou v reálném čase pružně reagovat na okamžitou a měnící se poptávku po produktech. Jednou z příležitostí je i vytvoření předpokladů pro duální roli Průmyslu 4.0, tj. podporu moderní průmyslové výroby v ČR, ale i exportu řešení či výsledků výzkumu na světové trhy. Zde se rovněž uplatní využití digitálních technologií v dalších sektorech hospodářství.

Konkurenceschopný obranný a bezpečnostní průmysl je jedním z předpokladů pro zajištění podstatných bezpečnostních zájmů ČR a rozvoje a udržení národních obranných schopností.

Faktorem důležitým pro udržení, resp. zvyšování konkurenceschopnosti obranného a bezpečnostního průmyslu je předvídatelný zdrojový rámec pro oblast obrany, což je zásadní předpoklad nejen pro efektivní fungování ozbrojených sil ČR, ale je i důležitým faktorem právě ve vztahu k českému obrannému a bezpečnostnímu průmyslu. Stabilní rozpočtové prostředí umožňuje střednědobé a dlouhodobé plánování ze strany Armády ČR, a tím dává obrannému a bezpečnostnímu průmyslu možnost na stanovené cíle adekvátně reagovat a v dostatečném časovém předstihu se v oblasti výzkumu a vývoje na jejich naplňování připravit. Jsou tak zesilovány vazby mezi českým obranným a bezpečnostním průmyslem a armádou, jakožto referenčním zákazníkem. Rozhodnutí postupně navyšovat rozpočet MO ve střednědobém horizontu tak, aby mohl v roce 2020 dosáhnout 1,4 % HDP (BS 2015), tak dává obrannému a bezpečnostnímu průmyslu jistou míru perspektivy.

Dalším důležitým faktorem je diverzifikace produkce. Důsledky hospodářských krizí se v oblasti obranného a bezpečnostního průmyslu projevují se zpožděním oproti civilním sektorům. Důvodem je fakt, že odběrateli vojenského materiálu jsou většinou státní subjekty a peníze na zbrojní nákupy tedy pocházejí ze státních rozpočtů, které jsou sestavovány na období jednoho roku, a tudíž nereagují (omezováním rozpočtů na nákup vojenské techniky) na krizi okamžitě. Negativní následky krizí podniky obranného a bezpečnostního průmyslu omezují či zcela eliminují proticyklickou diverzifikací svého výrobního portfolia mezi vojenskou, duální a civilní produkcí a taktéž regionální diverzifikací odbytového zaměření.

Pro české výrobce/vývozce je v současné době největším problémem nedostatek zaměstnanců s technickým vzděláním. Kvůli tomu pravděpodobně poroste export letos pomaleji, což může vést i ke zpomalení české ekonomiky. Nedostatek lidí může odrazovat zahraniční investory. Zaměstnavatelé v průmyslu se potýkají s nedostatkem kvalifikovaných pracovníků některých technických profesí. Kromě nových investorů může ČR přicházet i o ty současné. Pro nové investory nebo při úvahách o rozšiřování výroby stávajících firem je hledání nových zaměstnanců překážkou, která je může nasměrovat do jiné země. Disproporce mezi počtem odborníků odcházejících do důchodu v nebližších letech a množstvím kvalitních absolventů klíčových oborů středních a vysokých škol by mohla způsobit problémy jak s případným přísunem zahraničních investic, tak v provozu zavedených firem. Z tohoto důvodu je třeba problematiku technického vzdělávání všemi zainteresovanými stranami společně řešit.

Svaz průmyslu a dopravy ČR uvádí, že v průmyslu chybí nejméně 100 tisíc technicky vzdělaných pracovníků. Zároveň v odvětvích jako je strojírenství či automobilový průmysl odejde do roku 2020 kolem 60 tisíc technicky vzdělaných pracovníků do důchodu. Částečně by problém s nedostatkem odborných pracovníků mohli vyřešit cizinci. Spolupráce by se mohla rozvíjet hlavně v zemích východní Evropy. Najmout zaměstnance ze „třetích zemí“ je ale pro firmy administrativně náročné a trvá to v průměru jeden rok.

Zásadním krokem pro zlepšení kvality a atraktivity technických oborů je spolupráce škol a firem, především co největší množství praktické výuky přímo v reálném firemním prostředí. Z tohoto důvodu došlo v roce 2013 ke změně zákona o daních z příjmů a zaměstnavatelé spolupracující se školami mohou od 1. ledna 2014 uplatňovat daňová zvýhodnění na investice do vybavení k výuce a samotnou výuku žáků a studentů na pracovišti.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Odpovědné instituce: MPO, CzechTrade, CzechInvest, MZV

Základní nástroje (strategie, koncepce EU): Dohody o volném obchodu mezi EU a jejími členskými státy na jedné straně a ostatními státy na straně druhé

Základní nástroje (strategie, koncepce ČR: Exportní strategie ČR pro období 2012 až 2020, Národní inovační strategie, Koncepce zahraniční politiky, Strategický rámec udržitelného rozvoje ČR, Strategie mezinárodní konkurenceschopnosti ČR pro období 2012 – 2020, Akční plán na podporu hospodářského růstu a zaměstnanosti, Akční plán pro rozvoj digitálního trhu, Mapa globálních oborových příležitostí

C. SWOT analýza

Silné stránky

- ČR je nejprůmyslovější zemí EU.
- Moderní výrobní provozy.
- Špičková výzkumná a vývojová pracoviště.
- Vysoká kvalifikace části pracovníků.
- Příznivá geografická poloha.

Slabé stránky

- Nedostatek kvalifikovaných pracovníků některých technických profesí.

Příležitosti

- Udržení postavení ČR v tradičních průmyslových odvětvích.
- Získání vedoucí pozice v nových průmyslových oborech.
- Zajištění diverzifikace zahraničních odbytišť české průmyslové produkce.
- Zajištění zdrojového rámce pro oblast obrany ve výši 1,4 % HDP.

Hrozby

- Výrazná návaznost na jedno průmyslové odvětví – riziko poklesu poptávky po výrobcích automobilového průmyslu.
- Nedostatečná diverzifikace vývozu průmyslové produkce.
- Významná role zahraničních investorů ve větších podnicích.

- Odliv zahraničních investic v důsledku nedostatku kvalifikovaných pracovníků v technických profesích.

D. Doporučení k posílení odolnosti:

1. Realizovat pobídky do oborů s vysokou přidanou hodnotou a do regionů s vysokou nezaměstnaností.
2. Vytvářet nová pracovní místa a podporovat růst firem zvýšením obchodu a internacionalizací podnikání, posilovat prestiž ČR ve světě a v mezinárodních organizacích, využívat globální obchodní příležitosti pro růst prosperity ČR.
3. Spolupracovat při zajišťování českých oficiálních účastí na veletrzích a výstavách v zahraničí s oborovými asociacemi, Veletržním výborem při Svazu průmyslu, českými zastupitelskými úřady a jejich ekonomickými úseky v zahraničí, agenturami CzechTrade a CzechInvest včetně jejich zahraničních kanceláří.
4. Realizovat opatření pro zlepšení kvality a atraktivity technických oborů středních i vysokých škol a zvýšit investice do systému vzdělávání.
5. Vytvořit podmínky pro příjem zahraničních středoškolsky a vysokoškolsky technicky vzdělaných pracovníků.

