Návrh národních priorit orientovaného výzkumu, vývoje a inovací

ZÁVĚREČNÁ ZPRÁVA EXPERTNÍHO PANELU

Bezpečná společnost

(Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR)

Zpracovali:
Ing. Jaroslav Doležal, CSc
Doc. RNDr. Karel Oliva, Dr.
Mgr. Martin Faťun
Ing. Eva Hillerová

23. prosince 2011

Obsah

1. Obsah Závěrečné zprávy

Závěrečná zpráva expertního panelu zahrnuje popis složení expertního panelu, metodický postup a výsledky činnosti expertního panelu v průběhu projektu PRIORITY2030. Problémově vymezená prioritní oblast je podrobněji strukturována na dílčí výzvy, hrozby a příležitosti, k nimž byly identifikovány žádoucí stavy v horizontu roku 2030 (tzv. stěžení cíle). Závěrečná zpráva dále obsahuje seznam identifikovaných středně- a dlouhodobých výzkumných cílů a souvisejících směrů VaV, jejichž prostřednictvím lze těchto žádoucích stavů dosáhnout.

V další části Závěrečné zprávy je popsán způsob výběru prioritních výzkumných cílů, které spolu s definovanými podpůrnými opatřeními tvoří základ pro konečnou identifikaci národních priorit orientovaného výzkumu, vývoje a inovací ČR v této prioritní oblasti.

K sestavení Závěrečné zprávy panelu přispěli všichni členové expertního panelu; výsledná podoba Závěrečné zprávy pak byla finalizována předsedou panelu Ing. Jaroslavem Doležalem, CSc. a místopředsedou panelu Doc. RNDr. Karlem Olivou, Dr., ve spolupráci s tajemníky panelu Mgr. Martinem Faťunem a Ing. Evou Hillerovou.

Po ukončení činnosti expertního panelu byl název prioritní oblasti rozhodnutím Rady pro výzkum, experimentální vývoj a inovace ze dne 27. ledna 2012 dodatečně změněn na „Bezpečná společnost“. V této Závěrečné zprávě, která představuje výsledek činnosti expertního panelu, je proto stále používán původní název prioritní oblasti, Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR.

Prioritní oblast Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR

Roste komplexita hrozeb, rizik a z ní plynoucí nutnost adaptace bezpečnostního systému ČR. Potenciální bezpečnostní hrozby pro ČR se mohou řetězit a jejich následky vzájemně násobit. Zvyšuje se závislost na technologiích, dálkově transportované energii a zásobování. Mezi rizikové faktory patří permanentní nestabilita na periferii euroatlantického prostoru či možný souběh přírodních a člověkem způsobených pohrom (útoků či havárií).

Naše společnost přitom věnuje nízkou pozornost a prostředky na snížení své zranitelnosti. Neexistuje koordinovaná komplexní příprava na krizové situace, která by se závazně vztahovala nejen na bezpečnostní systém a veřejnou správu, ale i firmy, podnikatele a občany. Bezpečnostní politika se v turbulenci rozpočtových škrtů a politického boje stala nezřetelnou a bezpečnostní instituce se snaží udržet pouhou základní funkčnost. Významnou hrozbou je rovněž prohlubování systémové korupce, jejíž přetrvávání ohrožuje soudržnost celé společnosti.

V globálním kontextu musí být kladen důraz i na hrozby teroristických útoků a s nimi související ochranu kritických infrastruktur, energetickou bezpečnost a potlačování organizovaného zločinu. Nezbytné je rovněž adaptovat bezpečnostní systém ČR na zvládání dalších krizových situací, jako jsou živelní pohromy či havárie. Současně je třeba akcentovat nezbytnost aktivní spolupráce v rámci mezinárodních organizací a struktur.

Stanovení priorit bezpečnostního výzkumu navazuje na Meziresortní koncepci bezpečnostního výzkumu a vývoje ČR do roku 2015. Tato koncepce vymezuje tři základní oblasti, ze kterých lze vycházet, ale které formulaci priorit nijak neomezují:

- Bezpečnost občanů zahrnující terorismus, organizovanou kriminalitu, další formy závažné kriminality ohrožující bezpečnost státu a jejich potírání, ochranu obyvatelstva, bezpečnost měst a obcí v případě živelných pohrom a provozních havárií včetně bezpečnosti podzemních objektů, ochranu občanů proti kriminalitě, protispolečenskému jednání a socio-patologickým jevům, kybernetickou kriminalitu a on-line vyšetřování, nešíření zbraní hromadného ničení a malých střelných zbraní, technologie a metody detekce chemických, biologických a radiologických látek, jaderných materiálů a výbušnin, socio-ekonomickou a etickou oblast bezpečnosti, detekci anomálií v dopravě a tocích cestujících a environmentální bezpečnost.
- Bezpečnost kritických infrastruktur zahrnující energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotní péči, dopravu, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby, veřejnou správu, výzkumné organizace, chemický, jaderný a báňský průmysl, specifické průmyslové záležitosti a spojení mezi různými infrastrukturami.
- Krizové řízení zahrnující formování a implementaci bezpečnostní politiky, rozvoj bezpečnostního systému, včasné varování, komunikaci s veřejností, připravenost, prevenci, reakci a obnovu, civilně vojenskou spolupráci a civilní nouzové plánování, moderní metody zásahového tréninku a vnější krizový management EU.

2. Složení expertního panelu

2.1 Charakteristika složení expertního panelu

V souladu s Principy pro přípravu národních priorit výzkumu, experimentálního vývoje a inovací, které tvoří základní zadání projektu přípravy priorit orientovaného výzkumu, vývoje a inovací, byl expertní panel sestaven multidisciplinárně. Výběr členů expertního panelu ze souboru přihlášených odborníků byl uskutečněn s využitím následujících kritérií:

- *Zastoupení expertů pro různé vědní oblasti*

  Důvodem pro využití tohoto kritéria je skutečnost, že se jedná o heterogenní průřezovou prioritní oblast zasahující do širokého spektra společenskovědních, přírodovědných i technických oborů.

- *Zastoupení expertů z aplikační sféry se znalostí oborů významných z hlediska bezpečnostní problematiky*

  Jedná se zejména o oblast informačních a komunikačních technologií, jejíž aplikace mají bezprostřední dopad na účinnost a efektivitu procesů prevence, reakce a obnovy v případě mimořádných událostí a krizových situací .

- *Zastoupení expertů z institucí veřejné správy zabývajících se bezpečnostním výzkumem a bezpečnostní problematikou obecně*

  Vzhledem k tomu, že veřejná správa má koordinační a zastřešující roli v případě mimořádných událostí a krizových situací s celospolečenským, ale i regionálním nebo místním dopadem, je tato sféra nositelem důležité expertní znalosti pro formulaci potřeb a cílů v bezpečnostní oblasti.

- *Zastoupení expertů působících v oblasti kritických infrastruktur a ve specifických oblastech bezpečnosti*

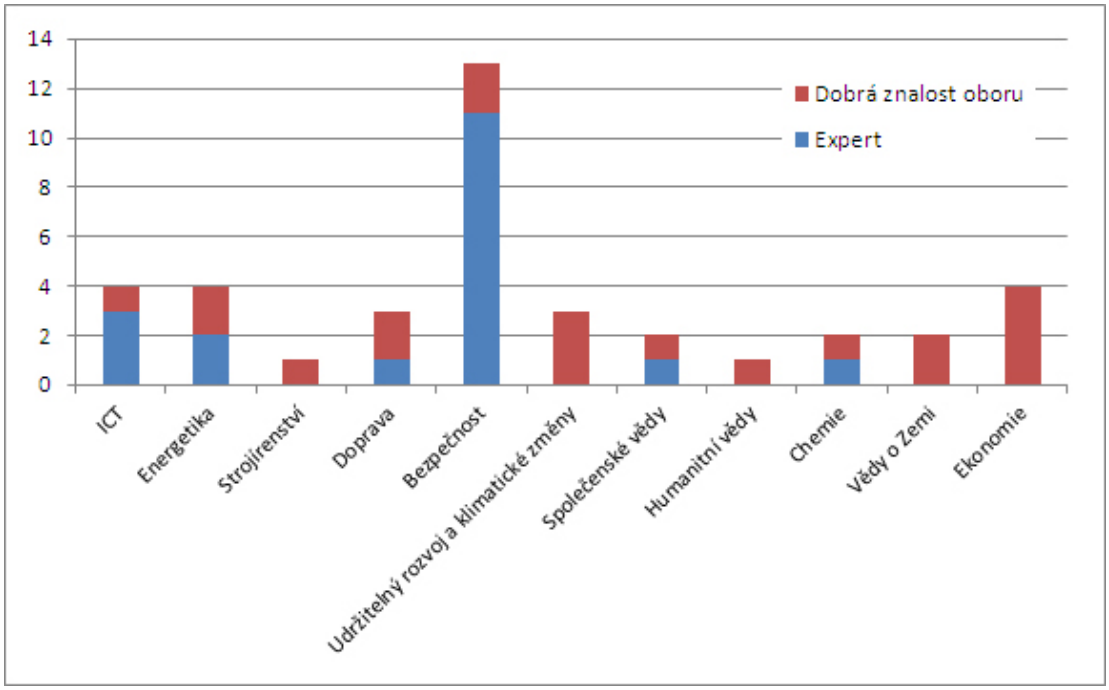
  Zejména se jedná o oblasti energetiky, dopravy, ekonomie, přírodních zdrojů a životního prostředí, které mají specifický význam pro zachování bezpečnosti a kvality života v případě mimořádných událostí a krizových situací.

- *Zastoupení expertů z různých regionů*

  Regiony v ČR jsou z hlediska své polohy, přírodních a společenských charakteristik vystaveny zčásti specifickým rizikům, čelí specifickým hrozbám a mají proto do určité míry specifické potřeby z hlediska zajištění bezpečnosti. Snahou proto bylo zajistit regionální diverzifikaci zastoupení expertů v panelu.

Výsledné složení panelu respektuje zaměření prioritní oblasti. Z hlediska odbornosti jsou v panelu zastoupeny různé obory, a to na expertní úrovni či na úrovni dobré znalosti oboru. Jelikož jádrem prioritní oblasti je rozvoj schopností bezpečnostního systému ČR, je v panelu nejvýznamnější zastoupení expertů, kteří mají expertní či dobrou znalost v oboru bezpečnosti.

Graf 1: Struktura členů expertního panelu podle odbornosti



Pozn.: Graf byl zpracován na základě vlastního posouzení odbornosti ve vybraných oborech jednotlivými členy panelu.

Zaměření expertního panelu odpovídá také jeho struktura podle typu organizací. Nejvýznamněji jsou v panelu zastoupeni odborníci z vysokých škol se zkušenostmi s různými aspekty bezpečnostní problematiky ve společenskovědních, přírodovědných i technických oborech. Třetinu expertů v panelu tvoří zástupci podnikového sektoru, dva zástupci reprezentují organizační složky státu a státní správy a dva členové panelu byly vybráni z resortních veřejných výzkumných institucí zaměřených na bezpečnostní problematiku .

Tab. 1: Struktura členů expertního panelu podle typu organizace

Typ organizace	**počet**	**v %**
Vysoká škola	6	40 %
Soukromý podnikatelský subjekt	5	33,3 %
Organizační složka státu nebo organizační jednotka MO a MV	2	13,3 %
Resortní v.v.i.	2	13,3 %
Celkem	**15**	

2.2 Personální obsazení expertního panelu

Vedení panelu:

JMÉNO	ORGANIZACE
Ing. Jaroslav Doležal, CSc. **Předseda expertního panelu**	Honeywell, spol. s.r.o.
Doc. RNDr. Karel Oliva, Dr. **Místopředseda expertního panelu**	Ústav pro jazyk český AV ČR, v.v.i.

Tajemníci panelu:

JMÉNO	ORGANIZACE
Mgr. Martin Faťun **Odpovědný tajemník**	Technologické centrum AV ČR
Ing. Eva Hillerová **Další tajemník**	Technologické centrum AV ČR

Členové panelu:

JMÉNO	ORGANIZACE
PhDr. Miloš Balabán, PhD.	Fakulta sociálních věd Univerzity Karlovy Praha
Ing. Ivan Beneš	CITYPLAN, spol. s.r.o.
RNDr. Josef Břínek, PhD.	Státní ústav jaderné, chemické a biologické ochrany, v.v.i.
Doc. Mgr. Oldřich Bureš, PhD., M.A.	Metropolitní univerzita Praha
Prof. RNDr. Pavel Danihelka, CSc.	Vysoká škola báňská – Technická univerzita Ostrava
Ing. Dana Drábová, PhD.	Státní úřad pro jadernou bezpečnost
Doc. Ing. Ivo Drahotský, PhD.	Univerzita Pardubice
Prof. RNDr. Jan Hajič, Dr.	Matematicko-fyzikální fakulta Univerzity Karlovy Praha
Lukáš Kencl, Dr.	České vysoké učení technické v Praze
Ing. Vít Líbal, PhD.	Honeywell, spol. s.r.o.
Ing. Karel Obluk, PhD.	AVG Technologies CZ, s.r.o.
Ing. Ludmila Petráňová	Ernst & Young
Ing. Zdeněk Prouza, CSc.	Státní ústav radiační ochrany, v.v.i
Ing. Jarmil Valášek, PhD.	Institut ochrany obyvatelstva , Ministerstvo vnitra – GŘ Hasičského záchranného sboru ČR
Mgr. Michal Vaněček	ISATech, s.r.o.

3. Činnost expertního panelu

Expertní panel pracoval od 12. října do poloviny prosince 2011. Jeho činnost byla rozdělena do tří navazujících fází:

- Strukturace prioritní oblasti
- Prioritizace cílů
- Konsolidace cílů a struktury prioritní oblasti

3.1 Strukturace prioritní oblasti

Cílem první fáze bylo strukturovat prioritní oblast do tematicky specifických oblastí a podoblastí, ke každé podoblasti stanovit stěžejní cíl, dílčí cíle a související směry výzkumu a vývoje (VaV), které umožní jejich naplnění.

Tato fáze činnosti expertního panelu byla realizována dvěma workshopy, které se konaly ve dnech 12. října 2011 a 24. října 2011.

Workshop 1

Na prvním workshopu byla s využitím podkladů připravených předsedajícími panelu ve spolupráci s tajemníky panelu strukturována prioritních oblast do 3 oblastí - Bezpečnost občanů, Bezpečnost kritických infrastruktur a zdrojů, Krizové řízení a bezpečnostní politika - obsahujících dohromady 11 podoblastí. Pro každou z těchto podoblastí byl formulován stěžejní cíl v horizontu roku 2030, vyjadřující žádoucí stav dané podoblasti. Stanoveného cíle má být dosaženo s přispěním VaV i dalších systémových opatření.

Navržený podkladový materiál obsahoval rovněž oblast č. 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR; zde panel konstatoval, že se vzhledem ke svému složení nemá kompetenci ke zpracování oblasti spadající do kompetence Ministerstva obrany a Armády České Republiky. Následně proto bylo předsedou panelu osloveno Ministerstvo obrany (MO) a jím delegovaný expertní tým pak byl se souhlasem Koordinační rady expertů (KRE) pověřen podrobnější strukturací této oblasti. Expertní tým MO rozdělil oblast obrany do 4 podoblastí a formuloval příslušné stěžejní cíle.

Workshop 2

Na druhém workshopu stanovili členové expertního panelu k daným stěžejním cílům (s horizontem do roku 2030) dílčí cíle (s bližším časovým horizontem). Tyto dílčí cíle představují postupné kroky k dosažení jednotlivých stěžejních cílů. Dílčí cíl je charakterizován stručným popisem a přínosem pro dosažení stěžejního cíle. Ke každému dílčímu cíli byly definovány související směry VaV, které jsou relevantní pro jeho naplnění. Pro oblast č. 4: „Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR“ navrhl obdobnou strukturaci opět pověřený expertní tým MO.

Výsledky této fáze činnosti expertního panelu realizované na workshopech 1 a 2 jsou uvedeny v Příloze 1.

3.2 Prioritizace cílů

Druhou fází činnosti expertního panelu byl samotný proces výběru prioritních výzkumných cílů na úrovni cílů dílčích. Cílem bylo redukovat jejich počet a dále detailně pracovat jen s dílčími cíli vysoké priority. Celý proces prioritizace sestával z několika na sebe navazujících kroků:

Prvním krokem bylo on-line hlasování prostřednictvím hlasovacího formuláře po dobu 10 dní v období mezi druhým a třetím workshopem. Hlasování o dílčích cílech prioritní oblasti „Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR“ bylo povoleno pouze členům tohoto panelu a předsedovi a místopředsedkyni Koordinační rady expertů. Hlasování se společně s předsedou a místopředsedou zúčastnilo všech 15 členů panelu expertů.

Pro oblast č. 4: „Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR“ proběhlo oddělené hlasování, které bylo realizováno pověřeným expertním týmem MO.

Jednotlivé dílčí cíle byly hodnoceny z hlediska jejich významnosti a dosažitelnosti. Významnost dílčího cíle byla posuzována v širších souvislostech, tedy nikoliv pouze v rámci daného stěžejního cíle, k němuž směřují. Prostřednictvím dosažitelnosti pak byla hodnocena schopnost a úroveň českého VaVaI daného dílčího cíle dosáhnout s přihlédnutím k dalším systémovým podmínkám.

Kritéria „významnost“ a „dosažitelnost“ byla sestavena z řady dílčích kritérií (Příloha 2.1). U všech těchto kritérií bylo hodnocení prováděno na stupnici 1-5 (výjimečně opačně v případě kritéria „Očekávaná finanční náročnost dosažení cíle“) s tímto významem:

- 1 = velmi nízký až zanedbatelný;
- 2 = nízký;
- 3 = střední;
- 4 = vysoký;
- 5 = velmi vysoký.

Před hlasováním o významnosti a dosažitelnosti jednotlivých dílčích cílů měl každý člen expertního panelu možnost zvolit, zda bude daný cíl hodnotit, či nikoliv. Pokud se rozhodl daný dílčí cíl hodnotit, v dalším kroku ohodnotil svojí odbornost. Od zvolené úrovně se odvíjela váha jeho hlasu. Hlasující měli možnost volby z následujících úrovní:

- „Základní nebo malá znalost“
- „Dobrá znalost“
- „Expert“

Výsledky expertního hodnocení jsou zpracovány v příloze 2.2 a byly jedním z podkladů pro výběr prioritních cílů VaVaI, tedy cílů nejvýznamnějších a zároveň alespoň z části dosažitelných. Koordinační rada expertů provedla výběr prioritních cílů VaVaI, který byl ve třetím kroku posouzen a finalizován členy expertního panelu.

3.3 Konsolidace struktury a cílů prioritní oblasti

Workshop 3

Na třetím workshopu dne 28. listopadu 2011 panel expertů posoudil výběr dílčích cílů provedený Koordinační radou expertů a rozhodl se udělit „divokou kartu“ (tj. dodatečné zahrnutí do výběru) dvěma dříve nevybraným dílčím cílům, pokrývajícím problematiku ochrany před kriminalitou, extremismem a terorismem, a to s ohledem na vysokou společenskou závažnost této problematiky.

Současně se panel rozhodl eliminovat z výběru provedeného KRE jiné dva dílčí cíle s ohledem na jejich úzkou příbuznost s jinými vybranými dílčími cíli.

V oblasti č. 4: „Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR“ panel doporučil upřesnění formulace některých dílčích cílů a přesunutí několika dílčích cílů, vzhledem k jejich charakteru, mezi systémová opatření. Tato doporučení byla pověřeným expertním týmem MO vzata v úvahu a na jejich základě byla vypracována konečná podoba prioritních stěžejních a dílčích cílů. Současně byl název oblasti č. 4 upraven do výsledné podoby „Obrana, obranyschopnost a nasazení ozbrojených sil“.

Výsledná podoba strukturace prioritní oblasti je popsána v kapitole 4.1. V důsledku eliminace některých dílčích cílů, k níž došlo během procesu prioritizace a konsolidace, bylo ve výsledné struktuře změněno číslování některých prioritních dílčích cílů oproti stavu po první fázi (který je popsán v Přílohách 1 a 2), tak aby čísla cílů v jednotlivých podoblastech tvořila souvislou číselnou řadu. Tyto změny jsou zachyceny v následujícím přehledu:

Výsledný prioritní dílčí cíl (číslování v kapitole 4)	**Původní označení pracovní verze dílčího cíle před konsolidací** (číslování v přílohách 1 a 2)
2.1.1 Rozvoj alternativních a nouzových krizových procesů	W 2.1.2
2.1.2 Zvyšování odolnosti KI	W 2.1.3
2.1.3 Zajištění a rozvoj interoperability KI	W 2.1.4
2.1.4 Účinná detekce a identifikace hrozeb	W 2.1.5
2.1.5 Rozvoj ICT, telematiky a kybernetické ochrany KI	W 2.1.6
3.2.2 Podpora specifických oblastí bezpečnosti	W 3.2.3
4.1.4 Rozvoj komunikačních a informačních systémů a kybernetická obrana	W 4.1.5

V závěru třetího workshopu panel navrhl systémová opatření pro jednotlivé oblasti (viz kapitola 4.2), indikátory pro kontrolu naplňování stěžejních cílů (viz kapitola 4.3) a poměrné rozdělení finančních prostředků mezi jednotlivé oblasti a stěžejní cíle (viz kapitola 4.4).

4. Výsledky činnosti expertního panelu

4.1 Struktura a cíle prioritní oblasti

Výsledkem činnosti expertního panelu je finální podoba struktury prioritní oblasti rozpracovaná do 25 dílčích cílů. Struktura je znázorněna v tabulce 2 a také v Příloze 3.

Tab. 2: Struktura prioritní oblasti Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR

Oblasti	Podoblasti	Prioritní dílčí cíle
1. Bezpečnost občanů	1.1 Ochrana obyvatelstva	1.1.1 Podpora opatření a úkolů ochrany obyvatelstva
		1.1.2 Zdokonalování služeb a prostředků ochrany
		1.1.3 Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů
	1.2 Ochrana před kriminalitou, extremismem a terorismem	1.2.1 Vytváření účinných metod analýzy druhů a rozšíření kriminality a implementace efektivních nástrojů jejího potlačování
		1.2.2 Minimalizace kybernetické kriminality a zneužívání informací
2. Bezpečnost kritických infrastruktur a zdrojů	2.1 Ochrana, odolnost a obnova kritických infrastruktur	2.1.1 Rozvoj alternativních a nouzových krizových procesů
		2.1.2 Zvyšování odolnosti KI
		2.1.3 Zajištění a rozvoj interoperability KI
		2.1.4 Účinná detekce a identifikace hrozeb
		2.1.5 Rozvoj ICT, telematiky a kybernetické ochrany KI
	2.2 Komunikace a vazby mezi kritickými infrastrukturami	2.2.1 Vzájemné závislosti systémů KI
		2.2.2 Informační podpora pro detekci možných nepříznivých ovlivnění
3. Krizové řízení a bezpečnostní politika	3.1 Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR	3.1.1 Vyhodnocení efektivity strategických řídicích a hodnotících dokumentů v oblasti bezpečnosti
		3.1.2 Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby
	3.2 Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření	3.2.1 Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR
		3.2.2 Podpora specifických oblastí bezpečnosti
	3.3 Systémy analýzy, prevence, odezvy a obnovy	3.3.1 Zlepšení systémů získávání a třídění bezpečnostních informací
		3.3.2 Analýza bezpečnostních informací

		3.3.3 Zdokonalování účinnosti bezpečnostního systému a krizového řízení
		3.3.4 Zdokonalení systémů pro podporu obnovy
	3.4 Legislativní a právní problémy	3.4.1 Legislativní postupy a opatření v případě ohrožení vnitřní bezpečnosti státu, mimořádných přírodních a antropogenních událostí a krizových situací
4. Obrana, obranyschopnost a nasazení ozbrojených sil	4.1 Rozvoj schopností ozbrojených sil	4.1.1 Vývoj nových zbraňových a obranných systémů
		4.1.2 Příprava, mobilita a udržitelnost sil
		4.1.3 Podpora velení a řízení
		4.1.4 Rozvoj komunikačních a informačních systémů a kybernetická obrana

Struktura prioritní oblasti je dále podrobně popsána do úrovně prioritních dílčích cílů. Pro každý prioritní dílčí cíl byl vypracován tzv. Identifikační list prioritního dílčího cíle, který obsahuje podrobnější informace. Soubor Identifikačních listů tvoří Přílohu 4.

Oblast 1: Bezpečnost občanů

Oblast zahrnuje terorismus, organizovanou kriminalitu i další formy závažné kriminality ohrožující bezpečnost státu včetně jejich potírání; ochranu obyvatelstva, bezpečnost měst a obcí v případě živelných pohrom a provozních havárií včetně bezpečnosti podzemních objektů; ochranu občanů proti kriminalitě, protispolečenskému jednání a socio-patologickým jevům; kybernetickou kriminalitu a on-line vyšetřování; nešíření zbraní hromadného ničení a malých střelných zbraní; technologie a metody detekce chemických, biologických a radiologických látek, jaderných materiálů a výbušnin, a v neposlední řadě také socio-ekonomické a etické aspekty bezpečnosti.

Podoblast 1.1: Ochrana obyvatelstva

Ochrana obyvatelstva patří mezi prioritní oblasti bezpečnosti České republiky a zahrnuje soubor činností a postupů věcně příslušných orgánů státní správy a samosprávy a dalších zainteresovaných organizací, složek a obyvatelstva, prováděných s cílem minimalizace negativních dopadů možných mimořádných událostí a krizových situací způsobených antropogenními hrozbami (průmyslové, radiační a ekologické havárie, požáry, velké migrace obyvatelstva, mezinárodní ozbrojené konflikty, použití a zneužití zbraní hromadného ničení CBRNE, velké sociální konflikty apod.) nebo přírodními hrozbami (živelní pohromy - povodně, vichřice, sesuvy půdy, lesní požáry apod.) na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. Tyto pohromy mohou mít kromě ohrožení bezpečnosti**,** životů a zdraví obyvatel a jejich majetku a životního prostředí dopad na ekonomiku země, zásobování energií, surovinami, pitnou vodou, či mohou způsobit poškození kritické infrastruktury, narušení počítačových sítí, přenosu dat a informací. Uvedené mimořádné události a krizové situace mohou být vzájemně závislé a synergické.

Stěžejní cíl 1.1:

Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva

Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.

Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva

Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR.

Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů
Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí, s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování.

Podoblast 1.2: Ochrana před kriminalitou, extremismem a terorismem
Objem zjištěné trestné činnosti v ČR setrvale klesá, nicméně celá oblast vyžaduje trvalé úsilí. Kriminální scéna prochází permanentním procesem adaptace na nové sociální a technologické impulsy. Kriminalita díky volnému pohybu osob v EU i díky celkové globalizaci nabyla výrazně transnacionální rozměr. Lze se i důvodně domnívat, že objem celkové trestné činnosti je podstatně vyšší než zjištěný. Veřejnost řadu případů neoznamuje a mnoho případů latentní kriminality (např. kriminalita proti duševnímu vlastnictví, korupce) je obecně tolerováno. Organizované zločinecké skupiny, extremisté a teroristé patří k nejprogresivnějším uživatelům moderních informačních a komunikačních technologií. V této oblasti lze mj. očekávat nárůst kybernetických útoků ze strany mezinárodních organizovaných skupin a vzrůst rizik spojených se zneužíváním osobních údajů, záznamů a digitální identity uživatelů, či s jejich vývozem za hranice ČR.
V rámci potírání kriminality je důležité trvale analyzovat a precizovat zákonná pravidla kriminalitě předcházející či ji potírající. Oběti trestné činnosti se v určitých ohledech těší menšímu rozsahu práv, než osoby obviněné či odsouzené. V souvislosti s kriminalitou jsou v ČR diskutována např. témata (de-)kriminalizace návykových látek, rozsahu „práva na zbraň“ a míry státní regulace téhož.
V ČR působí řada institucí bojujících proti kriminalitě, které jsou napojeny na evropský a globální bezpečnostní systém, nicméně nejsou stabilizovány. Policie ČR prochází reformním procesem v souvislosti s úspornými opatřeními. ČR vytvořila systém tří zpravodajských služeb, který je ale předmětem permanentních diskusí. V problematické situaci je sektor vězeňství, kde existuje nadměrná přeplněnost stávajících věznic. Celkově nebyl podrobně definován komplexní systém institucí v oblasti vnitřní bezpečnosti.

Stěžejní cíl 1.2:
Stěžejním cílem této oblasti je vybudovat v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře eliminovat všechny formy kriminality, extremismu a terorismu. To vyžaduje vyvážený systém prevence a represe a současně sledování vývojových trendů kriminality, extremismu a terorismu (včetně využití nových technologií či zneužití digitálních informací kriminálníky, adaptace kriminální sféry na nové demografické podmínky, mapování míry nehlášené kriminality a korupce apod.) a nástrojů pro odhalování a potírání těchto negativních jevů.

Dílčí cíl 1.2.1: Vytváření účinných metod analýzy druhů a rozšířenosti kriminality a implementace efektivních nástrojů jejího potírání
Cílem je rozvíjet nástroje analýzy hrozeb, rizik a rozšířenosti kriminality, včetně kriminality organizované, mapování trendů a vytváření nástrojů pro odhadování skutečné trestné činnosti (s ohledem na regiony, na socioekonomický vývoj, s ohledem na určité skupiny skutkových podstat, struktura pachatelů a obětí atd.) a také rozvoj nástrojů pro odhadování nezjištěné trestné činnosti. Dále je cílem rozvoj nových technik a technologií pro odhalování, dokazování a potírání trestných činů a projevů extremismu a terorismu.

	Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům.

Oblast 2: Bezpečnost kritických infrastruktur a zdrojů

Oblast zahrnuje zejména prevenci, ochranu a obnovu v odvětvích energetiky, vodního hospodářství, potravinářství a zemědělství, zdravotní péče, dopravy a logistiky, komunikačních a informačních systémů, bankovního a finančního sektoru, nouzových služeb a veřejné správy. Do této oblasti patří i problematika ochrany a zachování přírodních zdrojů.

Podoblast 2.1: Ochrana, odolnost a obnova kritických infrastruktur

Oblasti KI zahrnuje energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotní péči, dopravu a logistiku, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby a veřejnou správu.

Podoblast 2.1 těsně navazuje na popis a stěžejní cíl podoblasti 1.1 Ochrana obyvatelstva.

Zajištění funkčnosti kritických infrastruktur (KI) spočívá na všech třech faktorech, kterými jsou ochrana KI, odolnost KI a obnova funkce KI po přerušení její funkce. Jedná se v podstatě o tři bezpečnostní bariéry, které brání rozvinutí nežádoucích stavů do krizových situací z pohledu těch, kterým KI slouží. Smyslem ochrany KI je snížení zranitelnosti působením vnějších vlivů, jedná se o ochranu proti účinkům přírodních pohrom a úmyslných antropogenních činů. Smyslem zvyšování odolnosti je zajištění robustnosti systémů KI proti výskytu přírodních, technologických a antropogenních (včetně chyb obsluhy) hrozeb. Děje se tak zahrnutím robustnosti (včetně zajištění alternativních a náhradních mechanismů) do procesů navrhování, výstavby, obsluhy a údržby systémů KI s cílem zabezpečení alespoň určité nouzové úrovně služeb. Zajištění obnovy KI spočívá v úsilí o minimalizace doby obnovy tak, aby se s ohledem na dopady přerušení funkce KI zabránilo rozvoji krizové situace (její vážnost narůstá obvykle exponenciálně v závislosti na době přerušení funkce KI). Současně je třeba, aby při obnově bylo využito rozboru vzniklé situace k navržení preventivních opatření pro zmírnění dopadů při případném opakování pohromy (např. v elektroenergetice jsou tato opatření známá pod pojmem plány obrany a ochrany, v obchodní praxi je vhodným vodítkem norma ČSN BS 25999-1 Management kontinuity činností organizace).

Stěžejní cíl 2.1:

Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací.

Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury.

Aplikace managementu kontinuity činností organizací kritické infrastruktury.

Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů

Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI.

	Dílčí cíl 2.1.2: Zvyšování odolnosti KI Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů.
	Dílčí cíl 2.1.3: Zajištění a rozvoj interoperability KI Tvorba nástrojů pro zajištění a rozvoj interoperability KI (dopravní, energetické a dalších) s nadnárodními evropskými KI. Vazba na nadnárodní evropské síťové systémy (TEN-T, TEN-E). Modelování a výpočty sítí.
	Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).
	Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.

Podoblast 2.2: Komunikace a vazby mezi kritickými infrastrukturami

V současné době dokáží kritické infrastruktury dobře reagovat na problémy, které se projeví uvnitř vlastního systému a v rámci plánů na řešení krizových situací mají připravené postupy na obnovu provozu po odstranění poruchy. Analýzy rizik a spolehlivosti, které jsou prováděny interně pro tyto infrastruktury, však většinou nezahrnují dynamické vzájemné závislosti s ostatními kritickými infrastrukturami. V případě velkých pohrom bývá narušeno více systémů infrastruktury současně. Narušení funkce určitého systému může být způsobeno i problémem zavlečeným z jiného systému prostřednictvím vzájemných vazeb, a to s různým časovým průběhem závislým například na schopnosti akumulace a stavu zásob. Koordinace zásahů a obnovy provozu se v důsledku vzájemných závislostí stává zásadním nástrojem pro efektivní obnovu funkce území. V důsledku nekoordinovaných činností může dojít ke vzájemnému nežádoucímu působení a následkem toho mohou být zesíleny dopady pohromy na život dané komunity. Nekoordinovaný manipulační zásah v jedné infrastruktuře může znemožnit nebo zpomalit obnovu funkce jiné infrastruktury. Stejně tak se může projevit i absence potřebného zásahu.

Na základě dřívějších prací v oblasti výzkumu dopadů a účinků pohrom na život komunity se ukazuje, že zranitelnost souvisí jak s velkostí sídla, tak především s dobou, po kterou je přerušena funkce kritických infrastruktur zajišťujících základní fyziologické lidské potřeby (přiměřená teplota, voda, potraviny) a potřeba zajištění pocitu bezpečí u občanů (včetně funkce záchranných složek). Obvykle jsou systémy navrženy tak, že pokud dojde k obnově funkce těchto kritických infrastruktur do 24 hodin, je situace z hlediska ochrany obyvatelstva a udržení veřejného pořádku zvládnutelná místními složkami integrovaného záchranného systému. Naopak je prokázáno (například nedávnými zkušenostmi z New Orleans, Haiti, Chile), že pokud není obnoveno uspokojení základních fyziologických potřeb a potřeba bezpečí v několika dnech, pak se s jistotou od 5. dne po katastrofě život komunity rozkládá, místní záchranné složky a policie nejsou schopny zajistit obnovu pořádku a situace se mění v humanitární katastrofu vyžadující pomoc z jiných regionů, případně i mezinárodní.

Stát vyžaduje od subjektů kritické infrastruktury zpracování Plánů krizové připravenosti, které by měly postihnout nejen zachování kontinuity, ale i usnadnit koordinaci aktivit v kritických situacích a zajistit

potřebné zdroje. Zpracování těchto plánů je v současné době spíše formální, bez hlubšího provázání jednotlivých systémů kritické infrastruktury a bez náležité informační podpory. Vzájemné závislosti mezi systémy kritické infrastruktury nejsou do hloubky prozkoumány a nejsou k dispozici modely jejich chování, vizualizace celkového stavu a rozpoznávání kritických stavů.
Stěžejní cíl 2.2: Vytvoření informační podpory, která umožní modelování vzájemných závislostí alespoň nejdůležitějších systémů kritické infrastruktury. Dosažení dřívější detekce hrozeb plynoucích ze vzájemných vazeb a závislostí, přesnější a rychlejší predikce vývoje chování a nasazení regulačních mechanismů, které minimalizují pravděpodobnost eskalace krizové situace a případného celkového kolapsu komunity s dlouhodobými následky.

	Dílčí cíl 2.2.1: Vzájemné závislostí systémů KI Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií.
	Dílčí cíl 2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Vývoj systémů predikce a včasného varování.

Oblast 3: Krizové řízení a bezpečnostní politika

Oblast zahrnuje formování a implementaci bezpečnostní politiky, rozvoj bezpečnostního systému, včasné varování, komunikaci s veřejností, připravenost, prevenci, reakci a obnovu, civilně vojenskou spolupráci a civilní nouzové plánování, moderní metody zásahového tréninku a také problematiku vnějšího krizového řízení NATO a EU.

Podoblast 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Bezpečnostní politika státu vychází z principu nedělitelnosti bezpečnosti. Základním východiskem pro zajištění bezpečnosti ČR je členství v NATO a EU a plnění spojeneckých závazků, které ze členství v obou organizacích vyplývají. Prioritně se jedná o aktivní účast v systému kolektivní obrany NATO, zapojení do Společné bezpečnostní a obranné politiky EU a rozvoj schopností EU pro zvládání krizí. Úroveň a efektivnost bezpečnostní politiky ČR zásadně určuje úroveň bezpečnostního systému, který musí reagovat na dynamický vývoj, změny a trendy v oblasti bezpečnosti, společenského a ekonomického vývoje. ČR má plně integrovaný, funkčně i zdrojově provázaný bezpečnostní systém, který je schopen efektivně působit v krizových situacích a stavech a při mimořádných událostech. Klíčovou roli má v tomto směru Integrovaný záchranný systém ČR a jeho složky. Klíčové cíle a úkoly bezpečnostní politiky jsou zároveň integrální součástí dlouhodobých rozvojových strategií rozvoje na úrovni státu a krajů.

Stěžejní cíl 3.1:

Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídících a hodnotících dokumentů v oblasti bezpečnosti, které je nutno pravidelně aktualizovat v závislosti na vývoji bezpečnostního prostředí a v závislosti na strategických prioritách bezpečnostní politiky NATO a EU. Prioritou bezpečnostní politiky je zajištění připravenosti a akceschopnosti celého bezpečnostního systému ČR (zejména IZS a AČR) za krizových situací a krizových stavů a to jak samostatně, tak i v součinnosti se spojenci v NATO a EU, a dále při řešení mimořádných událostí, přírodních a antropogenních krizových situací. Bezpečnostní systém tak musí být připraven reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.

Dílčí cíl 3.1.1: Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti

Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda) a Parlament ČR jak přistupovat k tomuto procesu.

Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby

Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).

Podoblast 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významným předpokladem pro úspěšné zajištění krizového řízení a pro tvorbu a realizaci informované bezpečnostní politiky je vyhledávání a identifikace bezpečnostních hrozeb a z nich vyplývajících rizik. V daném případě se vychází z monitorování klíčových trendů ekonomického, společenského,

sociálního, technologického a bezpečnostního vývoje, událostí, ohnisek napětí, krizí a konfliktů. Informace vyplývající z tohoto procesu se částečně promítají do tvorby a realizace bezpečnostní politiky, resp. tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Stěžejní cíl 3.2:
Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik; v dlouhodobém horizontu (2020-2030), který funguje následujícím způsobem: Pravidelně se zpracovávají prognostické studie a scénáře vývoje bezpečnostní situace, které jsou předmětem expertního posuzování. Následně se vytváří soubor opatření pro eliminaci hrozeb podpořený i tvorbou (variantních) scénářů bezpečnostního vývoje. Závěry se promítají do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR
Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Dílčí cíl 3.2.2: Podpora specifických oblastí bezpečnosti
Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků.

Podoblast 3.3: Systémy analýzy, prevence, odezvy a obnovy
Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Stěžejní cíl 3.3:
Cílem této průřezové podoblasti je zajistit pro operativní i krizové činnosti interoperabilní technologie získávání, třídění, ukládání, analýzy, zpřístupnění a zabezpečení informací a znalostí z otevřených a zpravodajských zdrojů (civilních, obranných), dále navazující informační a aplikované technologie pro efektivní využití informací a znalostí pro účinnou prevenci hrozeb a případnou odezvu včetně nouzového řízení a následné obnovy. Zpřístupnění a zabezpečení informací (pro využití v prevenci a ochraně, jakož i v krizovém řízení) musí být zajištěno podle závažnosti a klasifikace pro všechny relevantní složky v odpovídající struktuře.

	Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů.
	Dílčí cíl 3.3.2: Analýza bezpečnostních informací Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů.
	Dílčí cíl 3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti.
	Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy.

Podoblast 3.4: Legislativní a právní problémy

Vysoká úroveň bezpečnosti České republiky a jejích občanů bude do značné míry záviset na schopnosti státu dosahovat takové poznatkové, technické, technologické a manažerské úrovně, která umožní získávat, osvojovat si a rozvíjet k tomu potřebné specifické schopnosti. Vzhledem k existujícím a nově predikovaným hrozbám je nutné rozvíjet a zkvalitňovat připravenost a akceschopnost státu v oblasti krizového řízení, ochrany obyvatelstva, obrany, ochrany kritické infrastruktury, integrovaného záchranného systému ČR, boje proti terorismu, boje proti kriminalitě atd. To je potřeba činit komplexně, tedy nejen z hlediska věcné působnosti, ale současně též odpovídajícím způsobem rozvíjet a zkvalitňovat legislativní rámec upravující práva a povinnosti při přípravě na řešení a při vlastním řešení mimořádných událostí a krizových situací.

Stěžejní cíl 3.4:

Rozvíjet legislativní postupy a navrhovaná legislativní opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů a složek, aby dynamicky reagoval na nově vznikající potřeby bezpečnostního systému ČR s preferencí krizových situací spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) nebo vnitřní bezpečnosti státu a dále pak při přírodních (živelních) a antropogenních (tj. lidmi nebo lidskou činností způsobených) pohromách.

	Dílčí cíl 3.4.1: Legislativní postupy a opatření v případě ohrožení vnitřní bezpečnosti státu, mimořádných přírodních a antropogenních událostí a krizových situací Analyzovat a vytvářet legislativní postupy a opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách. To vše s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje.

Oblast 4: Obrana, obranyschopnost a nasazení ozbrojených sil

Cílem rezortu Ministerstva obrany je disponovat do roku 2020 souborem sil, který bude garantovat naplnění politicko-vojenských ambicí ČR a účinné prosazení bezpečnostních zájmů státu v souladu s právním řádem ČR. Tyto schopnosti budou náležitým způsobem rozvíjeny v následující dekádě. Do rozvoje schopností budou důsledně promítnuty koncepční záměry výstavby ozbrojených sil z Bílé knihy o obraně a závazky, které ČR převzala v rámci obranného plánování NATO a EU.
Rozvoj schopností ozbrojených sil včetně systému jejich komplexního zabezpečení závisí na zvládnuté úrovni strategie a vojenského umění velitelským sborem, stavu a vycvičenosti vojenského personálu, vybaveností jednotek moderní výzbrojí a kvalitním logistickým zabezpečením. Bojové síly, síly bojové podpory a bojového zabezpečení budou schopny plnit úkoly v operacích od nízké po vysokou intenzitu (tj. v plném spektru operací), budou připraveny působit v prostoru nasazení koordinovaně s civilními aktéry vládního i nevládního charakteru v duchu komplexního přístupu (Comprehensive Approach), budou interoperabilní se spojenci, nasaditelné na strategické vzdálenosti, dlouhodobě udržitelné, se zajištěným velením a bezpečným přenosem dat v prostředí NEC, s vysokým stupněm univerzálnosti použití, modularity a odolnosti proti působení protivníka.
Systém obrany státu a krizového řízení v rezortu MO bude postupně optimalizován a bude udržovat svou schopnost pohotově a adekvátně reagovat na ohrožení v kontextu kolektivního zajišťování obrany státu.

Podoblast 4.1: Rozvoj schopností ozbrojených sil

Rozvoj schopností ozbrojených sil včetně systému jejich komplexního zabezpečení závisí na zvládnuté úrovni strategie a vojenského umění velitelským sborem, stavu a vycvičenosti vojenského personálu, vybaveností jednotek moderní výzbrojí a kvalitním logistickým zabezpečením. Bojové síly a síly bojové podpory a bojového zabezpečení budou schopny plnit úkoly v operacích od nízké po vysokou intenzitu (tj. v plném spektru operací), budou připraveny působit v prostoru nasazení koordinovaně s civilními aktéry vládního i nevládního charakteru v duchu komplexního přístupu (Comprehensive Approach), budou interoperabilní se spojenci, nasaditelné na strategické vzdálenosti, dlouhodobě udržitelné, se zajištěným velením a bezpečným přenosem dat v prostředí NEC, s vysokým stupněm univerzálnosti použití, modularity a odolnosti proti působení protivníka. Schopnosti vyjadřují způsobilost ozbrojených sil efektivně působit v krizových situacích a válečných konfliktech. Jedná se o:

- schopnosti, které Česká republika deklaruje jako svou specializaci v rámci NATO a EU, případně sdílené schopnosti s některým z členských států NATO nebo EU;
- schopnosti identifikované Organizací NATO pro výzkum a vývoj technologií (NATO RTO) a Evropskou obrannou agenturou (EDA) jako klíčové pro rozvoj ozbrojených sil;
- oblasti, kde již Česká republika disponuje potenciálem pro výzkum a vývoj (např. kybernetika, robotika, nanotechnologie, aktivní a pasivní ochrana jednotlivce a techniky, zbraně hromadného ničení);
- schopnost personálně řídit a rozvíjet ozbrojené síly též s podporou sociologického sledování a průzkumu a schopnost strategické analýzy trendů mezinárodní bezpečnosti, povahy rizik a ohrožení, charakteru konfliktů a role ozbrojených sil i civilních aktérů v nich.

Mezi významné faktory rozvoje kapacit ozbrojených sil patří kromě spojeneckého charakteru jejich působení (dnes se odrážejícího v účasti na expedičních misích NATO, systému NATINADS nebo misích SBOP) zejména bezpečnostní trendy jako tzv. nové války, asymetrická povaha globálních hrozeb, proměnlivé modality nasazení (tzv. *comprehensive approach*) nebo dopady ekonomické stagnace na vojenské výdaje, úvahy o vzniku společného evropského zbrojního trhu nebo kapacit tzv. *pooling and sharing* na regionální úrovni či rozvíjení evropské technologické báze mj. prostřednictvím EDA.

Stěžejní cíl 4.1: Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.	
	Dílčí cíl 4.1.1: Vývoj nových zbraňových a obranných systémů Cílem je hledání a realizace vhodného konceptu ochrany a obrany prostoru ČR, a to vlastními silami a prostředky a nebo zapojením se do mezinárodních projektů, které přinesou zejména úsporu personálu a zvýší efektivnost schopností ozbrojených sil.
	Dílčí cíl 4.1.2: Přeprava, mobilita a udržitelnost sil Cílem je rozvíjet a zdokonalovat metody, postupy, technická a jiná řešení, která povedou k vyšší mobilitě a dlouhodobé udržitelnosti sil v operacích. Ta je zejména spojena s ochrannou živé síly. Proto je cílem i vývoj a zdokonalování prostředků aktivní i pasivní ochrany živé síly a vojenské techniky v celém spektru operací, jako např. výstroj, výzbroj, prostředky balistické ochrany, individuální i kolektivní prostředky ochrany proti ZHN a maskování.
	Dílčí cíl 4.1.3: Podpora velení a řízení Cílem je rozvoj systémů velení a řízení v operacích umožňujících získání společného přehledu o vývoji situace s aliančními partnery a informační převahy nad protivníkem. Rozvoj technických a jiných řešení, která povedou ke zvýšení efektivnosti řízení rezortu MO, zejména k personálním úsporám. Modernizace a rozvoj zpravodajského, geografického a hydrometeorologického zabezpečení s důrazem na implementaci systému Intelligence, Surveillance, and Reconnaissance.
	Dílčí cíl 4.1.4: Rozvoj KIS a kybernetická obrana Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací.

4.2 Systémová opatření a další návrhy expertního panelu

Spolu s prioritními dílčími cíli byla v prioritní oblasti „Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR“ identifikována doprovodná opatření a jiné možnosti, které napomohou a usnadní dosáhnout stanovených dílčích a stěžejních cílů. Tato doprovodná opatření a jiné možnosti mají charakter převážně systémových opatření a doporučení.

Souhrn navržených doprovodných opatření pro prioritní oblast Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR:

- Optimalizace alokace zdrojů.
- Optimalizace funkčnosti integrovaného záchranného systému (IZS).
- Stabilizace jednotlivých složek IZS.
- Modernizace technických a technologických systémů.
- Zvýšení vzdělanosti a informační úrovně obyvatelstva, fyzických a právnických osob v oblasti mimořádných událostí a krizových situací.
- Zlepšení participace soukromých subjektů a/nebo poskytovatelů bezpečnosti v případech mimořádných situací a krizových stavů.
- Vytváření kapacit pro zajištění nouzové úrovně služeb.
- Aplikace managementu kontinuity činností v organizacích kritické infrastruktury.
- Zajištění mezinárodní spolupráce a interoperability na technické i organizační úrovni.
- Implementace legislativních aktů EU a strategických dokumentů EU a NATO do legislativy ČR a strategických a řídících dokumentů ČR v oblasti bezpečnosti.
- Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik v dlouhodobém horizontu a v tomto rámci příprava scénářů vývoje bezpečnostní situace a monitoring nově se objevujících společenských a technologických rizik, zvláště v intenzivně se rozvíjejících oblastech (nanotechnologie, biotechnologie, energetika, informační technologie), včetně možností jejich společenského zneužití.
- Zefektivnění náboru, přípravy, výcviku a vzdělávání vojenského personálu adekvátně trendům vedení operací.
- Řízení personálního procesu a zajištění kvalitního psychologického servisu pro vojáky a jejich blízké nutného z hlediska jejich specifické psychické zátěže v operacích.
- Udržení kvality života vojáků po ukončení jejich aktivní vojenské služby.

Oblast 1: Ochrana obyvatelstva

V oblasti Ochrana obyvatelstva byla navržena opatření směřující zejména k optimalizaci integrovaného záchranného systému (IZS), včetně alokace zdrojů a stabilizace jednotlivých složek IZS.

- Optimalizace alokace zdrojů.
- Optimalizace funkčnosti IZS.
- Stabilizace jednotlivých složek IZS.
- Modernizace technických a technologických systémů.
- Zvýšení vzdělanosti a informační úrovně obyvatelstva, fyzických a právnických osob v oblasti mimořádných událostí a krizových situací.
- Zlepšení participace soukromých subjektů a/nebo poskytovatelů bezpečnosti v případech mimořádných situací a krizových stavů.

Oblast 2: Bezpečnost kritických infrastruktur a zdrojů

V oblasti Bezpečnost kritických infrastruktur a zdrojů byla navržena opatření směřující k zajištění nouzové úrovně služeb v organizacích kritické infrastruktury.

- Optimalizace alokace zdrojů.
- Vytváření kapacit pro zajištění nouzové úrovně služeb.
- Aplikace managementu kontinuity činností v organizacích kritické infrastruktury.