HYBRIDNÍ HROZBY A JEJICH VLIV NA BEZPEČNOST OBČANŮ ČR

A. Popis a evaluace hrozby a rizik z ní vyplývajících pro ČR

1. Úvod

Reálie mezinárodní politiky 21. století odhalují rozsah, v němž jsou při vedení konfliktu uplatňovány nástroje z celého spektra dimenzí moci známého pod zkratkou DIMEFIL[82]. Řada státních i nestátních aktérů se snaží svých politických cílů dosáhnout pomocí otevřených i skrytých aktivit koordinovaných v rámci celé škály nástrojů moci, bez ohledu na případnou kolizi s mezinárodním řádem založeným na pravidlech. Právě v tomto kontextu se objevil pojem hybridní hrozby, respektive hybridního válčení. Kapitola zastřešuje řadu hrozeb z dalších kapitol, zejména Působení cizí moci, Hrozby v kyberprostoru, Energetická, surovinová a průmyslová bezpečnost, Terorismus a zčásti i Bezpečnostní aspekty migrace a Extremismus. Hrozby uvedené v těchto kapitolách mohou a nemusí být součástí koordinované kampaně. Proto se témata v těchto kapitolách do různé míry překrývají s touto kapitolou, která má ambici překryv koordinovat.

Již elementární vymezení „hybridní hrozby" ukazuje na skutečnost, že ji nelze pojímat v podobném smyslu, v jakém nahlížíme většinu ostatních hrozeb, kdy každá představuje ohrožení více méně jen v jedné dimenzi. To, co rozumíme pod hybridní hrozbou, je primárně metoda, způsob, jakým je vedena konfrontace, respektive konflikt. Tento způsob vedení konfliktu představuje širokou, komplexní, přizpůsobivou a integrovanou kombinaci konvenčních a nekonvenčních prostředků, otevřených a skrytých aktivit, majících primárně charakter nátlaku a podvratné činnosti, které jsou prováděny vojenskými, polovojenskými a různými civilními aktéry.[83]

Úkolem hybridní kampaně je využít slabin protivníka; maskovat se sledováním legitimních cílů; znemožnit jasnou interpretaci událostí a odhalení jejich vzájemné souvislosti; komplikovat či přímo znemožnit identifikaci původce a zastřít jeho úmysly; komplikovat, destabilizovat či přímo paralyzovat rozhodovací proces, a tím znemožnit včasnou a účinnou reakci ze strany napadeného. Hybridní útočník osnuje a provádí aktivity poškozující životní, strategické či obecně bezpečnostní zájmy jiného aktéra a přitom usiluje o vytvoření prostředí, kdy mu za tyto aktivity nelze (přinejmenším formálně) jednoznačně přiřknout odpovědnost, nebo tak lze učinit pouze velmi obtížně a spekulativně (viz koncept hodnověrného popření – „plausible deniability"). Hybridní útočník se bude snažit udržovat své aktivity pod prahem, jehož překročení by mezinárodní společenství považovalo za ozbrojenou agresi. Přímé vojenské konfrontaci se patrně bude snažit vyhnout, ovšem je nutné předpokládat, že do hybridní kampaně v nějaké podobě zakomponuje i použití vojenských prostředků.

Hybridní strategie mohou uplatnit státní stejně jako nestátní aktéři, a to různými modely napadení, které se mohou významně lišit stupněm své rozvinutosti a integrace.

---

[82] Diplomatic/Political, Information, Military, Economic, Financial, Intelligence, Legal.

[83] Pojmy hybridní válčení, hybridní způsob vedení konfliktu, hybridní kampaň nebo hybridní strategie je v podstatě možné chápat jako synonyma. V zájmu co nejvýstižnějšího a zároveň úsporného vyjádření všech těchto pojmů bude v dalším textu používán především výraz „hybridní kampaň". Kapitolou použité vymezení hybridní kampaně vychází zejména ze „Strategie pro úlohu NATO v boji proti hybridnímu válčení" z roku 2015.

Hybridní kampaň může propojovat řadu klasických nástrojů z již zmíněného spektra sfér vlivu, resp. dimenzí moci – DIMEFIL:

D) diplomacie/politika – uplatnění vlivu a vyvíjení nátlaku ústy a činy oficiální politické reprezentace;

I) informace – sdělovací prostředky, sociální sítě a jiné prostředky šíření informací, jejich manipulativní využití, dezinformační kampaň a propaganda;

M) ozbrojené síly – může jít o otevřené použití jako výhružka (demonstrace vojenské přítomnosti a pohotovosti) či přímo bojové použití nebo o různé formy skrytého nasazení jednotlivců, malých skupin a infiltrace napadeného státu s jejich využitím;

E) ekonomika – různé formy nátlaku ekonomické povahy (uvalení cla, embarga, odepření dodávek surovin či energie, zákaz používání dopravní nebo přepravní cesty, destabilizace klíčových odvětví, podniků apod.);

F) finančnictví – destabilizace měny, trhu s akciemi a dluhopisy, bankovního sektoru, ovlivňování klíčových finančních institucí;

I) zpravodajství – aktivity zpravodajských služeb, špionáž, získávaní spolupracovníků (zejména státních či politických činitelů) k protistátní činnosti;

L) veřejný pořádek a právní stát – využití různých rozvratných činností útočících na hodnotové, právní a další aspekty společenského uspořádání, např. podněcování nepokojů v napadené zemi s využitím etnických, náboženských či sociálních dělících linií ve společnosti, nebo použití široké škály teroristických útoků a dalších typicky kriminálních metod (např. únosy, vydírání a zastrašování).

Specifické postavení ve vztahu k výše uvedeným nástrojům má kybernetický prostor – představuje prostředí, kde se jednotlivé dimenze moci prolínají, a jeho význam pro fungování států a ekonomik je kritický. Kybernetické útoky umožňují zasáhnout a ohrozit fungování veřejné správy, kritické infrastruktury (dodávky elektřiny apod.), finančního sektoru, mohou ohrozit bezpečnost důležitých objektů, jsou prostředkem špionáže, dezinformační kampaně atd.

Samy o sobě nepředstavují hybridní metody vedení konfliktu v historii nic nového. Za novum však lze považovat rozsah a způsob, jak je škála výše uvedených nástrojů kombinována a koherentně použita k dosažení strategického cíle.