Oblast 3: Krizové řízení a bezpečnostní politika

V oblasti Krizové řízení a bezpečnostní politika byla navržena opatření směřující zejména k zajištění mezinárodní spolupráce a interoperability v oblasti bezpečnosti a k zajištění monitoringu nově se objevujících společenských a technologických rizik.

- Optimalizace alokace zdrojů.
- Zajištění mezinárodní spolupráce a interoperability na technické i organizační úrovni.
- Implementace legislativních aktů EU a NATO do legislativy ČR a strategických řídících dokumentů ČR v oblasti bezpečnosti.
- Zvýšení adaptability bezpečnostního systému na změna v bezpečnostním prostředí.
- Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik v dlouhodobém horizontu a v tomto rámci příprava scénářů vývoje bezpečnostní situace a monitoring nově se objevujících společenských a technologických rizik, zvláště v intenzivně se rozvíjejících oblastech (nanotechnologie, biotechnologie, energetika, informační technologie), včetně možností jejich společenského zneužití.

Oblast 4: Obrana, obranyschopnost a nasazení ozbrojených sil

V oblasti Obrana, obranyschopnost a nasazení ozbrojených sil byla navržena opatření směřující zejména do personální oblasti s ohledem na specifika vojenského personálu.

- Zefektivnění náboru, přípravy, výcviku a vzdělávání vojenského personálu adekvátně trendům vedení operací.
- Řízení personálního procesu a zajištění kvalitního psychologického servisu pro vojáky a jejich blízké nutného z hlediska jejich specifické psychické zátěže v operacích.
- Udržení kvality života vojáků po ukončení jejich aktivní vojenské služby.

4.3 Indikátory pro kontrolu dosahování cílů

Na úrovni stěžejních cílů byly expertním panelem navrženy indikátory, které umožní hodnocení a kontrolu jejich naplňování.

Podoblast	Indikátory
Podoblast 1.1: Ochrana obyvatelstva **Stěžejní cíl 1.1:** Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.	• Úroveň spokojenosti občanů s ochranou obyvatelstva v případě živelních pohrom a provozních havárií (Zdroj: CVVM AV ČR); • Absolutní hodnoty uchráněné při požárech (Zdroj: MV-GŘ HZS ČR); • Podíl podniků s produkty v oblasti bezpečnostních a záchranných složek (Zdroj: ČSÚ); • Počet osob zachráněných jednotkami požární ochrany (Zdroj: MV-GŘ HZS ČR); • Početní druhové mimořádné události a krizové situace se zásahy jednotek požární ochrany (Zdroj: MV-GŘ HZS ČR); • Počet a rozsah realizovaných preventivních opatření v ochraně obyvatelstva (Zdroj: orgány veřejné správy);
Podoblast 1.2: Ochrana před kriminalitou, extremismem a terorismem **Stěžejní cíl 1.2:** Stěžejním cílem této oblasti je vybudovat v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře eliminovat všechny formy kriminality, extremismu a terorismu, což vyžaduje vyvážený systém prevence a represe a současně sledování trendů, kterými se vývoj kriminality, extremismu a terorismu ubírá (včetně využití technologií či zneužití digitálních informací kriminálníky, adaptace kriminální sféry na nové demografické podmínky, mapování míry nehlášené kriminality a korupce apod.), a nástrojů jejího odhalování a potírání.	• Přijetí odpovídající legislativy a její využívání judikaturou; • Dotvoření bezpečnostního systému v oblasti boje proti kriminalitě, extremismu a terorismu; • Prevence násilného extremismu a terorismu, odhalování a případné zvládání následků teroristických útoků (Zdroj: ad hoc analýzy srovnávajícího potenciál a reálné pokusy o útoky); • Pokles trestné činnosti a zvýšení její objasněnosti (Zdroj: Zpráva o bezpečnostní situaci na základě evidence kriminality); • Zvýšení pocitu bezpečnosti občanů (Zdroj: Výzkumy CVVM); • Pokles extremistických akcí a deliktů (Zdroj: Zpráva o problematice extremismu v ČR na základě údajů bezpečnostních složek); • Zvýšení pocitu bezpečnosti u skupin ohrožených extremismem (Zdroj: ad hoc sociologická šetření, údaje specializovaných úřadů, např. Vládní agentury pro sociální začleňování apod.); • Statistiky teroristických útoků (Zdroj: vyhodnocení vládní Strategie boje proti terorismu);

Podoblast 2.1: Ochrana, odolnost a obnova kritických infrastruktur **Stěžejní cíl 2.1:** Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.	• Počet organizací – dodavatelů nezbytných výrobků prací a služeb – s certifikovaným systémem managementu kontinuity (Zdroj: krizové plány); • Snížení velikosti dopadu krize se zahrnutím KI a počet odvrácených hrozeb; • Snížení počtu a rozsahu selhání (i dílčích nebo krátkodobých) prvků KI;
Podoblast 2.2: Komunikace a vazby mezi kritickými infrastrukturami **Stěžejní cíl 2.2:** Vytvoření informační podpory, která umožní modelování vzájemných závislostí alespoň nejdůležitějších systémů kritické infrastruktury. Dosažení dřívější detekce hrozeb plynoucích ze vzájemných vazeb a závislostí, přesnější a rychlejší predikce vývoje chování a nasazení regulačních mechanismů, které minimalizují pravděpodobnost eskalace krizové situace a případného celkového kolapsu komunity s dlouhodobými následky.	• Počet případů, kdy byla na základě informační podpory provedena adekvátní preventivní nebo represivní opatřen, a rozsah těchto opatření; • Počet a velikost aplikovaných databází, map a metodik; • Snížení velikosti dopadu krize se zahrnutím KI a počet odvrácených hrozeb;

Podoblast 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR **Stěžejní cíl 3.1:** Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídících a hodnotících dokumentů v oblasti bezpečnosti, které je nutno pravidelně aktualizovat v závislosti na vývoji bezpečnostního prostředí a v závislosti na strategických prioritách bezpečnostní politiky NATO a EU. Prioritou bezpečnostní politiky je zajištění připravenosti a akceschopnosti celého bezpečnostního systému ČR (zejména IZS a AČR) za krizových situací a krizových stavů a to jak samostatně, tak i v součinnosti se spojenci v NATO a EU, a dále při řešení mimořádných událostí, přírodních a antropogenních krizových situací. Bezpečnostní systém tak musí být připraven reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.	• Optimalizace finančních prostředků vydávaných na zajištění bezpečnosti a obrany, fungování bezpečnostní ho systému; • Stav zajištění bezpečnosti/bezpečí občanů (např. pokles/zvýšení kriminality, akceschopnost při zajišťování zdraví a majetku občanů, při zajišťování ochrany kritické infrastruktury, apod.); • Schopnost plnit spojenecké závazky vůči EU a NATO;
Podoblast 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření **Stěžejní cíl 3.2:** Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik; v dlouhodobém horizontu (2020-2030), který funguje následujícím způsobem: Pravidelně se zpracovávají prognostické studie a scénáře vývoje bezpečnostní situace, které jsou předmětem expertního posuzování. Následně se vytváří soubor opatření pro eliminaci hrozeb podpořený i tvorbou (variantních) scénářů bezpečnostního vývoje. Závěry se promítají do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	• Počet a kvalita obsahu nově zpracovaných strategických a řídících dokumentů v oblasti bezpečnosti; • Počet a kvalita nových opatření k eliminaci hrozeb; • Míra připravenosti složek bezpečnostního systému čelit širšímu spektru hrozeb a rizik;
Podoblast 3.3: Systémy analýzy, prevence, odezvy a obnovy **Stěžejní cíl 3.3:** Cílem této průřezové podoblasti je zajistit pro operativní i v krizové činnosti interoperabilní technologie získávání, třídění, ukládání, analýzy, zpřístupnění a zabezpečení informací a znalostí z otevřených a zpravodajských zdrojů (civilních, obranných),	• Míra připravenosti složek bezpečnostního systému čelit širšímu spektru hrozeb a rizik; • Stav zajištění bezpečnosti/bezpečí občanů (akceschopnost při zajišťování zdraví a majetku občanů, při zajišťování ochrany kritické infrastruktury apod.);

dále navazující informační a aplikované technologie pro efektivní využití informací a znalostí pro účinnou prevenci hrozeb a případnou odezvu včetně nouzového řízení a následné obnovy. Zpřístupnění a zabezpečení informací (pro využití v prevenci a ochraně, jakož i v krizovém řízení) musí být zajištěno podle závažnosti a klasifikace pro všechny relevantní složky v odpovídající struktuře.	
Podoblast 3.4: Legislativní a právní problémy **Stěžejní cíl 3.4:** Rozvíjet legislativní postupy a navrhovaná legislativní opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů a složek, aby dynamicky reagoval na nově vznikající potřeby bezpečnostního systému ČR s preferencí krizových situací spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) nebo vnitřní bezpečnosti státu a dále pak při přírodních (živelních) a antropogenních (tj. lidmi nebo lidskou činností způsobených) pohromách.	• Počet právních předpisů, norem, směrnic a předpisů nelegislativní povahy spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) nebo vnitřní bezpečnosti státu a dále pak při přírodních (živelních) a antropogenních (tj. lidmi nebo lidskou činností způsobených) pohromách. (Zdroj: MV ČR a MO ČR); • Úroveň spokojenosti obyvatel a dalších subjektů se stavem legislativy;
Podoblast 4.1: Rozvoj schopností ozbrojených sil **Stěžejní cíl 4.1:** Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.	• Doba plné funkčnosti IS pod kybernetickou ochranou za rok v odpovědnosti NBÚ (Zdroj: NBÚ a jednotlivé ministerské CIRC); • Finanční hodnota materiálu, k jehož obchodu je třeba speciální povolení vydané MPO a MO, vyrobeného a vyvezeného po roce 2012 z ČR za daný rok (Zdroj: MPO, ČSÚ); • Počet incidentů (útok, výbuch EOD), při kterých je ohrožen život nebo zdraví vojáka v prostoru nasazení, ve srovnání s počtem mrtvých nebo raněných vojáků v těchto incidentech (Zdroj: MO);

4.4 Návrh orientační výše finančních nákladů pro dosažení cílů

Na úrovni oblastí a podoblastí bylo expertním panelem navrženo poměrné rozdělení finančních prostředků.

Oblast	Podíl finančních prostředků	Podoblast	Podíl finančních prostředků
1. Bezpečnost občanů	**30 %**	1.1 Ochrana obyvatelstva	**20 %**
		1.2 Ochrana před kriminalitou, extremismem a terorismem	**10 %**
2. Bezpečnost kritických infrastruktur a zdrojů	**28 %**	2.1 Ochrana, odolnost a obnova kritických infrastruktur	**23 %**
		2.2 Komunikace a vazby mezi kritickými infrastrukturami	**5 %**
3. Krizové řízení a bezpečnostní politika	**27 %**	3.1 Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR	**4 %**
		3.2 Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření	**5 %**
		3.3 Systémy analýzy, prevence, odezvy a obnovy	**17 %**
		3.4 Legislativní a právní problémy	**1 %**
4. Obrana,, obranyschopnosti a nasazení ozbrojených sil	**15 %**	4.1 Rozvoj schopností ozbrojených sil	**15 %**
Celkem	**100 %**		**100 %**

5. Přílohy

V přílohové části Závěrečné zprávy expertního panelu prioritní oblasti „Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR“ jsou zařazeny následující přílohy:

- Příloha 1: Strukturace prioritní oblasti po první fázi;
- Příloha 2: Prioritizace cílů;
    - 2.1 Kritéria významnosti a dosažitelnosti;
    - 2.2 Výsledky hlasovací procedury expertního panelu;
- Příloha 3: Schéma finální struktury prioritní oblasti „Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR;
- Příloha 4: Identifikační listy prioritních dílčích cílů.

Příloha 1: Strukturace prioritní oblasti po první fázi

Oblast 1: Bezpečnost občanů

Oblast zahrnuje terorismus, organizovanou kriminalitu, další formy závažné kriminality ohrožující bezpečnost státu a jejich potírání, ochranu obyvatelstva, bezpečnost měst a obcí v případě živelných pohrom a provozních havárií včetně bezpečnosti podzemních objektů, ochranu občanů proti kriminalitě, protispolečenskému jednání a socio-patologickým jevům, kybernetickou kriminalitu a on-line vyšetřování, nešíření zbraní hromadného ničení a malých střelných zbraní, technologie a metody detekce chemických, biologických a radiologických látek, jaderných materiálů a výbušnin, a v neposlední řadě také socio-ekonomické a etické aspekty bezpečnosti.

Podoblast 1.1: Ochrana obyvatelstva

Ochrana obyvatelstva patří mezi prioritní oblasti bezpečnosti České republiky a zahrnuje soubor činností a postupů věcně příslušných orgánů státní správy a samosprávy a dalších zainteresovaných organizací, složek a obyvatelstva, prováděných s cílem minimalizace negativních dopadů možných mimořádných událostí a krizových situací způsobených antropogenními hrozbami (průmyslové, radiační a ekologické havárie, požáry, velké migrace obyvatelstva, mezinárodní ozbrojené konflikty, použití a zneužití zbraní hromadného ničení CBRNE, velké sociální konflikty apod.) nebo přírodními hrozbami (živelní pohromy - povodně, vichřice, sesuvy půdy, lesní požáry apod.) na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. Tyto pohromy mohou mít kromě ohrožení bezpečnosti**,** životů a zdraví obyvatel a jejich majetku a životního prostředí dopad na ekonomiku země, zásobování energií, surovinami, pitnou vodou, či mohou způsobit poškození kritické infrastruktury, narušení počítačových sítí, přenosu dat a informací. Uvedené mimořádné události a krizové situace mohou být vzájemně závislé a synergické.

Stěžejní cíl 1.1:

Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

	Dílčí cíl W1.1.1: Podpora opatření a úkolů ochrany obyvatelstva Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Ekonomie Bezpečnostní technologie Civilní nouzové plánování
	Dílčí cíl W1.1.2: Zdokonalování služeb a prostředků ochrany	**Časový horizont:** 2030

	obyvatelstva Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR. Optimalizovat alokaci zdrojů.	(průběžně) **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Ekonomie Bezpečnostní technologie Civilní nouzové plánování
	Dílčí cíl W1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; zvyšování úrovně systému výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování; zvyšování úrovně problémově orientovaných komunikačních a informačních systémů; zvyšování úrovně zabezpečení životů a zdraví při mimořádných a krizových situacích.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Ekonomie Bezpečnostní technologie Civilní nouzové plánování

Podoblast 1.2: Ochrana před kriminalitou

Objem zjištěné trestné činnosti v ČR setrvale klesá, nicméně celá oblast vyžaduje trvalé úsilí. Kriminální scéna prochází permanentním procesem adaptace na nové sociální a technologické impulsy. Kriminalita díky volnému pohybu osob v EU i díky celkové globalizaci nabyla výrazně transnacionální rozměr. Lze se i důvodně domnívat, že objem celkové trestné činnosti je podstatně vyšší než zjištěný. Veřejnost řadu případů neoznamuje, mnoho případů latentní kriminality (např. kriminalita proti duševnímu vlastnictví, korupce) je obecně tolerováno. Organizované zločinecké skupiny patří k nejprogresivnějším uživatelům moderních informačních a komunikačních technologií. V této oblasti lze mj. očekávat nárůst kybernetických útoků ze strany mezinárodních organizovaných skupin a vzrůst rizik spojených se zneužíváním osobních údajů, záznamů a digitální identity uživatelů, či s jejich vývozem za hranice ČR.

V rámci potírání kriminality je důležité trvale analyzovat a precizovat zákonná pravidla kriminalitě předcházející či ji potírající. Oběti trestné činnosti se v určitých ohledech těší menšímu rozsahu práv, než osoby obviněné či odsouzené. V souvislosti s kriminalitou jsou v ČR diskutována např. témata (de-)kriminalizace návykových látek, rozsahu „práva na zbraň“, a míry státní regulace téhož.

V ČR působí řada institucí bojujících proti kriminalitě, které jsou napojeny na evropský a globální bezpečnostní systém, nicméně nejsou stabilizovány. Policie ČR prochází reformním procesem v souvislosti s úspornými opatřeními. ČR vytvořila systém tří zpravodajských služeb, který je ale předmětem permanentních diskusí. V problematické situaci je sektor vězeňství, kde existuje nadměrná přeplněnost stávajících věznic. Celkově nebyl podrobně definován komplexní systém institucí v oblasti vnitřní bezpečnosti.

Stěžejní cíl 1.2:

Stěžejním cílem této oblasti je vybudovat v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře eliminovat všechny

formy kriminality, což vyžaduje vyvážený systém prevence a represe a současně sledování trendů, kterými se vývoj kriminality ubírá (včetně využití technologií či zneužití digitálních informací kriminálníky, adaptace kriminální sféry na nové demografické podmínky, mapování míry nehlášené kriminality a korupce apod.), a nástrojů jejího odhalování a potírání.

	Dílčí cíl W1.2.1: Vytváření účinných metod analýzy druhů a rozšířenosti kriminality a implementace efektivních nástrojů jejího potírání Cílem je • Optimalizace systému boje proti kriminalitě; • Rozvoj nástrojů analýzy hrozeb, rizik a rozšířenosti kriminality, včetně kriminality organizované; • Rozvoj nových technik a technologií pro odhalování a dokazování trestných činů; • Rozvoj nástrojů zjištění stavu a dynamiky vývoje organizované kriminality na území ČR, včetně jejího propojení s hospodářskou kriminalitou; • Vymezení hranice mezi zjištěnou a nezjištěnou trestnou činností v rámci České republiky a snížení objemu nezjištěné kriminality; • Zmapování trendů a vytvoření nástrojů pro odhadování skutečné trestné činnosti (s ohledem na regiony, na socioekonomický vývoj, s ohledem na určité skupiny skutkových podstat, struktura pachatelů a obětí); • Definování, uplatnění a vyhodnocení efektivity protiopatření vůči kriminalitě.	**Časový horizont:** 2020 **Výzkumné směry** Kriminalistika Kriminologie Sociologie Ekonomie Biologie Chemie Informatika Právo
	Dílčí cíl W1.2.2: Minimalizace kybernetické kriminality a zneužívání informací Cílem je • Vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; • Koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům.	**Časový horizont:** 2020 **Výzkumné směry** Informatika Kriminalistika Kriminologie Ekonomie
	Dílčí cíl W1.2.3: Vyhodnocování dopadů právních úprav na kriminalitu a její trendy Cílem je • Rozvoj efektivních nástrojů pro zmapování dopadu právních úprav na míru kriminality a možnosti jejího potírání a pro zpětnou vazbu do legislativních procesů; • Vytváření a trvalé vyhodnocování legislativních nástrojů pro prevenci a potírání nových forem kriminality; Vytváření nástrojů analýzy legislativního rámce a jeho dopadů v oblasti zajištění vlastní bezpečnosti ze strany jednotlivce a státní regulace těchto práv.	**Časový horizont:** 2020 **Výzkumné směry** Právo Sociologie Kriminologie Informatika

Podoblast 1.3: Ochrana před extremismem

Problematika extremismu je natolik komplexní, že není možné se zaměřit na její potírání pouze represivními prostředky. Příčinami extremismu může být řada kulturních a socioekonomických trendů a skutečností. Bez integrovaných preventivních aktivit je úspěšný boj proti extremismu předem ztracený. Extremistická scéna citlivě reaguje na nálady ve společnosti jako celku a dovedně je využívá (krajní levice: hospodářská krize; krajní pravice: existence problematických sociálně vyloučených komunit). V české společnosti existují i extremistické skupiny, které usilují o odstranění demokratického ústavního státu. Jejich aktivity mohou sledovat quasilegální cestu k dosažení moci ve volbách, některé z nich však používají i násilné prostředky a mohou se uchýlit i k terorismu. V některých oblastech ČR vzniká interetnické napětí, kterého extremisté využívají ke své profilaci. V souvislosti s pokračující imigrací lze přepokládat i nárůst významu tohoto tématu pro domácí extremisty na straně jedné, a současně výraznější projevy extremismu v přistěhovaleckých diasporách na straně druhé. Extremistické subkultury patří mezi nejprogresivnější uživatele moderních informačních a komunikačních technologií. Extremismu jsou věnovány specializované strategické materiály (např. Koncepce boje proti extremismu), jejichž dopad není vždy zcela přesvědčivý, a plnění mnoha v nich obsažených stěžejních úkolů je odkládáno nebo se omezuje na pouhé proklamace.

Stěžejní cíl 1.3:

Stěžejním cílem této oblasti je vytvořit tolerantní společnost podporující demokratické mechanismy a hodnoty, která bude schopna eliminovat projevy extremismu, a to pokud možno preventivní cestou a diskursivním působením. Proti nebezpečným formám extremismu (zvláště násilným, včetně těch, které užívají teroristické metody) však musí mít společnost k dispozici efektivní nástroje ochrany.

	Dílčí cíl W1.3.1: Analýza hrozeb a rizik extremismu Cílem je: • Rozvoj metodiky analýzy jednotlivých forem extremismu v ČR, především dynamiky jejich vývoje; • Provádění analýzy příčin, průběhu a dopadů etnických, náboženských a sociálních konfliktů (v regionálním i globálním kontextu) a potenciálu pro jejich eskalaci do budoucna, zejména v kontextu imigrace do ČR.	**Časový horizont:** 2020 **Výzkumné směry** Sociologie Religionistika Informatika Právo
	Dílčí cíl W1.3.2: Vytváření efektivních nástrojů prevence extremismu a účinných protiopatření vůči němu Cílem je • Optimalizace systému prevence a potírání extremismu; • Koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti extremismu, vyhodnocování efektivity těchto nástrojů; • Zlepšování systému pro rozpoznávání a odhalování nových forem extremismu a entit jemu podléhajících.	**Časový horizont:** 2020 **Výzkumné směry** Informatika Kriminalistika Kriminologie Ekonomie

Podoblast 1.4: Ochrana před terorismem

Terorismus představuje závažnou bezpečnostní hrozbu s potencionálem významného ohrožení obyvatel České republiky a jejích klíčových spojenců v EU a NATO. Dosavadní velmi nízký počet teroristických útoků spáchaných na území ČR se nesmí stát důvodem k sebeuspokojení s kvantitou i kvalitou stávajících opatření v boji proti terorismu. Zejména vzhledem k členství ČR v mezinárodních organizacích (NATO, EU) a jejich operacím mimo území svých členských států nelze do budoucna vyloučit zvýšení rizika teroristických útoků i na území ČR či bezprostředně sousedících států. Ochrana

obyvatelstva před teroristickými útoky a jejich případnými následky je proto jednou z bezpečnostních priorit České republiky. Boj proti terorismu nejen na území České republiky je rovněž vyjádřením naší solidarity se spojenci, z nichž mnozí dlouhodobě čelí výrazně většímu počtu teroristických útoků na svém území.

Mezinárodní spolupráce v boji proti terorismu je v dnešním světě nutností i vzhledem k existenci globálně působících teroristických skupin a otevřenosti hranic v rámci EU. Je proto nutné, aby opatření přijatá Českou republikou nechránila pouze jeho obyvatelstvo, nýbrž i zamezila pobytu, tranzitu, financování a případné rekrutaci členů teroristických skupin páchajících své útoky v zahraničí. Teroristé navíc mají vždy výhodu překvapení a neustále hledají nové možnosti a způsoby svého působení, včetně zneužívání moderních technologií. Relativně nový rozměr ohrožení obyvatelstva České republiky a jeho spojenců proto představují i potencionální teroristické útoky na kritickou infrastrukturu státu, či možnost zneužití chemických, biologických, radioaktivních látek a jaderných materiálu teroristy.

Nutnou podmínkou pro dlouhodobou realizaci všech opatření v boji proti terorismu je i existence efektivních mechanismů pro jejich monitoring a kontrolu a to nejen z hlediska jejich efektivity a zdrojové náročnosti, nýbrž i z hlediska jejich dopadů na osobní svobody jednotlivých obyvatel a fungování demokratické společnosti jako celku.

Stěžejní cíl 1.4:

Snížení rizika ohrožení obyvatelstva ČR teroristickým útokem na přijatelnou úroveň při zachování principů demokratického právního státu zlepšením koordinace a spolupráce všech relevantních aktérů na národní i mezinárodní úrovni, zejména v rámci protiteroristických politik EU a NATO; neustálou inovací a adaptací systémů ochrany kritické infrastruktury s ohledem na aktuální teroristické hrozby, včetně potencionálního zneužití chemických, biologických, radioaktivních látek a jaderných materiálů teroristy nejen na území ČR; rozšířením a zdokonalením schopností IZS při reakcích na následky teroristického útoku na území ČR s důrazem na ochranu obyvatelstva a kritické infrastruktury; zvýšením efektivnosti opatření zamezujících zneužití území a obyvatelstva ČR k pobytu, tranzitu a financování terorismu.

	Dílčí cíl W1.4.1: Optimalizace alokace zdrojů a zvýšení efektivity opatření v boji proti terorismu Cílem je optimalizace alokace zdrojů a zvýšení efektivity opatření v boji proti terorismu na národní i nadnárodní úrovni, zejména s ohledem na zamezení zneužití území ČR k pobytu, tranzitu a financování terorismu se zaměřením na stav a dynamiku vývoje hrozby terorismu na území ČR, včetně jejího propojení na zahraniční a/nebo nadnárodní teroristické skupiny. Zvyšování přidané hodnoty opatření v boji proti terorismu na mezinárodní úrovni, zejména pak v rámci EU, NATO, OSN a dalších relevantních mezinárodních organizací, na základě komparace efektivity a nákladnosti opatření na mezinárodní a národní úrovni. Identifikace a minimalizace negativních etických, sociálních a lidsko-právních aspektů všech opatření v boji proti terorismu.	**Časový horizont:** 2020 **Výzkumné směry** Kriminologie Právní vědy Bezpečnostní vědy Ekonomie Filosofie a sociologie (vztah bezpečnosti a svobody)
	Dílčí cíl W1.4.2: Využití nových technologií v boji proti terorismu Cílem je identifikovat již existují i teprve vznikající technologie uplatnitelné ve všech oblastech boje proti terorismu. Identifikace a minimalizace negativních etických, sociálních a lidsko-právních aspektů případného využití nových technologií v boji proti terorismu	**Časový horizont:** 2020 **Výzkumné směry** Právní vědy Bezpečnostní vědy Bezpečnostní technologie Právo bezpečnostních technologií Informatika

Podoblast 1.5: Sociálně-ekonomické aspekty bezpečnosti

Pod socioekonomické aspekty bezpečnosti spadá problematika

- bezpečnosti měst a obcí před účinky živelních pohrom a provozních havárií,
- ekonomiky bezpečnosti,
- privatizace bezpečnosti,
- etiky, svobody a sociálních aspektů bezpečnosti.

Bezpečnost měst a obcí před účinky živelních pohrom a provozních havárií je spjata s rozvojovými programy území a s územním plánováním, a to s ohledem na rozvoj území a jeho bezpečnost. Zahrnuje řízení lidských aktivit z hlediska udržitelného rozvoje, což má přínosy nejen v posílení bezpečnosti, ale také v oblasti bydlení, životního prostředí, v ekonomickém rozvoji, rozvoji podnikatelských aktivit a získávání investic, rozvoji technické a dopravní infrastruktury území a rozvoji analytických a hodnotících nástrojů.

Ekonomika bezpečnosti se odvíjí od definování bezpečnostních zájmů, cílů bezpečnostní politiky a schopností složek bezpečnostního systému (zejména na ústřední úrovni) je efektivně realizovat. Reflektuje také fakt, že podobně jako stát coby poskytovatel bezpečnosti svého obyvatelstva i všichni aktéři obyvatelstvo ohrožující potřebují ke svému fungování lidské, finanční a materiální zdroje. Předmětem zájmu je proto lepší poznání zdrojové základny a ekonomické motivace aktérů, kteří bezpečí obyvatelstva ČR ohrožují. Zároveň je předmětem zájmu plánování, alokace a efektivita využití všech zdrojů poskytovateli bezpečnosti, kterými dnes již nejsou pouze složky státní správy, nýbrž i mnozí aktéři soukromého sektoru. Pokud budou preventivní opatření ke zvyšování odolnosti společnosti integrovány do praxe v oblasti územního plánování, územního řízení a stavebního řízení, lze dosáhnout nižších nákladů na zajištění bezpečnosti obyvatelstva, než při budování dodatečných bezpečnostních opatření. V případě obnovy po následcích pohrom by mělo být zásadou nikoliv prosté uvedení území a jeho infrastruktury do původního stavu, ale na základě poučení z průběhu pohromy by mělo být po obnově dosaženo vyšší odolnosti pro případ jejího opakování.

Rostoucí roli široké škály soukromých aktérů při zabezpečení ochrany obyvatelstva je nutno pečlivě analyzovat s ohledem na fakt, že jejich primární motivací je maximalizace soukromého zisku, nikoliv veřejné bezpečnosti všech obyvatel ČR. Zejména je proto třeba detailně analyzovat proces privatizace bezpečnosti v těch oblastech, které se přímo dotýkají majetku, zdraví a/nebo základních lidských práv obyvatelů ČR a to i s ohledem na jasné vymezení legislativních mantinelů pro působení soukromých společností při poskytování stále širší škály bezpečnostních služeb.

Opatření a metody v oblasti bezpečnosti jsou obecně velmi citlivými nástroji, a proto je třeba při jejich používání respektovat etické zásady a možné sociální dopady na různé skupiny obyvatel ČR. Nutnou podmínkou je proto i existence efektivních mechanismů pro monitoring a kontrolu všech opatření přijímaných k zajištění ochrany obyvatelstva a to nejen z hlediska jejich efektivity a zdrojové náročnosti, nýbrž i z hlediska jejich dopadů na osobní svobody jednotlivých obyvatel a fungování demokratické společnosti jako celku. Práce s médii představuje významný nástroj pro informování široké veřejnosti a pro vytváření názorů a postojů obyvatelstva. Základní práva jednotlivce ani svobodný přístup k informacím nemohou být omezovány kromě situací nejvyšší nutnosti, jejíž existence musí být legitimizována instrumenty vnější demokratické kontroly (přinejmenším parlamentní).

Stěžejní cíl 1.5:

Zajistit bezpečí a rozvoj chráněných zájmů měst a obcí s důrazem na aktivní chování, monitoring a na procesní řízení při živelních pohromách a provozních haváriích.

Reakce na bezpečnostní hrozby a přijatá opatření splňují požadavky efektivity při vynakládání finančních prostředků v jednotlivých oblastech bezpečnosti státu. Integrace preventivních bezpečnostních opatření do praxe v oblasti územního plánování, územního řízení a stavebního řízení. Eliminace zdrojové základny všech aktérů, kteří bezpečí obyvatelstva ČR ohrožují. Jednoznačné vymezení role soukromých poskytovatelů bezpečnosti a zajištění dostupnosti bezpečnosti všem obyvatelům ČR bez ohledu na jejich schopnost za ni zaplatit soukromým aktérům.

Zajištění souladu opatření k ochraně obyvatelstva ČR se základními lidskými právy a principy fungování demokratického státu. Dodržování a propagování *etických* a sociálních aspektů bezpečnosti v souladu s etickým bezpečnostním kodexem, který je mravní normou zahrnující respekt jak k ochraně celé společnosti, tak k ochraně individuality každého člověka. Práce s médii patří mezi strategické postupy řešení mimořádných událostí a krizových situací.

Dílčí cíl W1.5.1: Vypracování modelu efektivního zapojení soukromých subjektů v zajištění bezpečnosti občanů ČR Na základě analýzy stávajícího stavu zlepšit participaci soukromých subjektů a/nebo poskytovatelů bezpečnosti se zaměřením na oblasti ekonomického, legislativního, institucionálního, organizačního, technického, a personálního zajištění v případech mimořádných situací a krizových stavů.	**Časový horizont:** 2020 **Výzkumné směry** Ekonomie Právo Bezpečnostní vědy
Dílčí cíl W1.5.2: Zvýšení odolnosti (resilience) společnosti na úrovni jedince, komunity a státu Cílem výzkumu je navrhnout ekonomicky a legislativně zabezpečené postupy ke zvýšení připravenosti jedinců a komunity k sebeochraně v případech mimořádných situací a krizových stavů se zaměřením na vnímání a hodnocení rizik. Zefektivnění komplexního systému vzdělávání na všech úrovních.	**Časový horizont:** **Výzkumné směry 2020** Ekonomie Právo Sociální vědy Bezpečnostní vědy
Dílčí cíl W1.5.3: Etické a sociální aspekty bezpečnosti Cílem je tvorba nástrojů pro zajištění souladu opatření k ochraně obyvatelstva se základními lidskými právy a principy fungování demokratického státu a občanské společnosti se zaměřením na dodržování a propagování etických a sociálních aspektů bezpečnosti. Navrhnout systémová pravidla pro práci s médii v případech mimořádných událostí a krizových situací.	**Časový horizont:** 2020 **Výzkumné směry** Ekonomie Právo Sociální vědy Bezpečnostní vědy
Dílčí cíl W1.5.4: Optimalizace alokace a využití veřejných zdrojů Cílem je zvýšení efektivity alokace a využití veřejných zdrojů při mimořádných událostech a krizových situací na základě nových poznatků v oblasti cost-benefit analýz.	**Časový horizont:** 2020 **Výzkumné směry** Ekonomie Právo Sociální vědy Bezpečnostní vědy
Dílčí cíl W1.5.5 Environmentální bezpečnost Cílem je vytvoření a rozvoj nástrojů k zajištění environmentální bezpečnosti v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku environmentálních krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů.	**Časový horizont:** 2020 **Výzkumné směry** Enviromentalistika Ekonomie Právo Sociální vědy Bezpečnostní vědy

Oblast 2: Bezpečnost kritických infrastruktur a zdrojů

Oblast zahrnuje zejména prevenci, ochranu a obnovu v odvětvích energetiky, vodního hospodářství, potravinářství a zemědělství, zdravotní péče, dopravy a logistiky, komunikačních a informačních systémů, bankovního a finančního sektoru, nouzových služeb a veřejné správy. Do této oblasti patří i problematika ochrany a zachování přírodních zdrojů.

Podoblast 2.1: Ochrana, odolnost a obnova kritických infrastruktur

Oblasti KI zahrnuje energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotní péči, dopravu a logistiku, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby a veřejnou správu.

Podoblast 2.1 těsně navazuje na popis a stěžejní cíl podoblasti 1.1 Ochrana obyvatelstva.

Zajištění funkčnosti kritických infrastruktur (KI) spočívá na všech třech faktorech, kterými jsou ochrana KI, odolnost KI a obnova funkce KI po přerušení její funkce. Jedná se v podstatě o tři bezpečnostní bariéry, které brání rozvinutí nežádoucích stavů do krizových situací z pohledu těch, kterým KI slouží. Smyslem ochrany KI je snížení zranitelnosti působením vnějších vlivů, jedná se o ochranu proti účinkům přírodních pohrom a úmyslných antropogenních činů. Smyslem zvyšování odolnosti je zajištění robustnosti systémů KI proti výskytu přírodních, technologických a antropogenních (včetně chyb obsluhy) hrozeb. Děje se tak zahrnutím robustnosti (včetně zajištění alternativních a náhradních mechanismů) do procesů navrhování, výstavby, obsluhy a údržby systémů KI s cílem zabezpečení alespoň určité nouzové úrovně služeb. Zajištění obnovy KI spočívá v úsilí o minimalizace doby obnovy tak, aby se s ohledem na dopady přerušení funkce KI zabránilo rozvoji krizové situace (její vážnost narůstá obvykle exponenciálně v závislosti na době přerušení funkce KI). Současně je třeba, aby při obnově bylo využito rozboru vzniklé situace k navržení preventivních opatření pro zmírnění dopadů při případném opakování pohromy (např. v elektroenergetice jsou tato opatření známá pod pojmem plány obrany a ochrany, v obchodní praxi je vhodným vodítkem norma ČSN BS 25999-1 Management kontinuity činností organizace).

Stěžejní cíl 2.1:

Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací.

Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury.

Aplikace managementu kontinuity činností organizací kritické infrastruktury.

Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Dílčí cíl W2.1.1: Zajištění nezbytné funkčnosti (Minimum Service Level)	**Časový horizont:** 2020
Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI. Vytváření kapacit pro zajištění nouzové úrovně služeb.	**Výzkumné směry**
	Bezpečnostní vědy
	Technické a zemědělské vědy
	Energetické zdroje

		Udržitelný rozvoj
	Dílčí cíl W2.1.2: Rozvoj alternativních a nouzových krizových procesů Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Aplikace managementu kontinuity činností v organizacích kritické infrastruktury.	**Časový horizont: 2020** **Výzkumné směry** Bezpečnostní vědy Technické a zemědělské vědy Energetické zdroje Udržitelný rozvoj
	Dílčí cíl W2.1.3: Zvyšování odolnosti KI Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů.	**Časový horizont:** 2020 **Výzkumné směry** Bezpečnostní vědy Udržitelný rozvoj Informační technologie
	Dílčí cíl W2.1.4: Zajištění a rozvoj interoperability KI Tvorba nástrojů pro zajištění a rozvoj interoperability KI (dopravní, energetické a dalších) s nadnárodními evropskými KI. Vazba na nadnárodní evropské síťové systémy (TEN-T, TEN-E). Modelování a výpočty sítí.	**Časový horizont:** 2020 **Výzkumné směry** Bezpečnostní vědy Technické vědy Udržitelný rozvoj
	Dílčí cíl W2.1.5: Účinná detekce a identifikace hrozeb Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).	**Časový horizont: 2020** **Výzkumné směry** Bezpečnostní vědy Mezinárodní vztahy Informační technologie Udržitelný rozvoj
	Dílčí cíl W2.1.6: Rozvoj ICT, telematiky a kybernetické ochrany KI Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.	**Časový horizont: 2020** **Výzkumné směry** Bezpečnostní vědy Informační technologie

Podoblast 2.2: Komunikace a vazby mezi kritickými infrastrukturami

V současné době dokáží kritické infrastruktury dobře reagovat na problémy, které se projeví uvnitř vlastního systému, a v rámci plánů na řešení krizových situací mají připravené postupy na obnovu provozu po odstranění poruchy. Analýzy rizik a spolehlivosti, které jsou prováděny interně pro tyto infrastruktury, však většinou nezahrnují dynamické vzájemné závislosti s ostatními kritickými infrastrukturami. V případě velkých pohrom bývá narušeno více systémů infrastruktury současně.

Narušení funkce určitého systému může být způsobeno i problémem zavlečeným z jiného systému prostřednictvím vzájemných vazeb, a to s různým časovým průběhem, závislým například na schopnosti akumulace a stavu zásob. Koordinace zásahů a obnovy provozu se v důsledku vzájemných závislostí stává zásadním nástrojem pro efektivní obnovu funkce území. V důsledku nekoordinovaných činností může dojít ke vzájemnému nežádoucímu působení a následkem toho mohou být zesíleny dopady pohromy na život dané komunity. Nekoordinovaný manipulační zásah v jedné infrastruktuře může znemožnit nebo zpomalit obnovu funkce jiné infrastruktury. Stejně tak se může projevit i absence potřebného zásahu.

Na základě dřívějších prací v oblasti výzkumu dopadů a účinků pohrom na život komunity se ukazuje, že zranitelnost souvisí jak s velkostí sídla, tak především s dobou, po kterou je přerušena funkce kritických infrastruktur zajišťujících základní fyziologické lidské potřeby (přiměřená teplota, voda, potraviny) a potřeba zajištění pocitu bezpečí u občanů (včetně funkce záchranných složek). Obvykle jsou systémy navrženy tak, že pokud dojde k obnově funkce těchto kritických infrastruktur do 24 hodin, je situace z hlediska ochrany obyvatelstva a udržení veřejného pořádku zvládnutelná místními složkami integrovaného záchranného systému. Naopak je prokázáno (například nedávnými zkušenostmi z New Orleans, Haiti, Chile), že pokud není obnoveno uspokojení základních fyziologických potřeb a potřeba bezpečí v několika dnech, pak se s jistotou od 5. dne po katastrofě život komunity rozkládá, místní záchranné složky a policie nejsou schopny zajistit obnovu pořádku a situace se mění v humanitární katastrofu vyžadující pomoc z jiných regionů, případně i mezinárodní.

Stát vyžaduje od subjektů kritické infrastruktury zpracování Plánů krizové připravenosti, které by měly postihnout nejen zachování kontinuity, ale i usnadnit koordinaci aktivit v kritických situacích a zajistit potřebné zdroje. Zpracování těchto plánů je v současné době spíše formální, bez hlubšího provázání jednotlivých systémů kritické infrastruktury a bez náležité informační podpory. Vzájemné závislosti mezi systémy kritické infrastruktury nejsou do hloubky prozkoumány a nejsou k dispozici modely jejich chování, vizualizace celkového stavu a rozpoznávání kritických stavů.

Stěžejní cíl 2.2:

Vytvoření informační podpory, která umožní modelování vzájemných závislostí alespoň nejdůležitějších systémů kritické infrastruktury. Dosažení dřívější detekce hrozeb plynoucích ze vzájemných vazeb a závislostí, přesnější a rychlejší predikce vývoje chování a nasazení regulačních mechanismů, které minimalizují pravděpodobnost eskalace krizové situace a případného celkového kolapsu komunity s dlouhodobými následky.

	Dílčí cíl W2.2.1: Vzájemné závislostí systémů KI Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií.	**Časový horizont:** 2020 **Výzkumné směry** Bezpečnostní vědy Udržitelný rozvoj Informační technologie
	Dílčí cíl W2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Systémy predikce a včasného varování.	**Časový horizont: 2020** **Výzkumné směry** Bezpečnostní vědy Udržitelný rozvoj Informační technologie

Oblast 3: Krizové řízení a bezpečnostní politika

Oblast zahrnuje formování a implementaci bezpečnostní politiky, rozvoj bezpečnostního systému, včasné varování, komunikaci s veřejností, připravenost, prevenci, reakci a obnovu, civilně vojenskou spolupráci a civilní nouzové plánování, moderní metody zásahového tréninku a také problematiku vnějšího krizového řízení NATO a EU.

Podoblast 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního sytému ČR

Bezpečnostní politika státu vychází z principu nedělitelnosti bezpečnosti. Základním východiskem pro zajištění bezpečnosti ČR je členství v NATO a EU a plnění spojeneckých závazků, které ze členství v obou organizacích vyplývají. Prioritně se jedná o aktivní účast v systému kolektivní obrany NATO, zapojení do Společné bezpečnostní a obranné politiky EU a rozvoj schopností EU pro zvládání krizí. Úroveň a efektivnost bezpečnostní politiky ČR zásadně určuje úroveň bezpečnostního systému, který musí reagovat na dynamický vývoj, změny a trendy v oblasti bezpečnosti, společenského a ekonomického vývoje. ČR má plně integrovaný, funkčně i zdrojově provázaný bezpečnostní systém, který je schopen efektivně působit v krizových situacích a stavech a při mimořádných událostech. Klíčovou roli má v tomto směru Integrovaný záchranný systém ČR a jeho složky. Klíčové cíle a úkoly bezpečnostní politiky jsou zároveň integrální součástí dlouhodobých rozvojových strategií rozvoje na úrovni státu a krajů.

Stěžejní cíl 3.1:

Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídících a hodnotících dokumentů v oblasti bezpečnosti, které je nutno pravidelně aktualizovat v závislosti na vývoji bezpečnostního prostředí a v závislosti na strategických prioritách bezpečnostní politiky NATO a EU. Prioritou bezpečnostní politiky je zajištění připravenosti a akceschopnosti celého bezpečnostního systému ČR (zejména IZS a AČR) za krizových situací a krizových stavů a to jak samostatně, tak i v součinnosti se spojenci v NATO a EU, a dále při řešení mimořádných událostí, přírodních a antropogenních krizových situací. Bezpečnostní systém tak musí být připraven reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.

	Dílčí cíl W3.1.1: Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda) a Parlament ČR jak přistupovat k tomuto procesu.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Veřejná politika Bezpečnostní vědy Strategická studia Sociologie
	Dílčí cíl W3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Prognostika Strategická studia Bezpečnostní vědy Ochrana obyvatelstva

Podoblast 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významným předpokladem pro úspěšné zajištění krizového řízení a pro tvorbu a realizaci informované bezpečnostní politiky je vyhledávání a identifikace bezpečnostních hrozeb a z nich vyplývajících rizik. V daném případě se vychází z monitorování klíčových trendů ekonomického, společenského, sociálního, technologického a bezpečnostního vývoje, událostí, ohnisek napětí, krizí a konfliktů. Informace vyplývající z tohoto procesu se částečně promítají do tvorby a realizace bezpečnostní politiky, resp. tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Stěžejní cíl 3.2:

Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik; v dlouhodobém horizontu (2020-2030), který funguje následujícím způsobem: Pravidelně se zpracovávají prognostické studie a scénáře vývoje bezpečnostní situace, které jsou předmětem expertního posuzování. Následně se vytváří soubor opatření pro eliminaci hrozeb podpořený i tvorbou (variantních) scénářů bezpečnostního vývoje. Závěry se promítají do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

	Dílčí cíl W3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Prognostika Ochrana obyvatelstva Bezpečnostní vědy Strategická studia
	Dílčí cíl W3.2.2: Nová a neznámá rizika technologického a společenského rozvoje Vypracovat systém zajišťující monitoring nově se objevujících nebo dosud neznámých technologických rizik, zvláště v oblasti intenzivně se rozvíjejících oblastí (nanotechnologie, biotechnologie, energetika, informační technologie) včetně možností společenského zneužití. V případě identifikované hrozby vývoj preventivních opatření. Zajištění rovnováhy mezi principem předběžné opatrnosti a rozvojem.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Technologie Medicína Environmentalistika Informační technologie
	Dílčí cíl W3.2.3: Interakce energetické, vodní a potravinové bezpečnosti Analýza vazeb energetické, vodní a potravinové bezpečnosti. Stanovení, dosažení a udržování vhodné (optimální) míry soběstačnosti i se zahrnutím přínosů, ale i rizik vyplývajících z členství v EU, resp. z účasti na tvorbě a realizaci příslušných politik EU. Analýza možností řešení protichůdných nároků na jednotlivé systémy v zahraničí a v ČR. Návrh rozhodovacích modelů pro řešení protichůdných nároků a požadavků.	**Časový horizont:** 2020 **Výzkumné směry** Bezpečnostní vědy Mezioborové transdisciplinární interakce s možnými negativní účinky Nové přístupy k soběstačnosti ČR ve zdrojích energie, vody a v potravinách

Podoblast 3.3: Systémy analýzy, prevence, odezvy a obnovy

Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Stěžejní cíl 3.3:

Cílem této průřezové podoblasti je zajistit pro operativní i v krizové činnosti interoperabilní technologie získávání, třídění, ukládání, analýzy, zpřístupnění a zabezpečení informací a znalostí z otevřených a zpravodajských zdrojů (civilních, obranných), dále navazující informační a aplikované technologie pro efektivní využití informací a znalostí pro účinnou prevenci hrozeb a případnou odezvu včetně nouzového řízení a následné obnovy. Zpřístupnění a zabezpečení informací (pro využití v prevenci a ochraně, jakož i v krizovém řízení) musí být zajištěno podle závažnosti a klasifikace pro všechny relevantní složky v odpovídající struktuře.

	Dílčí cíl W3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů.	**Časový horizont:** 2020 **Výzkumné směry** Informační technologie Technická kybernetika Manažerské systémy řízení
	Dílčí cíl W3.3.2: Analýza bezpečnostních informací Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. Mezinárodní spolupráce, interoperabilita na technologické i organizační úrovni.	**Časový horizont:** 2020 **Výzkumné směry** Informační technologie Technická kybernetika Jazykověda Matematika Umělá inteligence
	Dílčí cíl W3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Informační technologie Ekonomika Manažerské systémy řízení
	Dílčí cíl W3.3.4: Zdokonalení systémů pro podporu obnovy	**Časový horizont:** 2030 (průběžně)

	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy.	**Výzkumné směry** Manažerské systémy řízení Informační technologie Ekonomika

Podoblast 3.4: Legislativní a právní problémy

Vysoká úroveň bezpečnosti České republiky a jejích občanů bude do značné míry záviset na schopnosti státu dosahovat takové poznatkové, technické, technologické a manažerské úrovně, která umožní získávat, osvojovat si a rozvíjet k tomu potřebné specifické schopnosti. Vzhledem k existujícím a nově predikovaným hrozbám je nutné rozvíjet a zkvalitňovat připravenost a akceschopnost státu v oblasti krizového řízení, ochrany obyvatelstva, obrany, ochrany kritické infrastruktury, integrovaného záchranného systému ČR, boje proti terorismu, boje proti kriminalitě atd. komplexně, to je nejen z hlediska věcné působnosti, ale současně též odpovídajícím způsobem rozvíjet a zkvalitňovat legislativní rámec upravující práva a povinnosti při přípravě na řešení a při vlastním řešení mimořádných událostí a krizových situací.

Stěžejní cíl 3.4:

Rozvíjet legislativní postupy a navrhovaná legislativní opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů a složek, aby dynamicky reagoval na nově vznikající potřeby bezpečnostního systému ČR s preferencí krizových situací spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) nebo vnitřní bezpečnosti státu a dále pak při přírodních (živelních) a antropogenních (tj. lidmi nebo lidskou činností způsobených) pohromách.