Jednotlivé prvky hybridní kampaně nemusí být nutně nezákonné či představovat hrozbu samy o sobě; nebezpečí spočívá právě v jejich sofistikované kombinaci, která současně usiluje o zastření pravého účelu jejích jednotlivých komponentů.

Rozvinutý model hybridní kampaně předvedla Ruská federace v konfliktu s Ukrajinou, jehož jedním vrcholem byla anexe Krymu v roce 2014, a druhou větví je snaha o zmrazení konfliktu ve východní části Ukrajiny. Ruská federace vede svou kampaň všemi metodami a formami nátlaku s velmi vysokou mírou koordinace a v dlouhodobém horizontu. Nelze ani odhlédnout od skutečnosti, že Ruská federace je jadernou mocností. Také metody boje teroristické organizace tzv. Islámský stát mají hybridní povahu, i když spektrum používaných nástrojů není tak široké. K těm hlavním patří propaganda prostřednictvím sociálních médií, manipulace s fakty a dezinformace, manifestace ozbrojené síly v kombinaci s využíváním podzemních sítí přívrženců a následovníků, boj asymetrickými prostředky, kybernetické útoky, zastrašování pomocí teroristických útoků apod. Manipulativní použití informací či multimediální působení je v případě tzv. Islámského státu výrazně sofistikovaněji používaným nástrojem než klasické vojenské zbraně. I o hybridním válčení však zcela jistě platí, že v konkrétních konfliktech nepochybně budou aplikovány různé a svému specifickému cíli přizpůsobené hybridní kampaně.

2. Identifikace rizik

Principiální riziko, kterému je vystaven subjekt napadený hybridní kampaní, spočívá v tom, že hybridní kampaň nebude schopen včas, v plném rozsahu či vůbec rozpoznat. Pokud nebude včas rozpoznán původce hybridní kampaně, šíře jeho metod ani jeho cíle, reakce nebude adekvátní, což se odrazí i na míře její úspěšnosti. Proto základním nástrojem bezpečnostního systému pro boj s hybridní kampaní je schopnost získávání informací a jejich vyhodnocení k identifikaci hybridní kampaně a jejího strůjce.

Další rizika je možné identifikovat na základě konkrétní kombinace nástrojů a metod, které při hybridní kampani mohou být použity, a jejich specifického zacílení. V tomto smyslu může ČR čelit nepřátelským akcím, které budou zacíleny proti třem základním zájmům, resp. pilířům státu:

a) Soudržná společnost a její ztotožnění se s ideově-hodnotovým zakotvením státu

Součástí hybridní kampaně může být ovlivňování politických struktur a politického rozhodovacího procesu, soudů, policie, ozbrojených sil, sdělovacích prostředků a veřejného mínění, usilující ve výsledku o destabilizaci či štěpení společnosti a podlomení důvěry obyvatelstva ve své ideově-politické uspořádání (demokratické zřízení, právní stát, garance základních lidských práv a svobod, garance politických a sociálních práv – jinými slovy ústavní liberalismus, a tomu odpovídající zahraničně politická orientace ČR vyjádřená např. členstvím v EU, NATO a dalších organizacích). Specifickým terčem hybridního působení by mohla být i vůle politické reprezentace a obyvatelstva splnit spojenecký závazek ČR ke kolektivní obraně ve prospěch jiného státu NATO, vystaveného zjevnému ohrožení, popřípadě poskytnout obdobnou vzájemnou asistenci členským státům EU.

Tento druh působení směřuje zejména proti následujícím zájmům ČR uvedeným v BS 2015:

- posilování soudržnosti a efektivnosti NATO a EU a zachování funkční a věrohodné transatlantické vazby;
- podpora demokracie, základních svobod a principů právního státu;
- vytváření podmínek pro tolerantní občanskou společnost, potlačování extremismu a jeho příčin;
- posilování veřejné informovanosti a aktivního podílu občanů na zajištění bezpečnosti.

Pravděpodobnost konfrontace s tímto typem aktivit je ve srovnání s ostatními metodami hybridní kampaně, které hypoteticky přicházejí v úvahu, relativně vysoká. Česká společnost je však homogenní etnicky, sociálně, i pokud jde o její základní hodnotovou orientaci. Součástí této orientace je i obecně nižší míra zájmu o politiku a nižší míra angažovanosti ve veřejných záležitostech. Celkové riziko vyplývající ze zaměření potenciální hybridní kampaně na destabilizaci společnosti s využitím jejích vnitřních dělících linií lze hodnotit jako **střední**.

b) Fungující ekonomika

Dílčím cílem hybridní kampaně může být poškození a destabilizace ekonomické základny státu, např. přerušením dodávek strategických surovin a energií, bojkotem českého vývozu apod. Specifickým problémem, který snižuje odolnost ekonomiky vůči snahám o její destabilizaci, je často nejasná struktura vlastnických vazeb v řadě významných odvětví.

Takové aktivity by poškozovaly zejména tyto dva strategické zájmy ČR:

- zajištění ekonomické bezpečnosti ČR a posilování konkurenceschopnosti ekonomiky;

- zajištění energetické, surovinové a potravinové bezpečnosti ČR a adekvátní úrovně strategických rezerv.

Pravděpodobnost protivníkova zaměření na poškození ekonomiky je relativně vysoká, neboť česká ekonomika je velmi otevřená a tedy vysoce náchylná reagovat na (negativní) podněty zvenčí. Vyšší riziko je identifikováno v zajištění energetických potřeb státu, neboť vlastní energetické suroviny ČR jsou omezené a ekonomika ve velké míře závisí na jejich dovozu. Zdroje dodávek přitom nejsou dostatečně diverzifikované. Pravděpodobnost, že k pokusu o poškození ekonomiky budou využiti vlastníci významných hospodářských subjektů spříznění s hybridním útočníkem, je relativně nízká. Důsledky takto organizovaných zásahů by zřejmě po určitou dobu byly závažné, ovšem silná integrace české ekonomiky v rámci EU nabízí možnosti rychlého zotavení. V tomto případě proto lze riziko hodnotit jako relativně **nízké**.

c) Bezpečnost a obrana

Nástrojem hybridní kampaně může být mobilizace zájmových – nábožensky, etnicky, národnostně či jazykově definovaných – či kriminálních skupin k protistátní činnosti a narušování veřejného pořádku. V tomto kontextu můžeme pro ilustraci poukázat na pojem „páté kolony“ nebo na tzv. Karaganovovu doktrínu (využití etnických menšin v zahraničí jako záminky pro vměšování se pod zástěrkou ochrany jejich práv). Specifickou variantou tohoto postupu může být snaha působit přímo na příslušníky ozbrojených sil, policie a dalších bezpečnostních složek s cílem využít potenciálních/latentních tendencí k extremismu a oslabit tak akceschopnost těchto složek. Někteří příslušníci bezpečnostních složek v minulosti již projevili sklony k extremismu. S tím souvisí i angažovanost bývalých profesionálních vojáků a policistů v nestátních polovojenských uskupeních. To je fenomén, kterému je i nadále zapotřebí věnovat pozornost.