	Dílčí cíl W3.4.1: Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací Rozvíjet legislativní postupy a opatření tak, aby legislativní rámec vytvářet komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Ekonomika Právní věda
	Dílčí cíl W3.4.2: Legislativní postupy a opatření při stavu ohrožení státu a válečném stavu Rozvíjet legislativní postupy a opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti	**Časový horizont: 2030 (**průběžně) **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Vojenské vědy Ekonomika

	s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) včetně vazeb na krizové situace související s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách.	Právní věda
	Dílčí cíl W3.4.3: Implementace legislativních aktů EU do oblasti bezpečnosti ČR Analyzovat relevantní legislativní akty EU a strategické dokumenty NATO navrhovat způsoby jejich implementace do legislativy České republiky tak, aby legislativní rámec vytvářející komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu, při přírodních a antropogenních pohromách a v souvislosti s vnějším ohrožením státu (stav ohrožení státu a válečný stav), byl plně v souladu s legislativou EU.	**Časový horizont: 2030 (průběžně)** **Výzkumné směry** Bezpečnostní vědy Ochrana obyvatelstva Vojenské vědy Ekonomika Právní věda
	Dílčí cíl W3.4.4: Harmonizace a standardizace Tvorba legislativního a právního rámce pro obchodní společnosti KI umožňující v tržním prostředí rozvíjet a zlepšovat systémy ochrany, odolnosti a obnovy KI. Harmonizace a standardizace (kultura resilience). Podklady pro vědecky zdůvodněné koncepce (strategie, politiky). Koncepce musí zohlednit nejen technické, ekologické a ekonomické aspekty, ale i aspekty právní, legislativní a mezinárodně politické.	**Časový horizont:** 2020 **Výzkumné směry** Bezpečnostní vědy Společenské vědy - právo Udržitelný rozvoj

Oblast 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR

Cílem rezortu Ministerstva obrany je disponovat do roku 2020 souborem sil, který bude garantovat naplnění politicko-vojenských ambicí ČR a účinné prosazení bezpečnostních zájmů státu v souladu s právním řádem ČR. Tyto schopnosti budou náležitým způsobem rozvíjeny v následující dekádě. Do rozvoje schopností budou důsledně promítnuty koncepční záměry výstavby ozbrojených sil z Bílé knihy o obraně a závazky, které ČR převzala v rámci obranného plánování NATO a EU
Rozvoj schopností ozbrojených sil včetně systému jejich komplexního zabezpečení závisí na zvládnuté úrovni strategie a vojenského umění velitelským sborem, stavu a vycvičenosti vojenského personálu, vybaveností jednotek moderní výzbrojí a kvalitním logistickým zabezpečením. Bojové síly, síly bojové podpory a bojového zabezpečení budou schopny plnit úkoly v operacích od nízké po vysokou intenzitu (tj. v plném spektru operací), budou připraveny působit v prostoru nasazení koordinovaně s civilními aktéry vládního i nevládního charakteru v duchu komplexního přístupu (Comprehensive Approach), budou interoperabilní se spojenci, nasaditelné na strategické vzdálenosti, dlouhodobě udržitelné, se zajištěným velením a bezpečným přenosem dat v prostředí NEC, s vysokým stupněm univerzálnosti použití, modularity a odolnosti proti působení protivníka.
Systém obrany státu a krizového řízení v rezortu MO bude postupně optimalizován a bude udržovat svou schopnost pohotově a adekvátně reagovat na ohrožení v kontextu kolektivního zajišťování obrany státu.

Podoblast 4.1: Rozvoj schopností ozbrojených sil

Rozvoj schopností ozbrojených sil včetně systému jejich komplexního zabezpečení závisí na zvládnuté úrovni strategie a vojenského umění velitelským sborem, stavu a vycvičenosti vojenského personálu, vybaveností jednotek moderní výzbrojí a kvalitním logistickým zabezpečením. Bojové síly a síly bojové podpory a bojového zabezpečení budou schopny plnit úkoly v operacích od nízké po vysokou intenzitu (tj. v plném spektru operací), budou připraveny působit v prostoru nasazení koordinovaně s civilními aktéry vládního i nevládního charakteru v duchu komplexního přístupu (Comprehensive Approach), budou interoperabilní se spojenci, nasaditelné na strategické vzdálenosti, dlouhodobě udržitelné, se zajištěným velením a bezpečným přenosem dat v prostředí NEC, s vysokým stupněm univerzálnosti použití, modularity a odolnosti proti působení protivníka. Schopnosti vyjadřují způsobilost ozbrojených sil efektivně působit v krizových situacích a válečných konfliktech. Jedná se o:

- schopnosti, které Česká republika deklaruje jako svou specializaci v rámci NATO a EU, případně sdílené schopnosti s některým z členských států NATO nebo EU;
- schopnosti identifikované Organizací NATO pro výzkum a vývoj technologií (NATO RTO) a Evropskou obrannou agenturou (EDA) jako klíčové pro rozvoj ozbrojených sil;
- oblasti, kde již Česká republika disponuje potenciálem pro výzkum a vývoj (např. kybernetika, robotizace, nanotechnologie, aktivní a pasivní ochrana jednotlivce a techniky, zbraně hromadného ničení);
- schopnost personálně řídit a rozvíjet ozbrojené síly též s podporou sociologického sledování a průzkumu a schopnost strategické analýzy trendů mezinárodní bezpečnosti, povahy rizik a ohrožení, charakteru konfliktů a role ozbrojených sil i civilních aktérů v nich.

Mezi významné faktory rozvoje kapacit ozbrojených sil patří kromě spojeneckého charakteru jejich působení (dnes se odrážejícího v účasti na expedičních misích NATO, systému NATINADS nebo misích SBOP) zejména bezpečnostní trendy jako tzv. nové války, asymetrická povaha globálních hrozeb, proměnlivé modality nasazení (tzv. *comprehensive approach*) nebo dopady ekonomické stagnace na vojenské výdaje, úvahy o vzniku společného evropského zbrojního trhu nebo kapacit tzv. *pooling and sharing* na regionální úrovni či rozvíjení evropské technologické báze mj. prostřednictvím EDA.

Stěžejní cíl 4.1:
Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.

	Dílčí cíl W4.1.1: Ochrana vzdušného prostoru České republiky Cílem je hledání a realizace vhodného konceptu ochrany vzdušného prostoru ČR, a to ať už vlastními silami a prostředky a nebo zapojením se do mezinárodních projektů, s důrazem na úsporu létajícího personálu a nové disruptivní technologie.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Bezpečnostní vědy Strategická studia Technické vědy Bezpečnostní technologie Právo Matematika
	Dílčí cíl W4.1.2: Přeprava, mobilita a udržitelnost ozbrojených sil Cílem je rozvíjet a zdokonalovat metody, postupy, technická a jiná řešení, která povedou k vyšší mobilitě a dlouhodobé udržitelnosti sil v operacích.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Bezpečnostní vědy Technické vědy Vojenské vědy
	Dílčí cíl W4.1.3: Podpora velení a řízení Cílem je rozvoj systémů velení a řízení v operacích umožňujících získání společného přehledu o vývoji situace s aliančními partnery a informační převahy nad protivníkem. Rozvoj technických a jiných řešení, která povedou ke zvýšení efektivnosti řízení rezortu MO, zejména k personálním úsporám. Modernizace a rozvoj zpravodajského, geografického a hydrometeorologického zabezpečení s důrazem na implementaci systému Intelligence, Surveillance, and Reconnaissance.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Vojenské vědy Manažerské systémy řízení Ekonomie Informační technologie Informatika Umělá inteligence
	Dílčí cíl W4.1.4: Ochrana sil a prostředků v operacích Cílem je vývoj a zdokonalování prostředků aktivní i pasivní ochrany živé síly a vojenské techniky v celém spektru operací, jako např. výstroj, výzbroj, prostředky balistické ochrany, individuální i kolektivní prostředky ochrany proti ZHN a maskování.	**Časový horizont:** 2020 **Výzkumné směry** Technické vědy Ochrana obyvatelstva Technologie Chemie Technická kybernetika Biologie Medicína
	Dílčí cíl W4.1.5: Rozvoj KIS a kybernetická obrana Cílem je rozvoj komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací.	**Časový horizont:** 2020 **Výzkumné směry** Informační technologie Informatika Bezpečnostní vědy

		Bezpečnostní technologie
		Umělá inteligence

Podoblast 4.2: Obranná politika v kontextu vývoje NATO a EU

ČR utváří a realizuje vlastní obrannou politiku v souladu s životními a strategickými bezpečnostními zájmy a zároveň v úzké provázanosti na obrannou a bezpečnostní politiku spojeneckých uskupení, jichž je členem – tedy především NATO a EU. Obranná politika zahrnuje identifikaci hrozeb a rizik, tvorbu scénářů použití ozbrojených sil, formování a rozvoj rozhodovacího procesu a konkrétní situace spojené s potřebou použití ozbrojených sil.

Stěžejní cíl 4.2:

ČR je schopna kvalitně a srozumitelně formulovat zájmy, cíle a principy své obranné politiky jak navenek ke svým spojencům v NATO a EU, tak směrem k domácí veřejnosti – občanům ČR. Zároveň je schopna plnit své spojenecké závazky a věrohodně posilovat svou obranyschopnost.

	Dílčí cíl W4.2.1: Racionální obranná politika Cílem je rozvoj metod, metodik a modelů používaných k identifikaci hrozeb a rizik, k vytváření scénářů použití ozbrojených sil a formulaci požadavků na efektivní systém obrany.	**Časový horizont:** 2030 (průběžně)
		Výzkumné směry
		Mezinárodní vztahy
		Strategická studia
		Sociální vědy
		Ekonomie
		Bezpečnostní vědy
		Prognostika
	Dílčí cíl W4.2.2: Strategické rozhodování Cílem je podpora strategického rozhodování orgánů odpovědných za obranu ČR na základě využití metod NATO Concept Development and Experimentation, umožňující formulovat a realizovat koncepce výstavby schopností ozbrojených sil a jejich použití v operacích. Rozvíjet a přizpůsobovat metody experimentování, jako je např. Wargaming, simulace, modelování apod., národním podmínkám.	**Časový horizont:** 2030 (průběžně)
		Výzkumné směry
		Veřejná politika
		Manažerské systémy řízení
		Matematika
		Vojenské vědy
		Informační technologie
		Strategická studia

Podoblast 4.3: Specifika vojenského personálu

Velikost a vyspělost ozbrojených sil je podmíněna dostatkem kvalitního vojenského personálu. Problémem může být jeho zajištění v období demografického stárnutí populace. To vyžaduje zlepšení přístupu k náboru vojenského personálu, jeho výběru, přípravě, výchově, výcviku, řízení kariér a k zabezpečení jeho plnohodnotné integrace zpět do civilního života.

Stěžejní cíl 4.3:

Cílem je analyzování trhu práce ve vztahu k specifickým potřebám ozbrojených sil a rozvoj metod, metodik a modelů umožňujících predikci této potřeby a vývoje demografických zdrojů a trhu práce. Zefektivnění přípravy, výcviku a vzdělávání personálu adekvátní trendům vedení operací. Řízení

personálního procesu a rozvoj metod kvalitního psychologického servisu pro vojáky a jejich blízké nutného z hlediska jejich specifické psychické zátěže v operacích. Udržení kvality života vojáků po ukončení jejich aktivní vojenské služby.		
	Dílčí cíl W4.3.1: Nábor a výběr personálu Cílem je rozvíjet metody a modely umožňující co nejúčinnější nábor vojenského personálu. Rozvoj metod výběru personálu pro jeho běžné zařazení v ozbrojených silách i pro nasazení do vojenských operací.	**Časový horizont:** 2020 **Výzkumné směry** Ekonomie Sociální vědy Sociologie
	Dílčí cíl W4.3.2: Vzdělávání, výcvik a výchova vojáků Cílem je rozvoj metod, konceptů a politik zaměřených na vzdělávání, výcvik a výchovu vojáků, které budou předcházet extremizmu a jiným sociálně nežádoucím jevům, a to zejména u hodnostních sborů mužstva, poddůstojníků a praporčíků. Zvýšení efektivnosti přípravy vojáků pro nasazení v kulturně-odlišném prostředí.	**Časový horizont:** 2020 **Výzkumné směry** Vojenské vědy Sociální vědy Sociologie Jazykověda
	Dílčí cíl W4.3.3: Řízený personální proces Cílem je analyzování a zdokonalování systému odměňování tak, aby vojenské povolání bylo i přes jeho specifika co nejatraktivnější na trhu práce. Rozvoj metod a konceptů používaných pro horizontální a vertikální řízení vojenských kariér. Rozvoj modelů a metod simulací pro řízení kariér a určení optimální personální struktury adekvátní scénářům použití ozbrojených sil.	**Časový horizont:** 2020 **Výzkumné směry** Sociologie Manažerské systémy řízení Sociální vědy Ekonomie
	Dílčí cíl W4.3.4: Zvovuzačlenění do civilního života Cílem je rozvoj metod, konceptů a politik zaměřených na zajištění co nejhladšího začlenění vojáků zpět do běžného civilního života, zahrnujících např. jejich dlouhodobou rekvalifikaci na civilní profese, odloučení od vojenského kolektivu, vyrovnání se s následky stresů nebo zranění z vojenské operace apod.	**Časový horizont:** 2020 **Výzkumné směry** Sociální vědy Sociologie Medicína

Podoblast 4.4: Strategické zpravodajství Úkolem strategického zpravodajství je zajistit výkon zpravodajské činnosti v souladu s prioritami České republiky v oblasti zahraniční politiky a vnitřní bezpečnosti.		
Stěžejní cíl 4.4: Cílem této průřezové oblasti je zajistit pro operativní i krizové situace interoperabilní technologie k získávání, třídění, ukládání, analýze a sdílení informací a znalostí z otevřených i zpravodajských zdrojů.		
	Dílčí cíl W4.4.1: Včasná identifikace hrozeb a vyhodnocování rizik pro životní a strategické zájmy ČR. Cílem je zlepšit systém a metody získávání a třídění všech druhů informací, identifikace zdrojů, ukládaní a sdílení dat. Zefektivnit kvalitativní i kvantitativní analýzu hrozeb a vyhodnocování bezpečnostních rizik pro ČR. Mezinárodní spolupráce a interoperabilita na technologické i organizační úrovni.	**Časový horizont:** 2030 (průběžně) **Výzkumné směry** Mezinárodní vztahy Bezpečnostní technologie Strategická studia Právní věda

		Informační technologie
	Dílčí cíl W4.4.2: Distribuce informací rozhodovacím místům obranného systému Cílem je zdokonalení spolupráce bezpečnostních složek a státní správy při distribuci informací a informačních zdrojů.	**Časový horizont:** 2020 **Výzkumné směry** Informatika Manažerské systémy řízení Veřejná politika

Příloha 2: Prioritizace cílů

2.1 Kritéria významnosti a dosažitelnosti

1. Významnost

Pro expertní panel byla sestavena individuální sada 14 kritérií významnosti, která specificky odpovídala zaměření panelu. Tato kritéria byla pro větší přehlednost rozdělena do tematických skupin:

Kritérium	Popis
Významnost cíle pro fungování státu a infrastruktur	
Průmysl, zemědělství, energetika	Význam pro zajištění chodu průmyslu, zemědělství a energetiky v případě mimořádných událostí.
Doprava a logistika	Význam pro zajištění chodu dopravy a zásobování v případě mimořádných událostí.
Informační a komunikační systémy	Význam pro zajištění chodu kritických informačních a komunikačních systémů v případě mimořádných událostí.
Veřejná správa a finance	Význam pro zajištění kritických funkcí veřejné správy a finančního sektoru v případě mimořádných událostí.
Zdravotní péče	Význam pro zajištění nezbytné zdravotní péče v případě mimořádných událostí.
Významnost cíle pro bezpečnost občanů a občanské společnosti	
Ochrana života a zdraví osob	Význam pro zajištění ochrany života a zdraví občanů v případě mimořádných událostí.
Ochrana majetku	Význam pro zajištění ochrany majetku občanů a veřejného majetku v případě mimořádných událostí.
Zachování etických norem	Význam pro zajištění toho, aby se občané i v případě mimořádných událostí chovali v souladu s obecně uznávanými etickými normami a dobrými mravy.
Bezpečnost životního prostředí	Význam pro zajištění maximální možné ochrany životního prostředí a přírodních zdrojů v případě mimořádných událostí a při likvidaci jejich následků.
Zachování kulturních hodnot	Význam pro zajištění maximální možné ochrany kulturních hodnot v případě mimořádných událostí a pří likvidaci jejich následků.
Zachování společenských hodnot (životní úroveň, vzdělanost, úroveň služeb veřejné správy apod.)	Význam pro zajištění maximální možné ochrany dosažených společenských hodnot (životní úroveň, vzdělanost, úroveň služeb veřejné správy apod.) v případě mimořádných událostí.
Významnost cíle pro obranu státu	
Ochrana území	Význam pro zachování územní celistvosti státu v případě

	vnějšího napadení.
Hájení zájmů v zahraničí	Význam pro zajišťování zájmů ČR v zahraničí např. formou politických jednání nebo zahraničních vojenských misí.
Zajištění vnitřní bezpečnosti	Význam pro zajištění vnitřní bezpečnosti státu a jeho obyvatel v případě mimořádných událostí (živelní katastrofy, sociální nepokoje, teroristické útoky apod.).

2. Dosažitelnost

Dosažitelnost dílčího cíle byla hodnocena prostřednictvím široce definovaných směrů VaV, které byly pro každý dílčí cíl identifikovány jako nejvíce relevantní.

Stejně jako kritérium významnosti se i dosažitelnost skládá z několika dílčích kritérií:

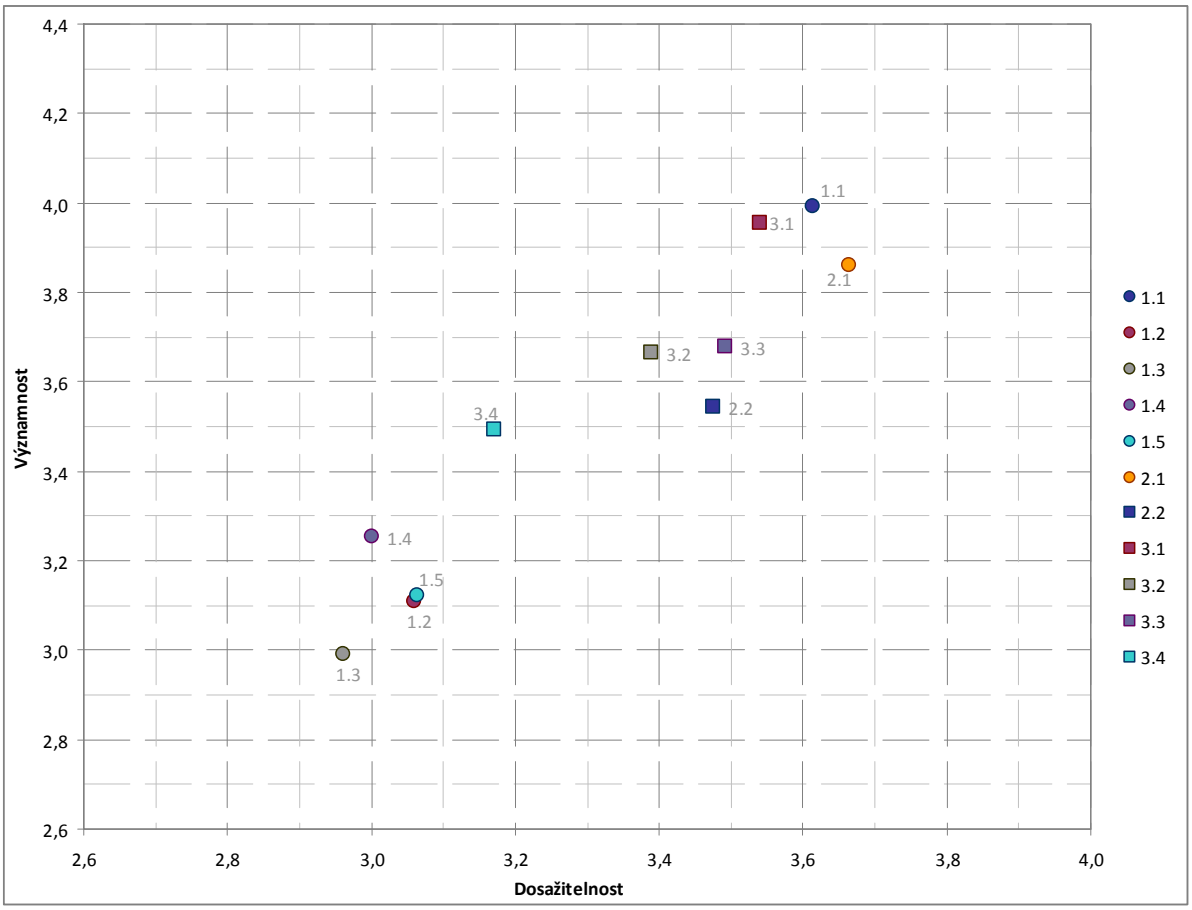
- ***Současná úroveň a kvalita výzkumu v ČR*** (zdali v ČR existuje v domácí základně VaV potenciál dosáhnout realizaci cíle; schopnost vyvinout vlastní řešení v rámci domácích kapacit (efektivně ve srovnání se světem);
- ***Úroveň výzkumné infrastruktury*** (zdali v daném směru VaV existuje v ČR dostatečně velká a kvalitní infrastruktura VaV);
- ***Podpora ve státní politice a regulaci*** (jaká je současná výše veřejné podpory na daný směr VaV a do jaké míry je veřejnou správou podporován systémově);
- ***Kvalita lidských zdrojů a úroveň vzdělávání*** (zdali ČR v daném výzkumném směru v současnosti disponuje dostatečným počtem kvalitních lidských zdrojů a kvalitním vzděláváním, nutných k naplnění cíle);
- ***Očekávaná finanční náročnost dosažení cíle*** (jak vysoké náklady jsou očekávány s rozvojem daného výzkumného směru (kritérium se hodnotilo opačně, tedy podle stupnice 5-1)
- ***Absorpční kapacita aplikační sféry*** (jaká v ČR existuje schopnost uplatnit výsledky VaV v potřebných oblastech. Zdali v ČR existuje potřebná absorpční kapacita v podobě již existujících firem, které by byly schopny výsledky VaV využít)

2.2 Výsledky hlasovací procedury expertního panelu

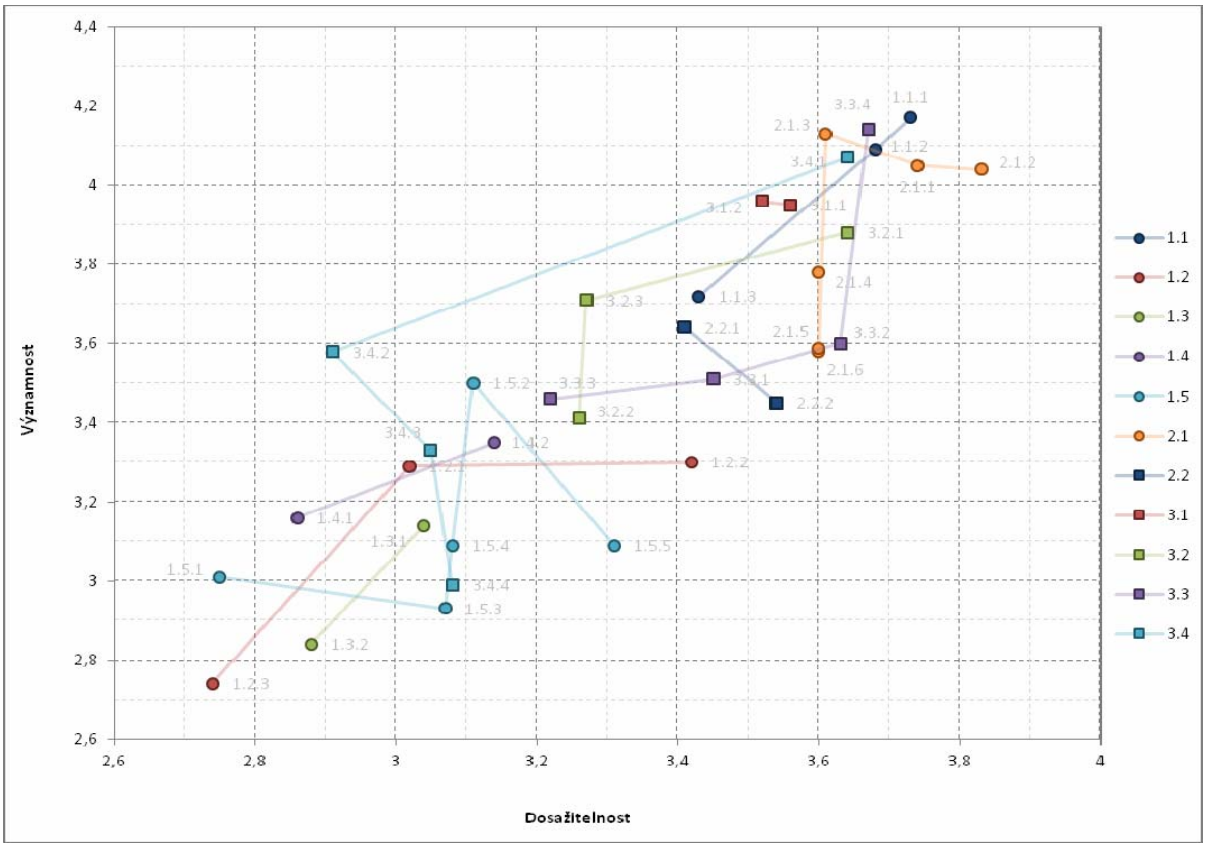
Na obrázcích v této kapitole je graficky znázorněno umístění stěžejních a dílčích cílů na základě výsledků hodnocení významnost a dosažitelnosti v tzv. pozičních grafech. V grafech umístění dílčích cílů jsou jednotlivé dílčí cíle ze stejné podoblasti (tj. příslušející ke stejnému stěžejnímu cíli) pro přehlednost „propojeny“ barevnou spojovací čarou. Číselné kódy stěžejních a dílčích cílů v použitých grafech odpovídá jejich označení v Příloze 1: Strukturace prioritní oblasti po první fázi.

Výsledky hodnocení významnosti a dosažitelnosti všech dílčích cílů jsou přehledně shrnuty v tabulce pod grafy. V další tabulce jsou potom uvedeny detailní výsledky hodnocení, včetně výsledků pro jednotlivá dílčí kritéria. Hodnota pro dané dílčí kritérium vždy odpovídá průměru hodnocení členů panelu, kteří o tomto dílčím cíli hlasovali (se započtením váhy podle jejich expertní úrovně).

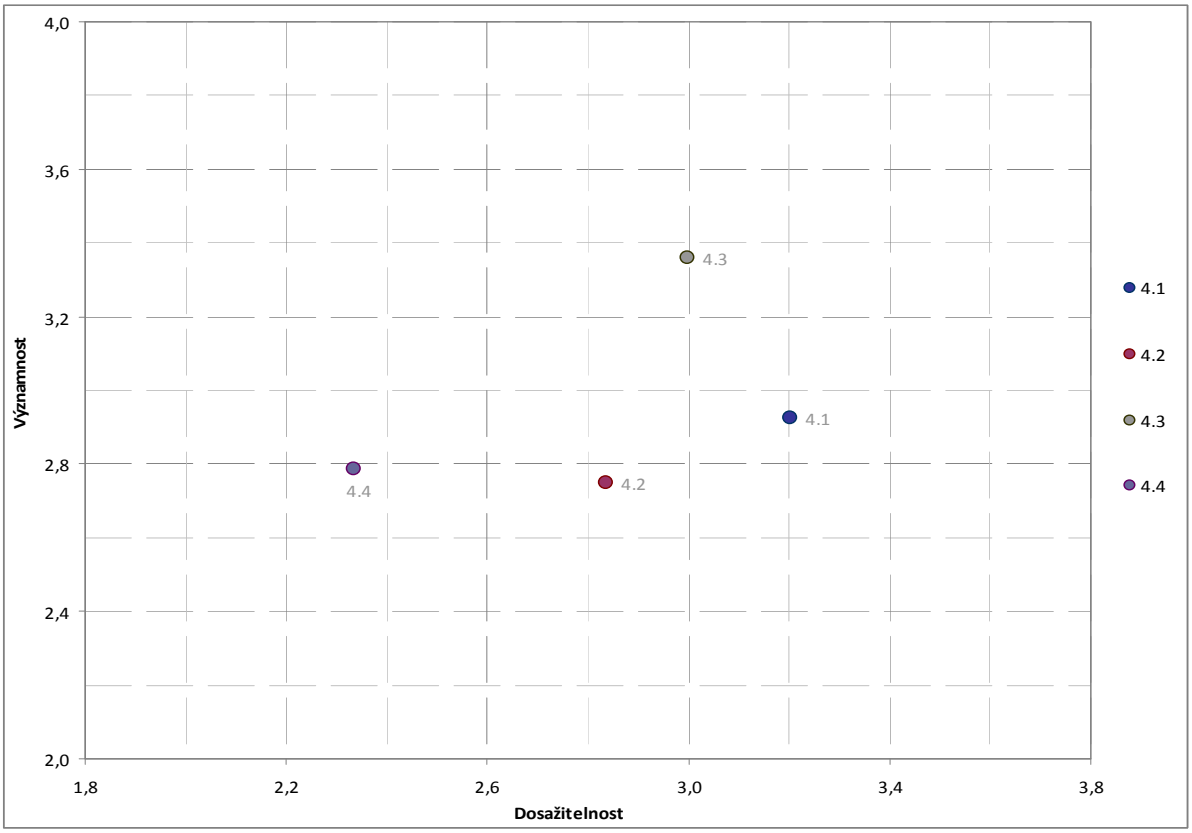
Poziční graf stěžejních cílů podle významnosti a dosažitelnosti (bez oblasti 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR)



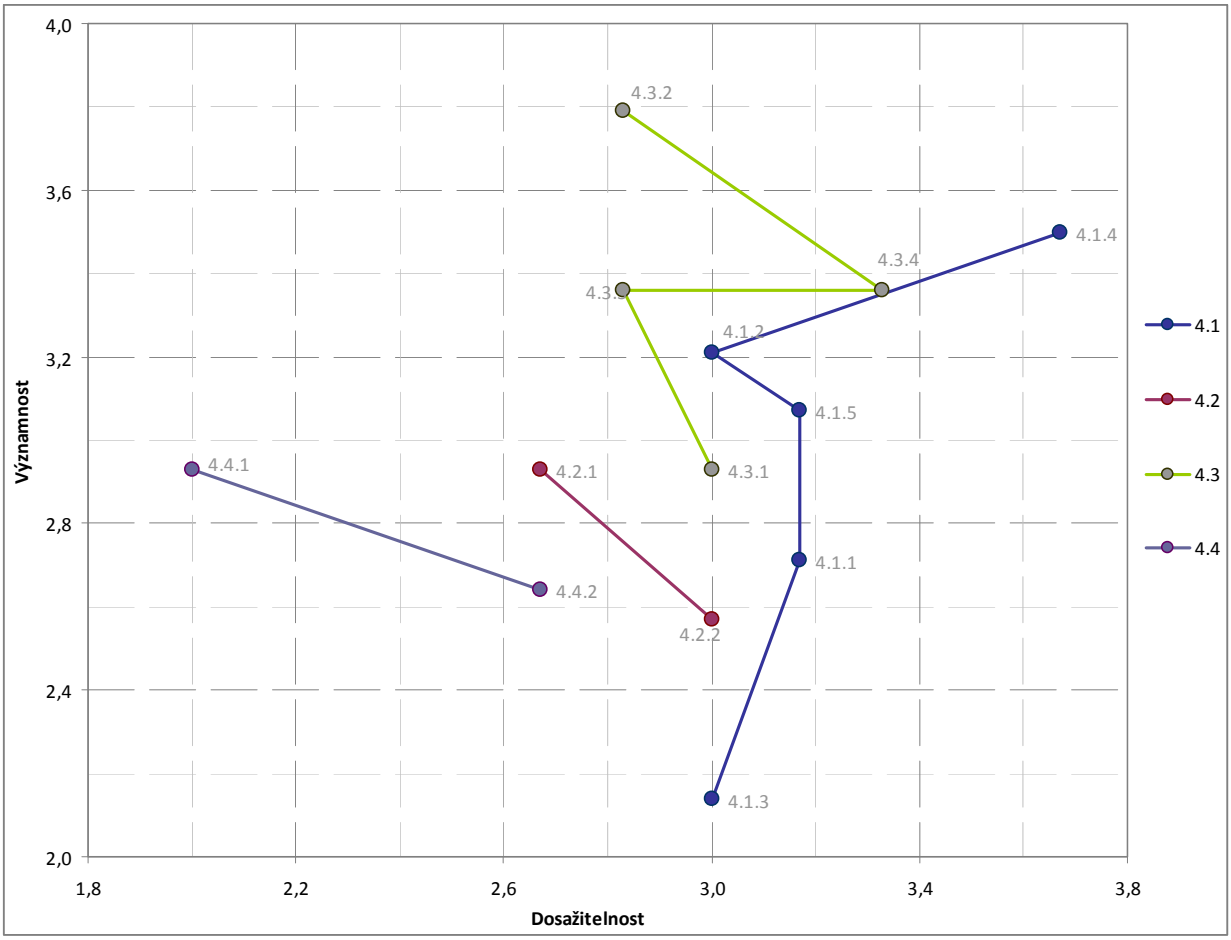
Poziční graf dílčích cílů podle významnosti a dosažitelnosti (bez oblasti 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR)



Poziční graf stěžejních cílů podle významnosti a dosažitelnosti - oblast 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR



Poziční graf dílčích cílů podle významnosti a dosažitelnosti - oblast 4: Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR



Souhrnné výsledky hlasování o významnosti a dosažitelnosti dílčích cílů

Číslo dílčího cíle	Název dílčího cíle	Významnost cíle	Dosažitelnost cíle
W 1.1.1	Podpora opatření a úkolů ochrany obyvatelstva	4,17	3,73
W 1.1.2	Zdokonalování služeb a prostředků ochrany obyvatelstva	4,09	3,68
W 1.1.3	Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	3,72	3,43
W 1.2.1	Vytváření účinných metod analýzy druhů a rozšířenosti kriminality a implementace efektivních nástrojů jejího potírání	3,29	3,02
W 1.2.2	Minimalizace kybernetické kriminality a zneužívání informací	3,30	3,42
W 1.2.3	Vyhodnocování dopadů právních úprav na kriminalitu a její trendy	2,74	2,74
W 1.3.1	Analýza hrozeb a rizik extremismu	3,14	3,04
W 1.3.2	Vytváření efektivních nástrojů prevence extremismu a účinných protiopatření vůči němu	2,84	2,88
W 1.4.1	Optimalizace alokace zdrojů a zvýšení efektivity opatření v boji proti terorismu	3,16	2,86
W 1.4.2	Využití nových technologií v boji proti terorismu	3,35	3,14
W 1.5.1	Vypracování modelu efektivního zapojení soukromých subjektů v zajištění bezpečnosti občanů ČR	3,01	2,75
W 1.5.2	Zvýšení odolnosti (resilience) společnosti na úrovni jedince, komunity a státu	3,50	3,11
W 1.5.3	Etické a sociální aspekty bezpečnosti	2,93	3,07
W 1.5.4	Optimalizace alokace a využití veřejných zdrojů	3,09	3,08
W 1.5.5	Environmentální bezpečnost	3,09	3,31
W 2.1.1	Zajištění nezbytné funkčnosti (Minimum Service Level)	4,05	3,74
W 2.1.2	Rozvoj alternativních a nouzových krizových procesů	4,04	3,83
W 2.1.3	Zvyšování odolnosti KI	4,13	3,61
W 2.1.4	Zajištění a rozvoj interoperability KI	3,78	3,60
W 2.1.5	Účinná detekce a identifikace hrozeb	3,58	3,60
W 2.1.6	Rozvoj ICT, telematiky a kybernetické ochrany KI	3,59	3,60
W 2.2.1	Vzájemné závislostí systémů KI	3,64	3,41
W 2.2.2	Informační podpora pro detekci možných nepříznivých ovlivňování	3,45	3,54
W 3.1.1	Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti	3,95	3,56
W 3.1.2	Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	3,96	3,52
W 3.2.1	Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	3,88	3,64
W 3.2.2	Nová a neznámá rizika technologického a společenského rozvoje	3,41	3,26
W 3.2.3	Interakce energetické, vodní a potravinové bezpečnosti	3,71	3,27
W 3.3.1	Zlepšení systémů získávání a třídění bezpečnostních informací	3,51	3,45
W 3.3.2	Analýza bezpečnostních informací	3,60	3,63
W 3.3.3	Zdokonalování účinnosti bezpečnostního systému a krizového řízení	3,46	3,22
W 3.3.4	Zdokonalení systémů pro podporu obnovy	4,14	3,67
W 3.4.1	Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací	4,07	3,64

W 3.4.2	Legislativní postupy a opatření při stavu ohrožení státu a válečném stavu	3,58	2,91
W 3.4.3	Implementace legislativních aktů EU do oblasti bezpečnosti ČR	3,33	3,05
W 3.4.4	Harmonizace a standardizace	2,99	3,08
W 4.1.1	Ochrana vzdušného prostoru České republiky	2,71	3,17
W 4.1.2	Přeprava, mobilita a udržitelnost sil	3,21	3,00
W 4.1.3	Podpora velení a řízení	2,14	3,00
W 4.1.4	Ochrana ozbrojených sil a prostředků v operacích	3,50	3,67
W 4.1.5	Rozvoj KIS a kybernetická obrana	3,07	3,17
W 4.2.1	Racionální obranná politika	2,93	2,67
W 4.2.2	Strategické rozhodování	2,57	3,00
W 4.3.1	Nábor a výběr personálu	2,93	3,00
W 4.3.2	Vzdělávání, výcvik a výchova vojáků	3,79	2,83
W 4.3.3	Řízený personální proces	3,36	2,83
W 4.3.4	Znovuzačlenění do civilního života	3,36	3,33
W 4.4.1	Včasná identifikace hrozeb a vyhodnocování rizik pro životní a strategické zájmy ČR	2,93	2,00
W 4.4.2	Distribuce informací rozhodovacím místům obranného systému	2,64	2,67

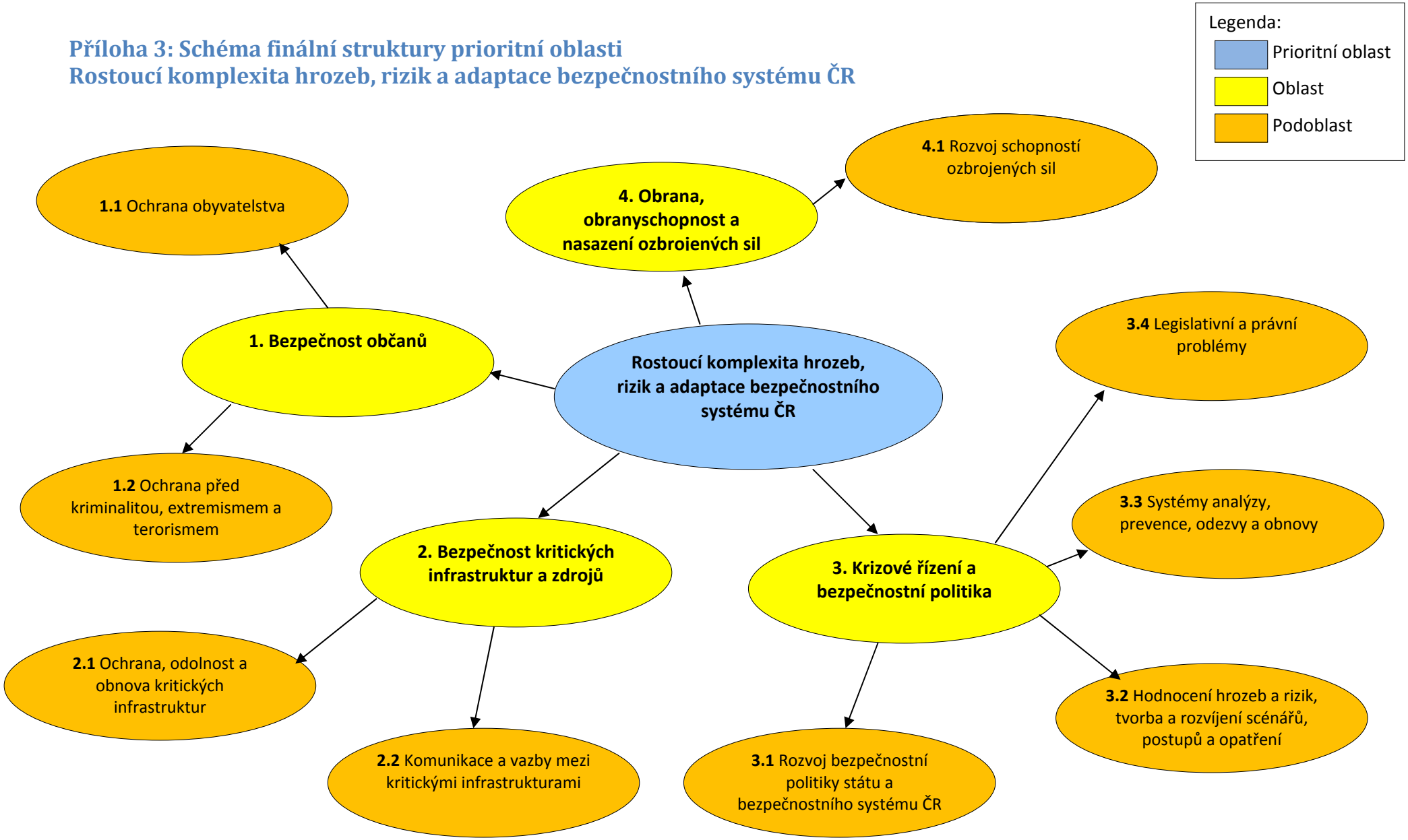
Podrobné výsledky hlasování o významnosti a dosažitelnosti dílčích cílů

Číslo dílčího cíle	Významnost cíle	Dosažitelnost cíle	Průmysl, zemědělství, energetika	Doprava a logistika	Informační a komunikační systémy	Veřejná správa a finance	Zdravotní péče	Ochrana života a zdraví osob	Ochrana majetku	Zachování etických norem	Bezpečnost životního prostředí	Zachování kulturních hodnot	Zachování společenských hodnot	Obrana území	hájení zájmů v zahraničí	Zajištění vnitřní bezpečnosti	Současná úroveň a kvalita výzkumu v ČR	Úroveň výzkumné infrastruktury	Podpora ve státní politice a regulaci	Kvalita lidských zdrojů a úroveň vzdělávání	Očekávaná finanční náročnost dosažení cíle	Absorpční kapacita aplikační sféry	Celkový počet hodnotitelů
W 1.1.1	4,17	3,73	4,50	4,27	4,48	4,00	4,10	4,90	4,08	3,87	4,15	3,67	4,00	4,21	3,38	4,75	4,17	4,12	3,94	3,90	2,15	4,10	17
W 1.1.2	4,09	3,68	4,08	4,12	4,30	4,24	4,04	4,76	4,12	3,74	3,82	3,54	4,28	4,20	3,38	4,62	4,04	3,96	3,70	4,08	2,00	4,28	16
W 1.1.3	3,72	3,43	3,61	3,41	3,98	4,18	3,50	4,75	4,09	3,11	3,77	2,93	3,91	3,80	2,68	4,36	3,57	3,86	3,25	3,75	2,41	3,75	16
W 1.2.1	3,29	3,02	3,00	2,82	3,27	3,77	2,18	4,23	4,45	4,05	2,27	3,05	3,95	2,50	2,32	4,23	3,27	2,91	2,86	3,05	2,64	3,41	12
W 1.2.2	3,30	3,42	3,62	2,90	4,93	4,02	2,31	3,40	4,31	3,40	1,98	1,98	3,38	2,57	2,71	4,64	3,48	3,33	2,93	3,86	2,74	4,19	14
W 1.2.3	2,74	2,74	2,67	2,56	3,17	3,28	2,06	3,39	3,72	2,39	2,06	1,78	3,33	2,44	2,06	3,50	2,50	2,67	2,33	2,78	3,44	2,72	10
W 1.3.1	3,14	3,04	2,26	2,16	2,89	3,37	2,16	4,37	3,79	3,89	2,21	3,79	4,05	2,53	2,26	4,21	3,11	3,11	2,74	3,00	3,37	2,89	13
W 1.3.2	2,84	2,88	1,94	2,06	3,24	3,35	1,71	3,59	3,29	3,53	1,59	3,18	3,59	2,35	2,12	4,29	2,76	2,88	2,59	2,88	3,59	2,59	13
W 1.4.1	3,16	2,86	2,92	3,04	3,46	3,29	1,96	4,79	3,58	3,04	2,42	2,58	3,29	2,50	3,04	4,38	2,71	2,96	2,42	3,00	3,21	2,88	13
W 1.4.2	3,35	3,14	3,18	3,29	4,09	3,41	2,18	4,79	3,82	3,21	2,68	2,65	3,74	2,68	2,91	4,26	3,15	3,03	2,94	3,32	2,94	3,44	14
W 1.5.1	3,01	2,75	3,55	3,67	3,58	2,82	2,24	3,97	3,85	2,64	2,79	2,36	3,21	2,09	1,79	3,64	2,18	2,55	2,64	2,67	3,48	3,00	13
W 1.5.2	3,50	3,11	3,40	3,45	3,36	3,45	3,10	4,55	4,12	3,17	3,10	3,05	4,14	3,57	2,05	4,50	2,69	3,19	2,40	3,26	3,31	3,79	15
W 1.5.3	2,93	3,07	2,41	2,27	2,73	3,34	2,32	3,15	2,63	3,93	2,49	3,20	4,34	2,51	2,24	3,46	2,66	2,88	2,44	3,46	3,93	3,02	15
W 1.5.4	3,09	3,08	3,32	3,32	3,56	4,03	3,09	3,65	3,50	2,21	2,76	2,29	3,50	2,71	1,68	3,59	2,79	3,29	2,79	3,29	3,44	2,88	14
W 1.5.5	3,09	3,31	3,73	3,08	2,75	3,15	2,60	3,88	2,83	2,28	4,90	2,43	3,60	2,10	2,33	3,65	3,45	3,58	3,20	3,60	2,50	3,55	15
W 2.1.1	4,05	3,74	4,78	4,76	4,65	4,49	3,93	4,75	4,00	3,15	3,56	3,05	3,93	4,07	3,09	4,45	4,27	3,87	3,67	3,98	2,45	4,18	16
W 2.1.2	4,04	3,83	4,70	4,57	4,65	4,30	3,59	4,80	4,30	3,24	3,87	2,87	3,96	4,09	2,98	4,57	4,35	4,04	3,67	4,31	2,35	4,24	15
W 2.1.3	4,13	3,61	4,82	4,78	4,76	4,13	3,89	4,67	4,33	3,11	3,87	3,22	4,33	4,22	2,82	4,82	3,91	3,85	3,35	3,95	2,40	4,20	16
W 2.1.4	3,78	3,60	4,49	4,60	4,51	3,70	3,32	4,23	3,91	2,45	3,40	2,62	4,04	3,70	3,28	4,60	3,72	3,68	2,98	3,96	3,04	4,23	14
W 2.1.5	3,58	3,60	4,57	4,49	4,45	3,62	3,02	4,25	3,89	2,26	3,28	2,32	3,58	3,49	2,36	4,60	3,70	3,68	3,17	3,94	3,21	3,89	17
W 2.1.6	3,59	3,60	4,06	3,89	4,94	3,94	3,17	3,96	4,00	2,35	2,98	2,15	3,67	3,74	2,85	4,56	3,83	3,70	3,20	4,09	2,78	3,98	15
W 2.2.1	3,64	3,41	4,63	4,54	4,48	4,02	3,23	4,21	3,92	2,42	2,94	2,35	3,67	3,54	2,31	4,67	3,40	3,25	3,02	3,83	3,04	3,90	15
W 2.2.2	3,45	3,54	4,09	4,17	4,37	4,09	3,04	3,87	3,57	2,20	3,11	2,11	3,61	3,41	2,35	4,35	3,41	3,65	3,11	3,91	3,26	3,87	14
W 3.1.1	3,95	3,56	4,12	3,90	3,93	4,29	3,73	4,24	4,27	3,22	3,56	3,37	4,32	4,29	3,71	4,41	3,56	3,61	3,46	3,68	3,10	3,93	15
W 3.1.2	3,96	3,52	4,22	4,09	4,07	4,17	3,39	4,41	4,22	3,22	3,54	3,02	4,30	4,48	3,89	4,48	3,43	3,72	3,26	3,83	2,98	3,91	15

Číslo dílčího cíle	Významnost cíle	Dosažitelnost cíle	Průmysl, zemědělství, energetika	Doprava a logistika	Informační a komunikační systémy	Veřejná správa a finance	Zdravotní péče	Ochrana života a zdraví osob	Ochrana majetku	Zachování etických norem	Bezpečnost životního prostředí	Zachování kulturních hodnot	Zachování společenských hodnot	Obrana území	hájení zájmů v zahraničí	Zajištění vnitřní bezpečnosti	Současná úroveň a kvalita výzkumu v ČR	Úroveň výzkumné infrastruktury	Podpora ve státní politice a regulaci	Kvalita lidských zdrojů a úroveň vzdělávání	Očekávaná finanční náročnost dosažení cíle	Absorpční kapacita aplikační sféry	Celkový počet hodnotitelů
W 3.2.1	3,88	3,64	4,04	3,91	4,20	4,02	3,40	4,24	4,04	3,16	3,64	3,00	4,07	4,27	3,82	4,56	3,76	3,89	3,38	3,76	3,16	3,91	15
W 3.2.2	3,41	3,26	4,04	3,61	3,98	3,18	3,12	4,29	3,61	2,94	3,29	2,20	3,51	3,25	2,61	4,18	3,35	3,45	2,96	3,53	2,76	3,51	16
W 3.2.3	3,71	3,27	4,54	4,08	3,92	4,26	3,64	4,33	3,54	2,77	3,46	2,92	3,97	3,41	2,51	4,51	3,08	3,18	2,59	3,69	3,41	3,67	13
W 3.3.1	3,51	3,45	4,05	3,88	4,44	3,85	2,73	4,00	3,63	2,44	3,07	2,39	3,61	3,61	3,12	4,34	3,54	3,51	2,93	3,85	3,05	3,83	15
W 3.3.2	3,60	3,63	3,77	3,49	4,71	4,03	2,94	4,17	4,00	2,69	3,17	2,83	3,74	3,40	3,11	4,34	3,97	3,71	2,94	4,14	3,14	3,89	15
W 3.3.3	3,46	3,22	3,59	3,52	4,48	3,84	2,77	4,00	3,59	2,34	3,05	2,36	3,89	3,77	2,66	4,52	3,11	3,20	2,84	3,57	3,09	3,48	16
W 3.3.4	4,14	3,67	4,72	4,44	4,37	4,33	4,23	4,53	4,33	3,28	3,65	3,67	4,47	4,05	3,23	4,63	3,81	3,77	3,56	4,05	2,81	4,00	15
W 3.4.1	4,07	3,64	4,39	4,37	4,17	4,44	3,95	4,54	4,24	3,51	3,61	3,49	4,15	4,07	3,44	4,56	3,66	3,80	3,66	3,93	2,95	3,85	13
W 3.4.2	3,58	2,91	3,62	3,54	3,50	4,08	3,31	3,92	3,65	2,73	3,04	2,62	3,81	4,38	3,58	4,35	2,77	2,88	2,58	2,88	3,38	2,96	11
W 3.4.3	3,33	3,05	3,62	3,42	3,42	3,73	2,81	3,65	3,19	2,81	3,15	2,42	3,15	3,50	3,73	3,96	2,85	2,81	2,69	3,31	3,35	3,31	11
W 3.4.4	2,99	3,08	3,61	3,36	3,42	3,24	2,64	3,70	3,24	2,21	2,79	2,36	3,76	2,33	2,09	3,12	2,70	2,97	2,42	3,09	3,94	3,36	13
W 4.1.1	2,71	3,17	5,00	2,00	5,00	3,00	1,00	5,00	4,00	1,00	1,00	1,00	3,00	5,00	1,00	1,00	3,00	4,00	3,00	4,00	1,00	4,00	1*
W 4.1.2	3,21	3,00	2,00	5,00	3,00	5,00	4,00	3,00	2,00	1,00	1,00	2,00	4,00	5,00	5,00	3,00	3,00	4,00	3,00	3,00	2,00	3,00	1*
W 4.1.3	2,14	3,00	2,00	2,00	3,00	4,00	1,00	1,00	2,00	1,00	1,00	1,00	3,00	3,00	3,00	3,00	3,00	2,00	3,00	3,00	3,00	4,00	1*
W 4.1.4	3,50	3,67	2,00	3,00	5,00	4,00	5,00	5,00	5,00	1,00	1,00	1,00	4,00	5,00	5,00	3,00	5,00	4,00	3,00	5,00	1,00	4,00	1*
W 4.1.5	3,07	3,17	3,00	3,00	5,00	4,00	1,00	3,00	5,00	1,00	1,00	2,00	4,00	3,00	3,00	5,00	3,00	3,00	3,00	4,00	3,00	3,00	1*
W 4.2.1	2,93	2,67	2,00	3,00	1,00	5,00	1,00	3,00	3,00	3,00	1,00	2,00	5,00	5,00	5,00	2,00	1,00	3,00	1,00	3,00	4,00	4,00	1*
W 4.2.2	2,57	3,00	2,00	1,00	3,00	5,00	1,00	2,00	4,00	2,00	1,00	1,00	4,00	5,00	3,00	2,00	2,00	3,00	1,00	3,00	4,00	5,00	1*
W 4.3.1	2,93	3,00	2,00	2,00	2,00	5,00	3,00	4,00	1,00	3,00	1,00	1,00	5,00	5,00	3,00	4,00	3,00	2,00	3,00	3,00	3,00	4,00	1*
W 4.3.2	3,79	2,83	3,00	2,00	1,00	5,00	2,00	5,00	4,00	5,00	3,00	3,00	5,00	5,00	5,00	5,00	2,00	3,00	2,00	3,00	3,00	4,00	1*
W 4.3.3	3,36	2,83	3,00	3,00	3,00	5,00	3,00	3,00	2,00	3,00	1,00	2,00	4,00	5,00	5,00	5,00	3,00	2,00	2,00	2,00	3,00	5,00	1*
W 4.3.4	3,36	3,33	2,00	3,00	2,00	5,00	5,00	5,00	2,00	3,00	1,00	2,00	5,00	5,00	2,00	5,00	3,00	3,00	3,00	4,00	2,00	5,00	1*
W 4.4.1	2,93	2,00	3,00	2,00	3,00	5,00	1,00	3,00	2,00	1,00	1,00	1,00	4,00	5,00	5,00	5,00	1,00	2,00	1,00	2,00	3,00	3,00	1*
W 4.4.2	2,64	2,67	3,00	3,00	3,00	5,00	1,00	1,00	1,00	1,00	1,00	1,00	3,00	5,00	4,00	5,00	2,00	2,00	1,00	3,00	4,00	4,00	1*

* Hodnocení dílčích cílů v oblasti 4: „Obrana, obranyschopnost a zahraniční nasazení ozbrojených sil ČR“ bylo provedeno pověřeným expertním týmem MO.