Bezpečnost ČR může být ohrožena i otevřeným či skrytým použitím ozbrojených sil, namířeným např. proti vojenskému angažmá ČR v rámci operací či jiných úkolů NATO a EU, nebo agresivním nasazením zpravodajských služeb či speciálních sil jiných států na území ČR.

Tyto aktivity by při určitém stupni eskalace mohly ohrozit přímo životní zájmy ČR. Dále směřují zejména proti těmto strategickým a dalším významným zájmům:

- bezpečnost a stabilita, především v euroatlantickém prostoru;
- zajištění vnitřní bezpečnosti a ochrany obyvatelstva;
- zajištění kybernetické bezpečnosti a obrany ČR;
- snižování kriminality s důrazem na hospodářskou kriminalitu, organizovaný zločin, kybernetickou kriminalitu a boj s korupcí;
- vytváření podmínek pro tolerantní občanskou společnost, potlačování extremismu a jeho příčin.

Pravděpodobnost masivního vojenského ohrožení území ČR je velmi nízká. V úvahu je však nutné brát skutečnost, že některé členské země NATO čelí hmatatelnějšímu ohrožení než ČR, a to může klást požadavky na solidární zapojení ČR v zájmu zajištění jejich bezpečnosti. Možnost ohrožení ozbrojených sil působících v operacích mimo území ČR je vysoká a přímo koresponduje s charakterem každého konkrétního nasazení. Při zapojení do operací stabilizačního typu s nižší intenzitou (které byly dominantním typem angažmá ozbrojených sil ČR v posledních cca 20 letech) mají ozbrojené síly ČR dostatečné schopnosti a kapacity, aby nebyly vystaveny nepřiměřenému riziku.

Riziko spíše střední závažnosti by vyplývalo z reálného stavu ozbrojených sil ČR z hlediska jejich personální a materiální naplněnosti a pohotovosti v případě potřeby jejich použití v náročnějších scénářích jako např. kolektivní odstrašení či kolektivní obrana v rámci NATO proti konvenčně silnému

protivníkovi nebo rozsáhlé posílení bezpečnostních složek na území ČR k zachování veřejného pořádku a bezpečnosti.

B. Odpovědné instituce v rámci bezpečnostního systému ČR a základní nástroje (legislativa, strategie, koncepce) pro eliminaci hrozeb a rizik

Následující text reflektuje skutečnost, že jednotlivé nástroje a metody využitelné hybridní kampaní a opatření proti nim jsou primárně předmětem téměř všech ostatních kapitol Auditu. Tato kapitola se proto zaměřuje na samotnou podstatu hybridní kampaně, tedy komplikování rozhodovacího procesu do té míry, kdy není schopen přijímat účinná protiopatření. Taková situace může nastat, pokud jednotlivé komponenty hybridního působení jsou řešeny individuálně a bez odhalení jejich vzájemné souvislosti.

Je velmi nepravděpodobné, že by ČR čelila rozvinuté hybridní kampani osamoceně. Podobně tuto hrozbu vnímají NATO a EU, a rozvíjejí proto své schopnosti, jak čelit hybridní kampani. Obě organizace jako řídící princip uznávají primární odpovědnost členských států a svou roli vidí jako podpůrnou. NATO svůj přístup definovalo ve „Strategii pro úlohu NATO v boji proti hybridnímu válčení“[84] a v doplňujících dokumentech z oblasti civilní připravenosti.[85] Přístup EU vyjadřuje společné sdělení Evropské komise a Vysoké představitelky pro zahraniční a bezpečnostní politiku „Společný rámec pro boj proti hybridním hrozbám: Reakce EU“.[86] Přístup, úloha a schopnosti obou organizací jsou do značné míry komplementární, proto je žádoucí jejich úsilí provázat a zvýšit tak jejich efektivitu. Obě organizace připravily svůj „manuál“ pro vzájemnou spolupráci a koordinaci v rámci odpovědi na hybridní útok.[87] ČR by měla aktivně přispívat k formování přístupu NATO a EU, jejich relevantní výstupy zohledňovat ve vlastním národním přístupu, být připravena pomoci zemím NATO a EU v případě jejich napadení, i připravena přijmout podporu, pokud by se sama stala terčem hybridní kampaně.

Odpovědné instituce jsou identifikovány na pozadí tří základních zájmů, respektive pilířů státu, proti nimž může hybridní kampaň působit.

Působení proti soudržnosti a ideově-hodnotovému zakotvení společnosti

Při reakci na tento druh působení protivníka sehrává důležitou úlohu celá politická reprezentace (parlament) a sebe-organizující se občanská společnost. Pokud však hovoříme v užším smyslu o bezpečnostním systému ČR, pak odpovědnou institucí je vláda.

Jádrem reakce proti této části spektra hybridní kampaně je věrohodně koncipovaná a realizovaná strategická komunikace státu (vlády) jednak vůči svému obyvatelstvu a jednak vůči protivníkovi. Jejím úkolem ve vztahu k vlastní společnosti je posilování její odolnosti a ujištění o připravenosti státu zajistit její bezpečnost. Odolnost společnosti stojí na sdílení stejných (základních) hodnot i vůle je chránit, na občanském uvědomění a solidaritě; rozvíjení dobrého vládnutí a odstraňování vnitřních

[84] Strategy on NATO’s Role in Countering Hybrid Warfare, PO (2015)0673, 1. 12. 2015.
[85] Report on the State of Civil Preparedness, PO (2016)0057, 5. 2. 2016 a další.
[86] Joint Communication to the European Parliament and the Council “Joint Framework on countering hybrid threats: a European Union response”, JOIN (2016) 18 final, 6. 4. 2016.
[87] NATO-EU Staff to Staff Hybrid Cooperation Playbook, DPRC-N (2016)0045, 11. 5. 2016; Joint Staff Working Document – EU operational protocol for countering hybrid threats – 'EU Playbook', SWD (2016) 227 final, 7. 7. 2016.

tenzí zvyšuje odolnost společnosti. Posilování této odolnosti je předmětem dlouhodobé společenské a politické diskuse a praxe a také vzdělávání. Vzhledem k tomu je poměrně složité pokoušet se zde hledat prostor pro uplatnění nějakých specifických nástrojů k zajištění bezpečnosti. Ve vztahu k protivníkovi je úkolem strategické komunikace vlády demonstrovat připravenost, schopnost a odhodlání bránit sebe i spojence, a odstrašit tak protivníka od jeho agresivních záměrů. Strategickou komunikaci vlády musí podporovat i další relevantní orgány/úřady podle povahy ohrožení – Ministerstvo zahraničních věcí, vnitra, obrany, průmyslu atd. Použití propagandy a dezinformací jako součásti hybridní kampaně je třeba vnímat v kontextu ostatních událostí, které – potenciálně i aktuálně – poškozují zájmy a bezpečnost státu a obyvatelstva, a zkoumat jejich potenciální vazbu. Kanály, respektive obecně informační prostor, které propaganda a dezinformační kampaně využívají, je třeba sledovat a vyhodnocovat nepřetržitě. Boj proti nepřátelské propagandě řeší podrobněji kapitola „Působení cizí moci“.