Příloha 3: Schéma finální struktury prioritní oblasti
Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR



Příloha 4: Identifikační listy prioritních dílčích cílů

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	1 Bezpečnost občanů
Podoblast:	1.1 Ochrana obyvatelstva
Stěžejní cíl:	Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

Název dílčího cíle:	**1.1.1 Podpora opatření a úkolů ochrany obyvatelstva**	**2030** (průběžně)
Popis dílčího cíle:	Rozvíjet a zdokonalovat organizační, technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na plánování a zavádění neodkladných, následných a dlouhodobých opatření na ochranu obyvatel – ukrytí, evakuaci/přesídlení, zdravotní péči postiženým, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití prostředků/zbraní hromadného ničení (CBRNE), na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování a komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých a na likvidaci následků dané mimořádné či krizové situace. *Základním cílem „ochrany obyvatelstva“ je rozvíjet a zdokonalovat procesy a mechanismy směřující k bezpečné společnosti, tzn. společnosti odolné vůči negativním vlivům potenciálních mimořádných a krizových situací ohrožujících zdraví a životy lidí a jejich životní podmínky. Tyto procesy a mechanizmy jsou pochopitelně determinovány předpokládaným rozvojem společnosti na jedné straně a mírou zranitelnosti s tímto rozvojem související na straně druhé. Prvořadou podmínkou rozvoje systému ochrany obyvatelstva jsou proto analýzy a vyhodnocení:* • *současného stavu bezpečnostního prostředí, v němž se ČR nachází,* • *místa a úlohy „ochrany obyvatelstva“ jakožto nedílné součástí bezpečnostní politiky ČR,* • *předpokládaného vývoje nové techniky, postupů a technologií v dané oblasti,* • *úlohy „Ženevského protokolu“ v podmínkách současnosti a předpokládaného budoucího vývoje společnosti.* *Potenciální hrozba přírodních katastrof a technologických havárií ohrožujících ČR současně vyžaduje trvalé vytváření prostoru a příležitostí směřujících k:* • *eliminaci zjednodušeného chápání bezpečnosti moderní společnosti,* • *začlenění prvků řízení bezpečnosti do rozhodovacích procesů všech orgánů veřejné správy,* • *vytvoření participativního modelu hodnocení zranitelnosti v rámci systému řízení bezpečnosti,* • *rozvoji integrovaného přístupu k problematice bezpečnosti státu (eliminace resortismu),* • *tvorbě modelů dynamického řízení aktiv infrastruktury,* • *spolupráci privátního sektoru a veřejné správy (Public Private Partnership),* • *rozvoji mezinárodní spolupráce,* • *eliminaci rizika omezené kompatibility se systémy bezpečnosti v rámci zemí EU,* • *zapojení obyvatel a veřejných společností do systému havarijní připravenosti – sebeochrana, participace na záchranných a likvidačních prací.*	

Vazba na ostatní dílčí cíle:		
Dílčí cil 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2**: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.4.1: Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací	Analyzovat a vytvářet legislativní postupy a opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.4:** Legislativní a právní problémy

Významnost dílčího cíle	
Významnost pro fungování státu a infrastruktur:	**4,3**
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**4,1**
Významnost cíle pro obranu státu:	**4,1**

	trvale udržitelného rozvoje společnosti. Od počátku 21. století je Česká republika konfrontována s novými bezpečnostními hrozbami, jejichž dosah bude dále zesilovat. Jsou to především environmentální hrozby (pitná voda, potravinové zdroje apod.), živelní pohromy a technologické havárie, potenciální rozšiřování prostředků/zbraní hromadného ničení (zejména v rozvojových zemích) apod. Analýza bezpečnostních hrozeb a z nich vyplývajících rizik ukazuje na nutnost komplexního zajištění a řízení bezpečnosti státu a ochrany jeho obyvatel. Předpokládané výsledky spoluvytváří makroekonomický rámec hospodářského rozvoje České republiky s akcentací priorit zvýšení bezpečnosti státu a občanů, zachování základních funkcí státu a fungování jeho infrastruktur jako rozhodujících podmínek efektivní ochrany obyvatelstva při mimořádných a krizových situacích mírového charakteru ale i v případě vyhlášení stavu ohrožení nebo válečného stavu; připravenosti sil a prostředků; vyváženého hospodářského růstu; respektování globalizačních trendů; stability veřejných financí; institucionální a legislativní připravenosti.

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Bezpečnostní vědy 2) Ochrana obyvatelstva 3) Ekonomie 4) Bezpečnostní technologie 5) Civilní nouzové plánování 6) Havarijní připravenost
Současná úroveň a kvalita výzkumu v ČR:	**4,2**	Současná úroveň a kvalita výzkumu v ČR odpovídá podmínkám VaVaI. Česká republika disponuje vysoce kvalifikovanými týmy s praktickými zkušenostmi konfrontovanými účastí v zahraničních misích i v rámci obsáhlé mezinárodní spolupráce v rámci NATO, EU a dalších struktur. Úroveň výzkumné infrastruktury je historicky na velmi vysoké úrovni. Existují dobré předpoklady pro dosažení stanovených cílů. Na Akademii věd ČR, v resortech Ministerstva vnitra ČR, SÚJB, civilních vysokých školách, ve výzkumných institucích a zainteresovaných podnikatelských subjektech existuje silné výzkumné zázemí se zaměřením na bezpečnostní aspekty prakticky všech stránek života společnosti. Obzvláště dobrých výsledků bylo dosaženo v oblastech detekce CBRNE a ochrany proti nim, aktivních a pasivních senzorů, analýz a identifikací nebezpečných látek, v oblasti vývoje modelů (podložených polními experimenty) hodnotících dopady uvolněných škodlivých látek na obyvatele a životní prostředí. Některé řešitelské týmy a řešitelské organizace mají předpoklady obstát v mezinárodním konkurenčním prostředí. Stát tuto oblast systematicky, komplexně a dlouhodobě koordinuje na odpovídající úrovni. Bezpečnost občanů, respektive ochrana obyvatelstva je chápána jako žádoucí stav, kdy jsou na nejnižší míru snížena rizika plynoucí z hrozeb vůči obyvatelstvu, svrchovanosti a územní celistvosti, demokratickému zřízení a principům právního státu, vnitřnímu pořádku, majetku, životnímu prostředí, plnění mezinárodních bezpečnostních závazků a dalším definovaným zájmům. Finanční prostředky vynaložené na výzkum, experimentální vývoj a inovace pro tento dílčí cíl je nezbytné považovat za základní vklad pro zvyšování úrovně připravenosti ČR na zvládání krizových situací vojenského i nevojenského charakteru. Z tohoto pohledu lze považovat dosažené bodové hodnocení za zcela podhodnocené. V reálném odhadu je adekvátní úroveň 1,2 bodového hodnocení. Absorpční kapacita aplikační sféry je vysoká a odpovídá potřebám. Uživatelem výsledků výzkumu a vývoje v oblasti ochrany obyvatelstva budou instituce státní správy a samosprávy, prvky Bezpečnostního systému ČR, bezpečnostní složky a podnikatelské subjekty působící v oblasti zajišťování bezpečnosti, odborná avšak i laická veřejnost, kdy je třeba akcentovat prvek sebeochrany obyvatel a jejich participaci na likvidaci následků mimořádných situací. Vzhledem ke stanoveným cílům existují v podmínkách ČR dobré podmínky pro realizaci nových poznatků v dané oblasti, zejména existuje relativně dobře připravená uživatelská sféra schopná tyto poznatky absorbovat a využít a zahrnující jak státní, tak soukromý sektor od producentů, přes služby až po koncové uživatele.
Úroveň výzkumné infrastruktury:	**4,1**	
Podpora ve státní politice a regulaci:	**3,9**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**	
Očekávaná finanční náročnost dosažení cíle:	**2,2**	
Absorpční kapacita aplikační sféry:	**4,1**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	1 Bezpečnost občanů
Podoblast:	1.1 Ochrana obyvatelstva
Stěžejní cíl:	Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

Název dílčího cíle:	**1.1.2 Zdokonalování služeb a prostředků ochrany obyvatelstva**	**2030** (průběžně)
Popis dílčího cíle:	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR a dalších složek/institucí participujících na detekci a monitorování, vzniku, vývoje a hodnocení těchto situací a likvidaci jejich následků. *Úroveň bezpečnosti ČR a jejich občanů závisí tedy na schopnosti státu dosahovat takové poznatkové technické a technologické úrovně, která umožní získat, osvojovat si a rozvíjet k tomu potřebné specifické schopnosti.* *Důležitá je podpora vzájemné spolupráce a komunikace mezi relevantními složkami a institucemi, které se podílejí na zajištění bezpečnosti a obrany státu a jeho obyvatel. Prohlubování připravenosti bezpečnostních a záchranných sborů ve společnosti prostřednictvím výzkumu a vývoje akcentuje důležitost všech procesů spojených s bezpečností a obranou státu a jeho obyvatel.* *Většina ze současných největších hrozeb nevyžaduje tradiční vojenskou reakci, nýbrž realizaci integrovaných systémů krizového řízení a na ně navazujících systémů záchranných, zdravotnických, sociálních, psychologických a dalších služeb, které musí pokrýt komplexně jak oblast prevence a detekce/monitoringu, tak odezvy na danou událost/situaci .* *Integrovaný záchranný systém je efektivní systém vazeb, pravidel spolupráce a koordinace záchranných a bezpečnostních složek, orgánů státní správy a samosprávy, fyzických a právnických osob při společném provádění záchranných a likvidačních prací a přípravě na mimořádné události. Stanovené věcné priority vyžadují orientaci projektů výzkumu a vývoje zejména na návrhy souboru organizačních, řídících, plánovacích, kontrolních, technických, technologických a dalších opatření:* • *pro optimalizaci, rozvoj schopností Integrovaného záchranného systému ČR a koordinovaného postupu jeho složek při přípravě reakce na mimořádné události a při vlastním provádění záchranných a likvidačních prací,* • *zaměřených na rozvoj akceschopnosti složek systému k provádění záchranných a likvidačních prací při mimořádných událostech a krizových situací, na vybavenost systému moderní technikou a technologiemi, na zvyšování úrovně strategických, taktických a operačních postupů, školení a výcvik,* • *směřujících k optimalizaci plošného pokrytí silami a prostředky,* • *pro stanovení a optimalizaci standardů technických podmínek techniky a věcných prostředků vybavení jednotek PO,* • *pro modernizaci věcných prostředků a výstroje hasičů v jednotkách PO s cílem zvýšení jejich komfortu a výkonových možností při zásahu,*	

		• *pro zdokonalení informační podpory velitele zásahu,* • *pro posílení schopností HZS ČR přejímat humanitární pomoc a záchranářů ze zahraničí a poskytovat ji do zahraničí,* • *pro zvýšení akceschopnosti HZS krajů a ZÚ HZS ČR při záchranných a likvidačních pracích v případě živelních a dalších pohromách,* • *pro optimalizaci systému vzdělávání a odborné přípravy příslušníků HZS a dalších složek systému havarijní připravenosti podílejících se zásahu při mimořádných situacích,* • *pro informační podporu sběru dat o jednotkách SDH obcí do informačního systému HZS ČR,* • *pro optimalizaci posttraumatické péče a psychosociální krizové pomoci obětem mimořádných událostí v úzké spolupráce se zdravotnickými zařízeními (příjmové nemocnice, zařízení poskytující speciální lékařskou péči),* • *k optimalizaci stavu civilních zdrojů zajišťujících bezpečnost ČR zejména ve vztahu na nové potřeby a možnosti jejich saturace,* • *pro optimalizaci komunikačního systému s cílem vytvářet efektivní podmínky pro činnost příslušných orgánů, zasahujících složek a pro rychlé poskytování tísňových informací obyvatelstvu v místech ohrožení* *Důležité je zvýšení efektivity alokace a využití veřejných zdrojů při mimořádných událostech a krizových situací na základě nových poznatků v oblasti cost-benefit analýz.*	
Vazba na ostatní dílčí cíle:			
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva		Rozvíjet a zdokonalovat organizační, technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná, následná a dlouhodobá opatření na ochranu obyvatel – ukrytí, evakuaci/přesídlení, zdravotní péči postiženým, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití prostředků/zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování a komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů		Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby		Zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy		Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,2**	Tento dílčí cíl je expertně čtvrtý nejvýše hodnocený cíl v rámci prioritní oblasti 6 „Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR“. To potvrzuje významnost a prioritu dílčího cíle pro fungování státu, infrastruktur, bezpečnost občanů, občanské společnosti a pro obranu státu. Klíčovou roli při zajišťování vnitřní bezpečnosti a ochrany obyvatelstva hrají bezpečnostní sbory, zejména pak Integrovaný záchranný systém – tzn. Hasičský záchranný sbor ČR, dále Policie ČR a Zdravotnická záchranná služba. Významnou roli mají i další složky systému havarijní připravenosti, které v rozsahu svých zákonných oprávnění se podílejí na detekci/monitorování vzniku a vývoje a hodnocení dané události, na zajištění zdravotní péče o postižené osoby a na zabezpečování veřejného pořádku. Specifickou roli má Armáda ČR, jejíž síly a prostředky mohou být využity k posílení Policie ČR a integrovaného záchranného systému v případě, že se jejich síly ukážou jako nedostatečné. Mezi ekonomické přínosy činnosti IZS, zejména HZS ČR patří zejména uchráněné hodnoty na zdraví a majetku nejen při požárech, ale i při dalších druzích událostí, jako jsou například dopravní nehody, živelné pohromy, úniky nebezpečných chemických látek, technické havárie, radiační nehody a havárie. Dalším důležitým ekonomickým přínosem jsou důsledky činnosti na poli prevence.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**4,0**	
Významnost cíle pro obranu státu:	**4,1**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Bezpečnostní vědy 2) Ochrana obyvatelstva 3) Ekonomie 4) Bezpečnostní technologie 5) Civilní nouzové plánování 6) Havarijní připravenost
Současná úroveň a kvalita výzkumu v ČR:	**4,0**	Současná úroveň a kvalita výzkumu v ČR je na vysoké úrovni. Česká republika disponuje kvalifikovanými týmy s odpovídajícími praktickými zkušenostmi. Úroveň výzkumné infrastruktury je dobrá. Existují dobré předpoklady pro dosažení stanovených cílů. Podnikatelská sféra obecně a zejména pak podnikatelská sféra působící v oblasti výroby je relativně dobře připravena a je schopna nové poznatky výzkumu a vývoje absorbovat a využít. Některé řešitelské týmy a řešitelské organizace mají předpoklady obstát v mezinárodním konkurenčním prostředí. Finanční prostředky vynaložené na výzkum, experimentální vývoj a inovace pro tento dílčí cíl je nezbytné považovat za podstatné pro zvyšování úrovně připravenosti ČR na zvládání mimořádných událostí a krizových situací. Z tohoto pohledu lze považovat dosažené bodové hodnocení za zcela podhodnocené. V reálném odhadu je adekvátní úroveň 1,4 bodového hodnocení. Vláda rozhodla v budoucnu prohlubovat spolupráci a vybavení základních složek Integrovaného záchranného systému včetně posílení spolupráce s Armádou ČR s cílem minimalizovat dopady mimořádných událostí na životy a majetek občanů a zefektivnit nakládání s prostředky veřejných rozpočtů. Je třeba zaměřit se na budování efektivních zařízení civilní ochrany, kde síly a prostředky veřejných institucí, privátního sektoru mohou významně přispět jak v oblasti prevence, tak likvidace následků mimořádných událostí. Jde o vybavení sboru dobrovolných hasičů za účelem jeho většího zapojení do řešení mimořádných událostí, avšak zapojení dalších institucí a obyvatel s cílem zvýšit jejich participaci na sebeochraně, ale i dalších činnostech, na nichž mohou efektivně participovat Absorpční kapacita aplikační sféry je na vysokém stupni. Uživatelem výsledků výzkumu a vývoje budou bezpečnostní a záchranné složky a podnikatelská sféra působící v oblasti zajišťování bezpečnosti. Důraz bude položen na to, aby výsledky výzkumu a vývoje naplňovaly požadované schopnosti bezpečnostních a záchranných složek. Výsledky výzkumu a vývoje musí být uchopitelné a využitelné zákazníky, kteří si je vyžádali, nebo musí vytvářet předpoklady pro následující vývoj, či inovace. Na projekty veřejných zakázek na vývoj či inovace musí navazovat následná akvizice ze strany zadavatele. Lze předpokládat stimulaci trhu bezpečnostních technologií s nabídkovou a poptávkovou stranou.
Úroveň výzkumné infrastruktury:	**4,0**	
Podpora ve státní politice a regulaci:	**3,7**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,1**	
Očekávaná finanční náročnost dosažení cíle:	**2,0**	
Absorpční kapacita aplikační sféry:	**4,3**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	1 Bezpečnost občanů
Podoblast:	1.1 Ochrana obyvatelstva
Stěžejní cíl:	Stěžejním cílem je zabezpečení odpovídající úrovně ochrany obyvatelstva evropského standardu, eliminace možností vzniku přírodních a antropogenních pohrom a minimalizace dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní podmínky. To zahrnuje rozvoj a zdokonalování technických, organizačních, řídících, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

Název dílčího cíle:	**1.1.3 Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů**	**2030** (průběžně)
Popis dílčího cíle:	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Ochranu obyvatelstva regionů, měst a obcí před účinky živelních pohrom a provozních havárií vytvářet z hlediska udržitelného rozvoje v rozvojových programech území a územním plánování a to s ohledem k rozvoji území a jeho bezpečnosti a řízení lidských aktivit (v oblasti bydlení, ekonomického a sociálního rozvoje, podnikatelských aktivit, rozvoje technické, sociální, dopravní a další infrastruktury). Posilovat ochranu obyvatelstva a rozvoj chráněných zájmů měst a obcí s důrazem na proaktivní přístupy, monitoring a na procesní řízení ochrany obyvatelstva při živelních pohromách a provozních haváriích.* *Vytvořit nové efektivní a funkční formy a metody vzdělávání občanů v oblasti ochrany obyvatelstva, zejména v problematice snižování rizik, ale také v oblasti sebeochrany a vzájemné pomoci při mimořádných událostech jako významného prvku eliminace následků mimořádných událostí. Aplikovat zásady a ustanovení mezinárodního humanitárního práva, s důrazem na Ženevské úmluvy z roku 1949 a jejich dodatkových protokolů (k jejich šíření se smluvní strany zavázaly i v době míru) a „Aktualizované obecné zásady Evropské unie na podporu dodržování mezinárodního humanitárního práva“ vydané Radou EU v roce 2009“ v podmínkách ČR. Aplikace* etických, *sociálních a právních aspektů ochrany obyvatelstva v souladu s mezinárodními smlouvami a etickým bezpečnostním kodexem, který je mravní normou zahrnující respekt jak k ochraně celé společnosti, tak k ochraně jednotlivého člověka.* *Zvýšit připravenost jedinců a komunity k sebeochraně v případech mimořádných situací a krizových stavů se zaměřením na vnímání a hodnocení rizik. Zefektivnění komplexního systému vzdělávání na všech úrovních.* *Zajistit soulad opatření k ochraně obyvatelstva se základními lidskými právy a principy fungování demokratického státu a občanské společnosti se zaměřením na dodržování a propagování etických a sociálních aspektů bezpečnosti. Navrhnout systémová pravidla pro práci s médii v případech mimořádných událostí a krizových situací.*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy. *Přes existenci preventivních opatření dochází čas od času k nadprojektovým mimořádným událostem. Součástí vzdělávání by mělo být uplatňována zásada využívat fázi obnovy nikoliv k pouhé obnově, ale i ke zvýšení odolnosti území / infrastruktury pro případ opakování takové události.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle	
Významnost pro fungování státu a infrastruktur: **3,7**	Tento dílčí cíl je expertně vysoce hodnocený cíl v rámci prioritní oblasti 6 Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR. To potvrzuje významnost a prioritu dílčího cíle pro fungování státu, bezpečnosti státu, regionu, obce, podniku, objektu, organizace, bezpečnost občanů, občanské společnosti a pro obranu státu. Předpokládané zaměření výzkumu a vývoje je tak bezprostředně spojeno s určením a specifikací negativ a pozitiv vnějšího i vnitřního prostředí; s vývojem priorit MV ČR jako ústředního orgánu státní správy pro krizové řízení civilní nouzové plánování, ochranu obyvatelstva, integrovaný záchranný systém a požární ochranu a zejména pak s postupným zvyšováním účinnosti technických, technologických, metodických, produktových, distribučních, organizačních, vzdělávacích, legislativních, informačních, komunikačních a rozhodovacích subsystémů Bezpečnostního systému České republiky; s postupným zvyšováním připravenosti státu, regionů, obcí, podniků, objektů a organizací efektivně reagovat na současné i předpokládané budoucí krizové situace mírového charakteru, ale i v případě vyhlášení stavu ohrožení nebo válečného stavu. Zaměření výzkumu a vývoje je tak významným přínosem pro fungování státu a jeho infrastruktur, pro zvýšení úrovně bezpečnosti občanů a občanské společnosti, ale i pro obranu státu při krizových situacích mírového i válečného charakteru.
Významnost cíle pro bezpečnost občanů a občanské společnosti: **3,8**	
Významnost cíle pro obranu státu: **3,6**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Ochrana obyvatelstva 3) Ekonomie 4) Bezpečnostní technologie 5) Civilní nouzové plánování
Současná úroveň a kvalita výzkumu v ČR: **3,6**	Současná úroveň a kvalita výzkumu v ČR a úroveň výzkumné infrastruktury je na kvalitativně vysoké úrovni s možnostmi dalšího potencionálního růstu. Stát tuto oblast systematicky, komplexně a dlouhodobě koordinuje na odpovídající úrovni. Česká republika disponuje kvalifikovanými týmy s praktickými zkušenostmi a odpovídající úrovní vzdělávání. Na nižší úrovní je zapojení mladých vědeckých pracovníků. Odhad finanční náročnosti dosažení cíle je vzhledem k rozsahu řešené problematiky a očekávaným výsledkům nízká. Z dlouhodobých zkušeností lze předpokládat míru finanční náročnosti na úrovni 1,7 bodové škály. Absorpční kapacita aplikační sféry je vzhledem ke skutečnosti, že zaměření výzkumu a vývoje řeší priority bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace, nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování, velmi vysoká. Uživatelem výsledků výzkumu a vývoje budou instituce státní správy a samosprávy, prvky Bezpečnostního systému ČR, bezpečnostní složky a podnikatelské subjekty působící v oblasti zajišťování bezpečnosti.
Úroveň výzkumné infrastruktury: **3,9**	
Podpora ve státní politice a regulaci: **3,3**	
Kvalita lidských zdrojů a úroveň vzdělávání: **3,8**	
Očekávaná finanční náročnost dosažení cíle: **2,4**	
Absorpční kapacita aplikační sféry: **3,8**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	1 Bezpečnost občanů
Podoblast:	1.2 Ochrana před kriminalitou, extremismem a terorismem
Stěžejní cíl:	Stěžejním cílem této oblasti je vybudovat v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře eliminovat všechny formy kriminality, extremismu a terorismu, což vyžaduje vyvážený systém prevence a represe a současně sledování trendů, kterými se vývoj kriminality, extremismu a terorismu ubírá (včetně využití technologií či zneužití digitálních informací kriminálníky, adaptace kriminální sféry na nové demografické podmínky, mapování míry nehlášené kriminality a korupce apod.), a nástrojů jejího odhalování a potírání.