Do této oblasti působení hybridní kampaně je třeba zahrnout i aktivity zaměřené na ovlivnění politických struktur a politického rozhodovacího procesu, soudů, policie, ozbrojených sil a dalších státních/veřejných institucí – jinými slovy útok proti fungování státu. Instituce, které těmto aktivitám mohou efektivně čelit, jsou obecně orgány vyšetřující (závažnou) trestnou činnost, typicky korupci, a také zpravodajské služby.

Působení proti fungující ekonomice

I v této oblasti zacílení hybridní kampaně je účelnější odkázat na identifikaci rizik a přehled institucí a jejich dostupných nástrojů obsažené v kapitolách „Energetická, surovinová a průmyslová bezpečnost“ či „Stabilita měny a finančních institucí“. Budou-li některé formy ekonomického nátlaku či podkopávání ekonomiky využity jako součást hybridní kampaně, je velice pravděpodobné, že i metody k boji proti nim budou mít povahu regulačních, respektive restriktivních a preskriptivních opatření dotýkajících se fungování trhů, obchodní výměny, zajištění surovin a chodu průmyslu. Bezpečnostní systém však musí být schopen odhalit potenciální souvislost událostí poškozujících ekonomiku s jinými aktivitami namířenými proti zájmům ČR.

Působení proti bezpečnosti státu a občanů

Mezi institucemi odpovědnými za řešení této oblasti zacílení hybridní kampaně mají prvotní roli instituce získávající informace (dále také jen „zpravodajské služby“):

- BIS,
- ÚZSI,
- VZ.

Specifickou, průřezovou úlohu mají orgány kybernetické bezpečnosti:

- NBÚ se svými podřízenými prvky,
- síť pracovišť typu CERT (Computer Emergency Response Team),
- Národní centrum kybernetických sil vytvářené u VZ.

K institucím, které mají hlavní výkonné pravomoci a nástroje, patří:

- MV,
- orgány vnitřní bezpečnosti a ochrany obyvatelstva,
- ozbrojené síly ČR.

Nepochybně i další instituce mohou přispívat k zajištění bezpečnosti a obrany, zejména získáváním informací, např. Ministerstvo zahraničních věcí. Celkovou odpovědnost a koordinační roli má vláda. Nejvýznamnější rozhodnutí v záležitostech obrany státu svěřuje Ústava Parlamentu ČR.

Odpovědné instituce, jejich nástroje a kapacity

Zpravodajské služby

Základním posláním BIS, ÚZSI a VZ je získávání informací a jejich vyhodnocování s cílem odhalit ohrožení zájmů a bezpečnosti státu a obyvatelstva. Tato činnost probíhá neustále. V případě potřeby zvýšit intenzitu zpravodajské činnosti při identifikaci zvýšených aktivit proti bezpečnosti státu a obyvatelstva může vláda kapacity zpravodajských služeb posílit. Činnost zpravodajských služeb je v současnosti vymezena zákonem č. 153/1994 Sb., o zpravodajských službách ČR, zákonem č. 154/1994 Sb., o bezpečnostní informační službě a zákonem č. 289/2005 Sb., o Vojenském zpravodajství.

Klíčovým příspěvkem k odhalení hybridní kampaně je kontinuální získávání informací zpravodajskými službami v rámci jejich zákonné působnosti a jejich sdílení. To umožňuje vzájemnou konfrontaci informací a odhalení případné souvislosti různých aktivit, které jsou součástí jedné hybridní kampaně. Spektrum relevantních informací je velmi široké – zahrnuje události s negativním dopadem na ekonomiku státu a fungování klíčových odvětví či podniků, aktivity ideově a zájmově definovaných skupin, charakter kybernetických bezpečnostních incidentů apod. Činnost zpravodajských služeb obnáší zejména získávání přehledu o situaci. Současná zákonná úprava jim neumožňuje aktivní zapojení do preventivních a reaktivních opatření k zajištění bezpečnosti státu.

Orgány kybernetické bezpečnosti

Národní bezpečnostní úřad (NBÚ) je od roku 2011 gestorem kybernetické bezpečnosti. Zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, byl oficiálně pověřen výkonem státní správy v oblasti kybernetické bezpečnosti. Aktuální Národní strategie kybernetické bezpečnosti ČR nastavuje základní přístupy, nástroje a úkoly relevantních institucí, zohledňuje i nadnárodní dimenzi kybernetických hrozeb. Role NBÚ ve vztahu k působení hybridní kampaně spočívá především v zajišťování kybernetické bezpečnosti, bránění konkrétním kybernetickým útokům a zvyšování odolnosti české informační infrastruktury. K tomuto účelu funguje v rámci NBÚ vrcholové pracoviště typu CERT (Computer Emergency Response Team) – vládní CERT GovCERT.CZ. Obdobnou činnost vyvíjejí i další týmy CERT fungující u jiných institucí.

Národní centrum kybernetických sil (NCKS) se nachází ve stadiu výstavby k získání schopností provádět široké spektrum operací v kyberprostoru nezbytných k zajištění kybernetické obrany ČR.

NBÚ může svými kapacitami napomáhat zejména Policii ČR při odhalování a vyšetřování kybernetických útoků. NBÚ může díky dobře nastavené spolupráci se zpravodajskými službami, Policií ČR a dalšími institucemi napomáhat s identifikací odpovědnosti za závažné kybernetické útoky. Personální kapacity NBÚ pro tyto aktivity jsou však omezené. Bližší posouzení dostatečnosti existujících kapacit pro komplexní řešení rozsáhlých kybernetických útoků v rámci intenzivnější hybridní kampaně je velmi obtížné, neboť záleží i na možnostech koordinace činnosti jednotlivých CERT týmů, obecně je však třeba doporučit jejich posílení. Podrobněji se touto problematikou zabývá kapitola „Hrozby v kyberprostoru“.

MV, orgány vnitřní bezpečnosti a ochrany obyvatelstva

MV má z kompetenčního zákona č. 2/1969 Sb., celou řadu gescí, které ho činí odpovědným ústředním správním úřadem k řešení působení primárně nevojenských nástrojů hybridní kampaně. Do jeho působnosti patří zajišťování veřejného pořádku, vnitřní bezpečnosti, ochrana obyvatelstva a další agendy vnitřní správy státu.

Podrobněji se úkolům a nástrojům MV a Policie ČR v těchto agendách věnují kapitoly „Terorismus“, „Extremismus“, „Bezpečnostní aspekty migrace“, „Organizovaný zločin“ či „Působení cizí moci“. Ty také souhrnně popisují příspěvek, jímž by MV a Policie ČR přispěly k reakci na hybridní kampaň, pokud by její součástí byly např. právě teroristické akce, aktivity extremistických skupin, využití neřízené migrace nebo skupin organizovaného zločinu.

Zapojení základních a ostatních složek integrovaného záchranného systému (IZS) do řešení mimořádných událostí a krizových situací by probíhalo prostřednictvím IZS, jehož koordinací je pověřen Hasičský záchranný sbor ČR. Typové činnosti složek IZS jsou připraveny například pro případ použití špinavé bomby, hrozby použití nebo nálezu nástražného výbušného systému, chemického útoku v metru, útoku aktivního střelce, atd. Kapacitám a schopnostem HZS ČR a IZS se věnují kapitoly „Přírodní hrozby“ a „Antropogenní hrozby“.

V případě hybridní kampaně zacílené specificky proti ČR musí být bezpečnostní systém připraven i na potřebu působit proti rozptýleným, skrytým nebo obtížně identifikovatelným skupinám ozbrojených osob využívajícím taktiky asymetrického boje nebo terorismu s cílem rozvrátit veřejný pořádek, ohrozit bezpečnost obyvatel a destabilizovat stát.

Odpovědnost řešit ohrožení vnitřní bezpečnosti přísluší primárně Policii ČR. Pokud by její kapacity a schopnosti nestačily k zajištění vnitřního pořádku a bezpečnosti, může být Policie ČR posílena vybranými prvky ozbrojených sil a dalších bezpečnostních sborů.

Ozbrojené síly ČR

Role ozbrojených sil ČR spočívá především v odstrašení, odvrácení a eliminaci vnějších útoků proti bezpečnosti státu a občanů. Možnosti použití, úkoly a nástroje ozbrojených sil jsou vymezeny zejména zákony: ústavním zákonem č. 110/1998 Sb., o bezpečnosti ČR; zákonem č. 222/1999 Sb., o zajišťování obrany ČR; zákonem č. 219/1999 Sb., o ozbrojených silách ČR; zákonem č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon), dále Bezpečnostní strategií ČR a Obrannou strategií ČR. Požadované schopnosti a kapacity ozbrojených sil stanovují zejména Dlouhodobý výhled pro obranu 2030, Koncepce výstavby Armády ČR do roku 2025 a řada dalších koncepcí nižší úrovně zaměřených na dílčí oblasti schopností nebo na specifické nástroje a mechanismy – využití Aktivní zálohy, přípravu obyvatelstva k obraně a další.

Hybridní kampaň by v extrémním případě mohla vést i k vypuknutí konfliktu za rozsáhlého použití ozbrojených sil. ČR zajišťuje svou obranu na principu kolektivní obrany v rámci NATO. ČR je obklopena spojeneckými zeměmi a není hraničním státem Aliance.

Ozbrojené síly proto nejsou koncipovány pro samostatnou obranu teritoria ČR, ale pouze pro poskytnutí proporcionálního příspěvku ke kolektivní obraně za účasti všech členů NATO. V případě hybridní kampaně využívající i vojenských nástrojů tak role ozbrojených sil ČR spočívá především v přispění k odstrašení, případně odražení útoku na sebe či jiného člena Aliance. Minimálním spojenci očekávaným příspěvkem ČR ke kolektivní obraně (jejíž součástí je i odstrašení) je brigádní úkolové uskupení pozemních sil v odpovídající míře vybavené veškerou potřebnou podporou a zabezpečením (včetně části vzdušných sil), které mu umožní samostatné a plnohodnotné plnění bojových úkolů. Ozbrojené síly proto v mírové struktuře mají jen minimum volných kapacit, které by umožňovaly rozsáhlejší nasazení, než takto koncipovaný příspěvek. K odražení ozbrojeného útoku, který by se odehrával v těsné blízkosti nebo přímo zasahoval území ČR, by přirozeně byly využity veškeré

kapacity ozbrojených sil, včetně záloh a dalších nástrojů mobilizace. V mimořádných situacích mohou být ozbrojené síly využity také k posílení Policie ČR při plnění úkolů zajištění vnitřního pořádku a bezpečnosti. Podle potřeby posouzené ad hoc na základě konkrétní situace mohou ozbrojené síly vyčlenit v principu celé spektrum svých schopností a kapacit.

Odhalování případného rozvratného působení na vojáky (např. podněcování extremismu) je primárně úlohou Vojenské policie.

Vláda ČR

Vládě přísluší celková odpovědnost za zajištění bezpečnosti a obrany státu a obyvatelstva. Má k dispozici celý bezpečnostní systém a relevantní pracovní orgány jako BRS a Ústřední krizový štáb pro řešení krizových situací.

Povinnosti a pravomoci vlády jsou vymezeny zejména ústavním zákonem č. 1/1999 Sb., Ústava ČR; ústavním zákonem č. 110/1998 Sb., o bezpečnosti ČR; zákonem č. 222/1999 Sb., o zajišťování obrany ČR; zákonem č. 219/1999 Sb., o ozbrojených silách ČR.

Klíčovou úlohou vlády je přijímat rozhodnutí o konkrétních opatřeních k zajištění bezpečnosti a obrany, jinými slovy řídit řešení krizové situace. K tomu je nezbytné zajistit několik základních vzájemně provázaných podmínek – usnášeníschopnost vlády, zabezpečené pracoviště a zabezpečené spojení umožňující řídit prvky bezpečnostního systému.

V případě hybridní kampaně vedené proti ČR nebo skupině států, jíž je ČR členem (např. státy NATO či EU), potřebuje vláda především spolehlivé a včasné vyhodnocení informací k přijímání potřebných rozhodnutí. Tempo hybridní kampaně může být různé, od dlouhodobého pozvolného působení po intenzivní, velmi dynamicky se odvíjející sled událostí. Vláda může stát před nutností rozhodovat se v extrémně krátkém čase. Krizové rozhodování vlády proto musí být vyřešeno způsobem, který za všech okolností bude garantovat usnášeníschopnost vlády, zvláště pak v podmínkách časové tísně[88].

Klíčovým faktorem pro odhalení hybridní kampaně vedené proti ČR nebo jejím spojencům je kontinuální získávání a vyhodnocování informací. Sdílení informací by mělo probíhat v jednom místě. Právě takový mechanismus vláda ve struktuře bezpečnostního systému potřebuje.

Prezident republiky

Pravomoci prezidenta republiky ve vztahu k obraně státu upravuje ústavní zákon č. 1/1999 Sb., Ústava ČR; zákon č. 219/1999 Sb., o ozbrojených silách ČR a zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon).

Prezident je vrchním velitelem ozbrojených sil. Jeho role je především symbolická a ceremoniální – jmenuje a povyšuje generály, jmenuje vojáky do nejvyšších vojenských funkcí či schvaluje základní vojenské řády. Rozhodnutí vydané prezidentem republiky jako vrchním velitelem ozbrojených sil vyžaduje ke své platnosti spolupodpis předsedy vlády nebo jím pověřeného člena vlády. Za rozhodnutí prezidenta republiky, které vyžaduje takový spolupodpis, odpovídá vláda.

[88] Tato problematika je již dlouhodobě řešena v rámci dokumentu „Optimalizace současného bezpečnostního systému ČR“ – viz úkol z usnesení vlády ze dne 2. prosince 2015 č. 980.

Parlament ČR

Pravomoci Parlamentu ČR jsou zakotveny v ústavním zákoně č. 1/1999 Sb., Ústava ČR a v ústavním zákoně č. 110/1998 Sb., o bezpečnosti ČR.

Parlament ČR rozhoduje o vyhlášení stavu ohrožení státu a válečného stavu, je-li ČR napadena, nebo je-li třeba plnit mezinárodní smluvní závazky o společné obraně proti napadení a o účasti ČR v obranných systémech mezinárodní organizace, jíž je ČR členem. Dále vyslovuje souhlas s vysláním ozbrojených sil ČR mimo území ČR a s pobytem ozbrojených sil jiných států na území ČR, nejsou-li taková rozhodnutí vyhrazena vládě.

V době, kdy je Poslanecká sněmovna Parlamentu ČR rozpuštěna, činí tato rozhodnutí Senát Parlamentu ČR. Také Parlament ČR, respektive Senát, může stát před nutností rozhodovat se v extrémně krátkém čase. Je proto nezbytné v praxi zajistit podmínky, které by za všech okolností garantovaly usnášeníschopnost Parlamentu ČR[89].

C. SWOT analýza

Vzhledem k tomu, že hybridní způsob vedení konfliktu je komplexním přístupem kombinujícím celou řadu nástrojů, ambicí této SWOT analýzy je posoudit odolnost a možnosti bezpečnostního systému ČR jako celku.

Silné stránky

- Pevné strukturální začlenění ČR do NATO a EU. Obě organizace poskytují v současnosti nejvyšší možné záruky bezpečnosti a kolektivní obrany.
- Rozvinutý bezpečnostní systém ČR s přiměřenou strukturou pracovních koordinačních orgánů založený na komplexním přístupu k řešení krizových situací.
- Zkušenost s fungováním účelově zřízených platforem pro sdílení informací a koordinaci činnosti – např. společná zpravodajská skupina zřízená primárně pro řešení teroristických hrozeb.
- Existence integrovaného záchranného systému, který dokáže efektivně řešit širokou škálu důsledků mimořádných událostí a krizových situací ohrožujících zdraví, život, majetek obyvatelstva a životní prostředí.
- Relativně vysoká míra homogenity české společnosti, relativně rozvinutá občanská společnost s potenciálem mobilizovat se pro ochranu národních zájmů.

Slabé stránky

- Omezená schopnost identifikace hybridního útoku vedeného proti ČR z důvodu absence mechanismu systematického komplexního vyhodnocování událostí a aktivit, které by vedlo k rozpoznání potenciální hybridní kampaně.

[89] Tato problematika je již dlouhodobě řešena v rámci dokumentu „Optimalizace současného bezpečnostního systému ČR“ – viz úkol z usnesení vlády ze dne 2. prosince 2015 č. 980.

- V rámci cvičení krizového řízení jsou nedostatečně řešeny situace, které by testovaly infrastrukturu a procedury k zachování fungování a rozhodování vlády, zejména když protivník usiluje právě o rozvrácení rozhodovacího procesu. Scénáře cvičení krizového řízení neřeší potřebu zabezpečit usnášeníschopnost Parlamentu ČR.
- Celkové mírové kapacity ozbrojených sil ČR při plnění obvyklých úkolů neumožňují významně posílit Policii ČR, zejména na delší časové období. Není připraven mechanismus pro rychlé navýšení početního stavu ozbrojených sil, buď náborem dobrovolníků, nebo provedením mobilizace záloh. Armáda ČR má relativně malý komponent speciálních sil.
- Na ozbrojené síly ČR obecně není kladen požadavek, aby byly schopny reagovat na podnět v extrémně krátkém čase. Chybí mechanismus pro velmi rychlé vyžádání sil a prostředků ozbrojených sil ČR pro posílení Policie ČR k plnění úkolů zajištění bezpečnosti na území ČR.
- Zdlouhavý proces pořizování výzbroje, výstroje a dalšího materiálu cestou veřejných zakázek v případě potřeby rychlé reakce.
- Absence mechanismu pro přípravu a zapojení veřejnosti v případě rozsáhlého ohrožení vnitřní bezpečnosti ČR nebo zajištění fungování státu za krizových stavů.
- Nedostatečné kapacity odborného personálu, který může zajišťovat kybernetickou bezpečnost, monitorovat a analyzovat kybernetické útoky a také je eliminovat.
- Nedostatečné prověřování dodavatelů informačních a komunikačních technologií (ICT) a samotných ICT produktů (software i hardware) v institucích významných pro bezpečnost státu. Špatně nastavené politiky kybernetické bezpečnosti v těchto institucích a podcenění vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti.
- Absence systematického přístupu a efektivních nástrojů pro realizaci strategické komunikace vlády a dalších institucí veřejné správy.
- Náchylnost části populace ČR k ovlivnění prostřednictvím propagandy a dezinformační kampaně a zpochybňování/podceňování existence takové propagandy některými veřejně činnými osobami.
- Nedostatečné materiálně-technické podmínky u řady státních institucí, které brání vytvoření bezpečného komunikačního prostředí a použití moderních komunikačních a informačních technologií pro potřeby zajištění bezpečnosti a obrany státu a řešení krizových situací.

Příležitosti

- Široké možnosti sdílení informací a zkušeností v rámci NATO a EU týkajících se efektivních metod a nástrojů, jak čelit hybridní kampani a jak posilovat celkovou odolnost společnosti vůči útoku.
- NATO a EU aktuálně pracují na definování svého přístupu, jak čelit hybridní kampani vedené proti nim (nebo proti jejich členským státům), a zároveň intenzivně pracují na nastavení mechanismů, jak v situaci hybridního útoku vzájemně spolupracovat a asistovat svým členským státům. ČR se do těchto procesů může aktivně zapojit, ovlivnit výsledek a získané zkušenosti využít pro adaptaci vlastního bezpečnostního systému.
- Využití cvičení krizového řízení NATO a EU zaměřených specificky na scénáře hybridního útoku k testování všestranné připravenosti bezpečnostního systému ČR.

- Politické strany zastoupené v Poslanecké sněmovně Parlamentu ČR (s výjimkou KSČM) v březnu 2014 deklarovaly svou odpovědnost za bezpečnost občanů ČR a své odhodlání k prosazení kroků nezbytných pro zajištění obrany země.

Hrozby

- Řada dílčích nepříznivých faktorů relevantních i v kontextu hybridní hrozby je identifikována v ostatních kapitolách, zejména v „Působení cizí moci“ a „Hrozby v kyberprostoru“. Ty lze doplnit o hrozby týkající obecněji celého bezpečnostního sektoru.
- Nečekaný vývoj událostí, který by vedl k prioritizaci veřejných výdajů ČR ve prospěch jiných sektorů, než je bezpečnost a obrana.
- Tendence některých států, členů NATO a EU, ke zdrženlivosti při sdílení citlivých zpravodajských informací.
- Stagnace v posilování a prohlubování vzájemné spolupráce mezi NATO a EU.

D. Doporučení k posílení odolnosti

Posouzení možného ohrožení ČR metodami hybridní kampaně ve světle současných nástrojů a kapacit institucí bezpečnostního systému nevede k žádným alarmujícím závěrům. Legislativu a konkrétní operativní nástroje jednotlivých institucí lze hodnotit jako celkově přiměřené. Přesto ČR má určité deficity ve svých možnostech, jak co nejefektivněji hybridní kampani čelit. K jejich odstranění jsou doporučena následující opatření:

1. Vytvořit v rámci bezpečnostního systému ČR platformu pro sdílení informací, v níž se budou sbíhat informace a indikace, na základě kterých bude schopna identifikovat potenciální hybridní kampaň. Nemusí jít nutně o zřizování nové instituce, ale o vytvoření specifické kapacity lidí s požadovanou odborností v rámci již existujících institucí a jejich působností v rámci stávající legislativy.
2. Vytvořit systém varovných indikátorů, s jejichž pomocí budou i jiné instituce, než zpravodajské služby, schopny zachytit informace, které mohou přispět k odhalení probíhající hybridní kampaně.
3. Definovat strategický přístup ČR, jak čelit hybridní kampani vedené proti ní nebo proti jinému státu NATO či EU (může být součástí Bezpečnostní strategie ČR nebo samostatným strategickým dokumentem). Přitom vycházet z analýzy přínosů, které nabízí mezinárodní spolupráce, primárně v rámci EU a NATO.
4. V rámci vybraných cvičení krizového řízení se zaměřit na testování infrastruktury a procedur k zabezpečení funkčnosti a rozhodování vlády v nejnáročnějších situacích.
5. Změny ve struktuře ozbrojených sil a jejich pohotovosti navázat na vydání nových cílů obranného plánování NATO. Ty vyjadřují příspěvek, který spojenci od ČR očekávají v rámci závazku společné obrany, a promítnou se v nich i požadavky adaptace NATO na nové bezpečnostní prostředí. Ministři obrany tyto cíle budou schvalovat v červnu 2017.
6. Zjednodušit proces akvizice výzbroje, materiálu a služeb pro ozbrojené síly cestou veřejných zakázek, aby umožňoval jejich pořízení ve velmi krátké době, zejména při ochraně podstatných bezpečnostních zájmů ČR.

7. Přizpůsobit právní rámec pro umožnění aktivního zapojení zpravodajských služeb ČR do realizace opatření na obranu proti hybridní kampani vedené proti ČR nebo státům NATO a EU.
8. Posoudit, zda současné nastavení možností použití ozbrojených sil ČR (jednotlivců i jednotek) k zajištění bezpečnosti na území ČR vyhovuje i v kontextu hybridních hrozeb.
9. Prozkoumat možnosti vytvoření mechanismu pro přípravu a zapojení veřejnosti v případě rozsáhlého ohrožení vnitřní bezpečnosti ČR nebo zajištění fungování státu za krizových stavů, jako součást implementace koncepce ochrany obyvatelstva a přípravy občanů k obraně státu.
10. Vytvořit podmínky pro efektivní a věrohodnou strategickou komunikaci vlády, tj. stanovit koncepční přístup a nastavit mechanismus pro systematickou koordinaci všech relevantních aktérů veřejné správy.
11. Posílení občanského vzdělávání na školách (základní hodnoty, mediální gramotnost, jednání v krizových situacích).
12. V rámci cvičení a testování bezpečnosti a odolnosti klíčové kybernetické infrastruktury pravidelně aplikovat scénáře hybridního útoku (zaměřit se na distribuční energetické soustavy, informační sítě veřejné správy atd.).
13. S využitím moderních komunikačních a informačních technologií zajistit bezpečné komunikační prostředí pro potřeby řízení při řešení všech typů krizových situací.

SEZNAM ZKRATEK

BIS	Bezpečnostní informační služba
BRS	Bezpečnostní rada státu
BS 2015	Bezpečnostní strategie České republiky 2015
CBRN	chemické, biologické, radiologické a jaderné látky a materiály
ČHMÚ	Český hydrometeorologický ústav
ČIŽP	Česká inspekce životního prostředí
ČR	Česká republika
ERÚ	Energetický regulační úřad
EU	Evropská unie
HOPKS	hospodářské opatření pro krizové stavy
HZS ČR	Hasičský záchranný sbor České republiky
IZS	integrovaný záchranný systém
JPO	jednotky požární ochrany
MD	Ministerstvo dopravy
MF	Ministerstvo financí
MK	Ministerstvo kultury
MMR	Ministerstvo pro místní rozvoj
MO	Ministerstvo obrany
MPO	Ministerstvo průmyslu a obchodu
MSp	Ministerstvo spravedlnosti
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
MV	Ministerstvo vnitra
MZdr	Ministerstvo zdravotnictví
MZe	Ministerstvo zemědělství
MŽP	Ministerstvo životního prostředí
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NESO	Národní organizace pro společný postup ve stavu ropné nouze
ORP	obec s rozšířenou působností
OSN	Organizace spojených národů
Policie ČR	Policie České republiky
PR	public relations

RMS	radiační monitorovací síť
SSHR	Správa státních hmotných rezerv
SEI	Státní energetická inspekce
SIVS	Systém integrované výstražné služby
SÚJB	Státní úřad pro jadernou bezpečnost
SVS	Státní veterinární správa
ÚSC	územně samosprávný celek
ÚSÚ	ústřední správní úřad
ÚZSI	Úřad pro zahraniční styky a informace
VZ	Vojenské zpravodajství
ZZS	zdravotnická záchranná služba
ZKB	zákon o kybernetické bezpečnosti

AUDIT NÁRODNÍ BEZPEČNOSTI

Vydalo
Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality
Nad Štolou 3, 170 34 Praha 7 – Letná

Praha, 2016
Text neprošel jazykovou korekturou.