Název dílčího cíle:	**1.2.1 Vytváření účinných metod analýzy druhů a rozšířenosti kriminality a implementace efektivních nástrojů jejího potírání**	**2020**
Popis dílčího cíle:	Cílem je rozvíjet nástroje analýzy hrozeb, rizik a rozšířenosti kriminality, včetně kriminality organizované, mapování trendů a vytváření nástrojů pro odhadování skutečné trestné činnosti (s ohledem na regiony, na socioekonomický vývoj, s ohledem na určité skupiny skutkových podstat, struktura pachatelů a obětí atd.) a také rozvoj nástrojů pro odhadování nezjištěné trestné činnosti. Dále je cílem rozvoj nových technik a technologií pro odhalování, dokazování a potírání trestných činů a projevů extremismu a terorismu.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých. *Varování před a příprava na případné extrémistické a teroristické útoky (1.2.1) jsou důležitým vstupem pro přípravy na vznik krizových situací a minimalizaci jejich následků (1.1.1).*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací	Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům. *Spolupráce v oblasti odhalování a potírání kriminality kybernetické (1.2.2) a ne-kybernetické (1.2.1) je zásadní, organizované skupiny se často angažují ve více druzích kriminality. Represe vůči kybernetické kriminalitě by měla přijí v reálném světě. Rovněž extremistické a teroristické skupiny patří mezi nejpokročilejší uživatele nových technologií, jež zneužívají pro své účely.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem

Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness). Rozpoznání hrozby případných extrémistických a teroristických útoků (1.2.1) vůči kritickým infrastrukturám je důležitou součástí identifikace hrozeb vůči KI (2.1.4).	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 3.1.1: Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti	Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda) a Parlament ČR jak přistupovat k tomuto procesu. *Výstupy z analýz a mapování trestné činnosti v 1.2.1 jsou přímými vstupy do vyhodnocování v 3.1.1.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému). *Nástroje analýzy mapující dynamický vývoj kriminální činnosti, extremismu a terorismu a jejich informační výstupy (1.2.1) jsou důležitým vstupem pro predikci vývoje bezpečnostních rizik a adaptabilitu na změny v bezpečnostním prostředí (3.1.2).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Nástroje analýzy mapující dynamický vývoj kriminální činnosti, extremismu a terorismu a jejich informační výstupy (1.2.1) jsou důležitým vstupem pro analýzu bezpečnostních hrozeb a predikci rizik (3.2.1),*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací	Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů. *Nástroje analýzy mapující dynamický vývoj kriminální činnosti, extremismu a terorism a jejich informační výstupy (1.2.1) jsou důležitým vstupem pro zlepšování systémů získávání a třídění (3.3.1) a analýzy (3.3.2) bezpečnostních informací, jakož i pro trvalé vyhodnocování a zdokonalování účinnosti bezpečnostního systému (3.3.3).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.3.2: Analýza bezpečnostních informací	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

	Nástroje analýzy mapující dynamický vývoj kriminální činnosti, extremismu a terorism a jejich informační výstupy (1.2.1) jsou důležitým vstupem pro zlepšování systémů získávání a třídění (3.3.1) a analýzy (3.3.2) bezpečnostních informací, jakož i pro trvalé vyhodnocování a zdokonalování účinnosti bezpečnostního systému (3.3.3).	
Dílčí cíl 3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení	Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti. *Nástroje analýzy mapující dynamický vývoj kriminální činnosti, extremismu a terorism a jejich informační výstupy (1.2.1) jsou důležitým vstupem pro zlepšování systémů získávání a třídění (3.3.1) a analýzy (3.3.2) bezpečnostních informací, jakož i pro trvalé vyhodnocování a zdokonalování účinnosti bezpečnostního systému (3.3.3).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,0**	Úspěšnost v prevenci a potírání kriminality, extremismu a terorismu je základním předpokladem důvěry a sounáležitosti mezi občany a státem a základním kamenem fungující demokracie a občanské společnosti. Případné pronikání organizovaného zločinu či extremismu do státních struktur může stát ochromit, učinit neefektivním či zcela destabilizovat, a to jak v hospodářské, tak v politické rovině. Pro úspěšné fungování občanské společnosti je důležitá i ochrana různých menšin, často snadněji zranitelných specifickými druhy kriminality či agresí ze strany extremistů. Předcházení případným teroristickým útokům je neméně významné, ať už z pohledu ochrany kritických infrastruktur či bezpečnosti občanů. Mnoho dalších dílčích cílů obranyschopnosti země je přímo závislých na schopnosti efektivně a přesně mapovat a analyzovat stav kriminality a extremistickych a teroristických aktivit a hrozeb v zemi, což výrazně zvyšuje význam tohoto dílčího cíle.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,7**	
Významnost cíle pro obranu státu:	**3,0**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Kriminalistika 2) Kriminologie 3) Sociologie 4) Ekonomie 5) Biologie 6) Chemie 7) Informatika 8) Právo

Současná úroveň a kvalita výzkumu v ČR:	**3,3**
Úroveň výzkumné infrastruktury:	**2,9**
Podpora ve státní politice a regulaci:	**2,9**
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,0**

Očekávaná finanční náročnost dosažení cíle:	**2,6**	v kriminologickém, právním i sociologickém výzkumu kriminality (včetně organizované kriminality a korupce). Kvalitní je kriminalistický výzkum, který však potřebuje zásadní technologickou modernizaci v řadě oborů. Totéž platí i pro informatiku v boji proti uvedeným hrozbám, kde je třeba ji koncentrovat kolem nově vznikajících potřeb specializovaného pracoviště Národního bezpečnostního úřadu. Ekonomický výzkum uvedených fenoménů (s dílčí výjimkou korupce) je slabý a je v nepoměru k rozvinutosti a pokročilosti ekonomie v jiných oblastech (přičemž obecně je třeba reflektovat i debatu o kvalitě a odůvodněnosti IF faktoru u některých ekonomických periodik vycházejících v ČR).
Absorpční kapacita aplikační sféry:	**3,4**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	1 Bezpečnost občanů
Podoblast:	1.2 Ochrana před kriminalitou, extremismem a terorismem
Stěžejní cíl:	Stěžejním cílem této oblasti je vybudovat v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře eliminovat všechny formy kriminality, extremismu a terorismu, což vyžaduje vyvážený systém prevence a represe a současně sledování trendů, kterými se vývoj kriminality, extremismu a terorismu ubírá (včetně využití technologií či zneužití digitálních informací kriminálníky, adaptace kriminální sféry na nové demografické podmínky, mapování míry nehlášené kriminality a korupce apod.), a nástrojů jejího odhalování a potírání.

Název dílčího cíle:	**1.2.2 Minimalizace kybernetické kriminality a zneužívání informací**	**2020**
Popis dílčího cíle:	Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění rganizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům. *Se zvyšováním využití výpočetní techniky a chytrých mobilních zařízení se zvyšuje i atraktivita této oblasti pro skupiny organizovaného zločinu. Kromě přímých ekonomických dopadů na firmy a občany však kybernetická kriminalita představuje i možné ohrožení kritické infrastruktury a bezpečnosti země.*	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.2.1: Vytváření účinných metod analýzy druhů a rozšířenosti kriminality a implementace efektivních nástrojů jejího potírání	Cílem je rozvíjet nástroje analýzy hrozeb, rizik a rozšířenosti kriminality, včetně kriminality organizované, mapování trendů a vytváření nástrojů pro odhadování skutečné trestné činnosti (s ohledem na regiony, na socioekonomický vývoj, s ohledem na určité skupiny skutkových podstat, struktura pachatelů a obětí atd.) a také rozvoj nástrojů pro odhadování nezjištěné trestné činnosti. Dále je cílem rozvoj nových technik a technologií pro odhalování, dokazování a potírání trestných činů a projevů extremismu a terorismu. *Vazba je především na první dva z výše uvedených bodů.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů. *Kromě přímých dopadů při cíleném útoku na kritickou infrastrukturu jsou závažná i rizika pramenící z vedlejších efektů kybernetické kriminality – přetížení infrastruktury, zahlcení systémů a jejich částí, počítačové viry v řídících částech KI apod.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 3.3.2: Analýza bezpečnostních informací	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. *Analýza možných hrozeb, sledování dat umožňující včasnou detekci a především rozvíjení scénářů možných útoků a jejich dopadů je z hlediska ochrany před kybernetickou kriminalitou a minimalizace jejích dopadů naprosto zásadní.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 4.1.4: Rozvoj KIS a kybernetická obrana	Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací	**Oblast 4:** Obrana, obranyschopnost a nasazení ozbrojených sil **Podoblast 4.1:** Rozvoj schopností ozbrojených sil

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,6**	Hlavní rizika kybernetické kriminality pramení z přímých dopadů na ekonomiku, možného využití k průmyslové špionáži a k útokům na kritickou infrastrukturu. Především možné zásadní narušení kritické infrastruktury, ať už jsou to komunikační kanály, řídící systémy průmyslových a energetických komplexů nebo zdravotnická a záchranná infrastruktura, představují největší bezpečnostní rizika pro fungování infrastruktur a zajištění bezpečnosti státu.Z hlediska zajištění bezpečnosti občanů a občanské společnosti jsou kritické hospodářské dopady kybernetické kriminality a především oblast ochrany osobních údajů a osobní identity. Zneužití osobních údajů možnými útoky na sociální sítě, systémy elektronické pošty, infrastruktury různých tzv. cloud systémů, ale především útoky na informační systémy státní a veřejné správy představují významné riziko pro důvěru občanů ve fungování státu a státní správy.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,1**	
Významnost cíle pro obranu státu:	**3,3**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Informatika 2) Kriminalistika 3) Kriminologie 4) Ekonomie

Současná úroveň a kvalita výzkumu v ČR:	**3,5**
Úroveň výzkumné infrastruktury:	**3,3**
Podpora ve státní politice a regulaci:	**2,9**
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**
Očekávaná finanční náročnost dosažení cíle:	**2,7**

Absorpční kapacita aplikační sféry: 4,2	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.1 Ochrana, odolnost a obnova kritických infrastruktur
Stěžejní cíl:	Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Název dílčího cíle:	**2.1.1 Rozvoj alternativních a nouzových krizových procesů**	**2020**
Popis dílčího cíle:	Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI. *Na základě zjištěných nedostatků v procesech a neexistenci nebo nefunkčnosti některých provozních prvků doporučovat opatření pro zvyšování odolnosti KI.*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR. *Dílčí cíl 2.1.1 je nezbytným krokem pro zvyšování kvalitativní a snižování kvantitativní úrovně podpůrných procesů zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných krizových situacích.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva

	vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Rozvoj alternativních a nouzových krizových procesů snižuje závažnost dopadů mimořádných událostí a krizových situací na regiony, města, obce, zdraví a životy lidí, jejich majetky a životní prostředí.*	
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů. *Rozvoj alternativních a nouzových krizových procesů je vhodným opatřením tam, kde je zvyšování odolnosti KI technicky či ekonomicky nedostupné*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. *V současném stavu techniky jsou téměř všechny systémy KI včetně alternativních a nouzových procesů závislé na funkčnosti a bezpečnosti ICT*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.1: Vzájemné závislosti systémů KI	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. *Vzájemná závislost systémů KI může způsobovat zesilující negativní účinky mimořádných událostí a domino efekty*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami
Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy. *Rozvoj funkčnosti KI je závislý na na systému podpory obnovy.*	**Oblast 3: Krizové řízení a bezpečnostní politika** **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,4**	Alternativní nouzové a krizové procesy umožňující nezbytnou úroveň provozu (Minimal Service Level) při nefunkčnosti částí KI a jejich nadřazených soustav mají kritický význam pro zajišťování základních fyziologických potřeb a zajištění bezpečnosti občanů, státu, majetku a životního prostředí.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,8**	
Významnost cíle pro obranu státu:	**3,9**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Manažerské systémy řízení 2) Bezpečnostní vědy 3) Technické a zemědělské vědy 4) Energetické zdroje 5) Udržitelný rozvoj

Současná úroveň a kvalita výzkumu v ČR:	**4,4**	Obecné zásady (například managementu kontinuity) jsou k dispozici. Současná výzkumná infrastruktura je schopna tyto zásady v rámci aplikovaného výzkumu adaptovat na jednotlivé oblasti kritické infrastruktury. V řadě případů se bude jednat o „soft“ opatření, která nemusí být ekonomicky příliš náročná. Výsledky výzkumu mohou být uplatněny a využity prakticky u všech subjektů kritické a další nezbytné infrastruktury. Bude se prakticky jednat o procesní analýzy zaměřené na optimalizaci systémového řešení s významnou složkou osobních nákladů, tedy 4 klasifikace finanční náročnosti..
Úroveň výzkumné infrastruktury:	**4,0**	
Podpora ve státní politice a regulaci:	**3,7**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,3**	
Očekávaná finanční náročnost dosažení cíle:	**2,4**	
Absorpční kapacita aplikační sféry:	**4,2**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.1 Ochrana, odolnost a obnova kritických infrastruktur
Stěžejní cíl:	Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Název dílčího cíle:	**2.1.2 Zvyšování odolnosti KI**	**2020**
Popis dílčího cíle:	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů.	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Zvýšená odolnost KI snižuje její zranitelnost a tím i četnost mimořádných událostí a krizových situací*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů	Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI. *Kde je zvyšování odolnosti KI technicky či ekonomicky nedostupné, je nutné zajisti*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

	rozvoj alternativních a nouzových krizových procesů zmírňujících dopady mimořádných událostí	
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. *V současném stavu techniky jsou téměř všechny systémy KI závislé na funkčnosti a bezpečnosti ICT*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.1: Vzájemné závislosti systémů KI	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. *Vzájemná závislost systémů KI může způsobovat zesilující negativní účinky mimořádných událostí a domino efekty*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Rozvoj analytických nástrojů umožní postihnout variabilitu bezpečnostních hrozeb, průběhů scénářů (a) vývoje bezpečnostní situace nejen v ČR, ale i v Evropě a tím pádem i ve světě.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,5**	Odolnost KI má kritický význam pro zajištění bezpečnosti občanů, státu, majetku a životního prostředí. Bez nových analytických nástrojů bude stagnovat schopnost postihnout průběh scénářů novodobých bezpečnostních hrozeb snižujících odolnost KI.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,9**	
Významnost cíle pro obranu státu:	**4,0**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Bezpečnostní vědy (Bezpečnostní inženýrství) 2) Udržitelný rozvoj 3) Informační technologie
Současná úroveň a kvalita výzkumu v ČR:	**3,9**	V některých oblastech, jako jsou například jaderná energetika a přenosová soustava České republiky, je praxe zvyšování odolnosti velmi dobře zvládnuta. Současná výzkumná infrastruktura je schopna tyto zásady a přístupy v rámci aplikovaného výzkumu adaptovat na další oblasti kritické infrastruktury. Pro ověření navrhovaných opatření bude vhodné realizovat pilotní projekty, z nichž některé mohou být finančně náročné. Výsledky výzkumu mohou být uplatněny a využity prakticky u všech subjektů kritické a další nezbytné infrastruktury, avšak budou většinou vyžadovat úpravu legislativy a předpisů. Do oblasti vyšší finanční náročnosti posune dílčí cíl nutný proces verifikace a validace vyvinutých analytických metod a nástrojů.
Úroveň výzkumné infrastruktury:	**3,9**	
Podpora ve státní politice a regulaci:	**3,3**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**	
Očekávaná finanční náročnost dosažení cíle:	**2,4**	
Absorpční kapacita aplikační sféry:	**4,2**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.1 Ochrana, odolnost a obnova kritických infrastruktur
Stěžejní cíl:	Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Název dílčího cíle:	**2.1.3 Zajištění a rozvoj interoperability KI**	**2020**
Popis dílčího cíle:	Tvorba nástrojů pro zajištění a rozvoj interoperability KI (dopravní, energetické a dalších) s nadnárodními evropskými KI. Vazba na nadnárodní evropské síťové systémy (TEN-T, TEN-E). Modelování a výpočty sítí.	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. V současném stavu techniky jsou téměř všechny systémy KI závislé na funkčnosti a bezpečnosti ICT	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.1: Vzájemné závislosti systémů KI	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. Vzájemná závislost systémů KI může způsobovat zesilující negativní účinky mimořádných událostí a domino efekty	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. Výsledky analýz bezpečnostních hrozeb a tvorba scénářů vývoje	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

	bezpečnostní situace ve světě a Evropě ovlivňuje potřebu rozvoje interoperability a vazeb na evropskou KI zejména v oblasti síťových systémů a zajištění přístupu ke zdrojům, jež je nutno dovážet.	
Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy. Zajištění a rozvoj interoperability KI má význam pro prevenci, odezvy a obnovu. Snižuje pravděpodobnost vzniku mimořádných událostí a přispívá ke zkracování doby obnovy.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,1**	Vzhledem k tomu, že ČR je otevřená ekonomika s významným podílem zahraničního obchodu a omezenými zdroji domácích zdrojů energie, je napojení na celoevropské energetické a dopravní sítě zcela zásadní z hlediska energetické a ekonomické bezpečnosti.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,4**	
Významnost cíle pro obranu státu:	**3,9**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Technické vědy 3) Udržitelný rozvoj

Současná úroveň a kvalita výzkumu v ČR:	**3,7**	Úroveň a kvalita výzkumné infrastruktury je v oblastech energetiky a dopravy vysoká. Současná výzkumná infrastruktura je schopna tyto úlohy řešit včetně výzkumu na celoevropské úrovni spolu se zahraničními týmy. V řadě případů se bude jednat o „soft“ opatření, která nemusí být ekonomicky příliš náročná. Výsledky výzkumu mohou být uplatněny při tvorbě a realizaci strategických a koncepčních dokumentů, zejména v oblasti energetiky a dopravy.
Úroveň výzkumné infrastruktury:	**3,7**	
Podpora ve státní politice a regulaci:	**3,0**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,0**	
Očekávaná finanční náročnost dosažení cíle:	**3,0**	
Absorpční kapacita aplikační sféry:	**4,2**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.1 Ochrana, odolnost a obnova kritických infrastruktur
Stěžejní cíl:	Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Název dílčího cíle:	**2.1.4 Účinná detekce a identifikace hrozeb**	**2020**
Popis dílčího cíle:	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Účinná detekce a identifikace hrozeb ve vztahu ke KI umožňuje snižování rizika a zvyšování ochrany obyvatelstva.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování	Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Vývoj systémů predikce a včasného varování. *Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI poskytuje podporu pro účinnou detekci a identifikaci*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami

	hrozeb v oblasti KI	
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Analýza vývoje bezpečnostní situace ve světě, Evropě a ČR je jedním z východisek pro stanovení požadavků na potřebnou adaptaci systémů KI*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.2.2: **Podpora specifických oblastí bezpečnosti**	Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků *Pro účinnou detekci a identifikaci hrozeb je třeba veškeré činnosti nahlížet z pohledu kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel tak, aby nedocházelo především v oblasti základních fyziologických potřeb (voda, energie, potraviny) k řešení jedné bezpečnosti na úkor zbývajících.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,0**	Účinná detekce a identifikace hrozeb má kritický význam pro proaktivní adaptaci systémů KI a tím ekonomicky optimální zajištění bezpečnosti občanů, majetku a životního prostředí.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,3**	
Významnost cíle pro obranu státu:	**3,5**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Mezinárodní vztahy 3) Informační technologie 4) Udržitelný rozvoj

Současná úroveň a kvalita výzkumu v ČR:	**3,7**	Současná výzkumná infrastruktura je schopna tyto zásady a přístupy. Hlavní problém bude spočívat v rezortním přístupu, který znesnadňuje koordinaci snižování rizika napříč resorty, aby nedocházelo k nepříznivému ovlivňování. V řadě případů se bude jednat o „soft“ opatření, která nemusí být ekonomicky příliš náročná. Výsledky výzkumu mohou být uplatněny a využity prakticky u všech subjektů kritické a další nezbytné infrastruktury.
Úroveň výzkumné infrastruktury:	**3,7**	
Podpora ve státní politice a regulaci:	**3,2**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**	
Očekávaná finanční náročnost dosažení cíle:	**3,2**	
Absorpční kapacita aplikační sféry:	**3,9**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.1 Ochrana, odolnost a obnova kritických infrastruktur
Stěžejní cíl:	Zajištění funkčnosti KI s cílem zamezit rozvinutí nežádoucích stavů vzniklých v důsledku vnějších vlivů, zahrnujících přírodní pohromy a úmyslné antropogenní činy, do kritických situací. Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury. Aplikace managementu kontinuity činností organizací kritické infrastruktury. Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů KI, rozhodování a řízení návazných procesů souvisejících se zabezpečením KI a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury.

Název dílčího cíle:	**2.1.5 Rozvoj ICT, telematiky a kybernetické ochrany KI**	**2020**
Popis dílčího cíle:	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. *Podíl ICT technologií na provozu a řízení KI roste a tento růst se dá předpokládat i ve středně a dlouhodobém výhledu. Stejně tak roste význam ICT technologií pro ochranu, odolnost a obnovu KI. Řešení předkládaná v rámci tohoto dílčího cíle by se měla zaměřit na využití ICT technologií pro včasné odhalení a prevenci bezpečnostních hrozeb, podporu řešení krizových situací v případě nastalých incidentů, analýzu, vyhodnocení a připravenost struktur a lidských zdrojů na bezpečnostní incidenty a jejich průběh.* *Kybernetická ochrana systémů KI a ochrana citlivých informací hraje v tomto celku zcela jedinečnou úlohu. Frekvence a pravděpodobnost kybernetických útoků na informační systémy se v posledních měsících dramaticky zvyšovala. Tento trend bude jistě pokračovat a v blízké budoucnosti se informační systémy stanou prostorem, ve kterém se děje kriminalita s velkými následky ale i prostorem, kde budou probíhat cílené útoky nepřátelských režimů a mocností na fungování celé společnosti. Řešení předkládaná v rámci tohoto dílčího cíle by se proto měla věnovat zneužitelnosti ICT systémů KI a jejich kybernetické ochraně.*	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací	Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům. *Dílčí cíl 1.2.2 se zabývá kybernetickou kriminalitou na úrovni ochrany občanů, zatímco dílčí cíl 2.1.5 se zaměřuje specificky na oblast KI. Oba cíle se zároveň překrývají (používají stejné, nebo koncepčně podobné metody) a doplňují (kybernetický útok na KI, kterému zabránit/odolat*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem

	ukládá cíl 2.1.5 je zároveň kriminálním činem, jehož odhalení a prevenci ukládá cíl 1.2.2).	
Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů	Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI. *Technologie podílející se na ochraně KI při nastalém incidentu nutně musí přesahovat do oblasti řešení krizových situací. Například přístupové systémy KI musí v případě krize přejít do nouzového režimu, kdy dovolují přístup, monitorovací ochranné systémy dávají informace použitelné pro efektivní evakuaci apod.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů. *Technologická řešeni zadaná cílem 2.1.5 jsou specifickou podmnožinou cíle 2.1.2.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness). *Technologická řešeni zadaná cílem 2.1.5 jsou specifickou podmnožinou cíle 2.1.4.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1 :** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.1: Vzájemné závislostí systémů KI	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. *Řešení stěžejního cíle 2.2 je nutným aspektem funkčnosti řešení cíle 2.1.5 kvůli závislostem mezi propojenými KI. Jinými slovy: kde existují závislosti mezi různými KI, technologická řešení musí tyto závislosti zohledňovat.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami
Dílčí cíl 2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování	Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Vývoj systémů predikce a včasného varování. Řešení stěžejního cíle 2.2 je nutným aspektem funkčnosti řešení cíle 2.1.5 kvůli závislostem mezi propojenými KI. Jinými slovy: kde existují závislosti mezi různými KI, technologická řešení musí tyto závislosti zohledňovat.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami

Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Ochrana KI jako jedna z nejdůležitějších oblastí musí být vzata v úvahu při vytváření strategie na národní úrovni.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací	Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů. *Informační technologie zabezpečení KI které jsou zadáním cíle 2.1.5 jsou nezbytnou součástí systémů analýzy, prevence a obnovy na národní úrovni*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3**: Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.3.2: Analýza bezpečnostních informací	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. *Informační technologie zabezpečení KI které jsou zadáním cíle 2.1.5 jsou nezbytnou součástí systémů analýzy, prevence a obnovy na národní úrovni*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3**: Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení	Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti. *Informační technologie zabezpečení KI které jsou zadáním cíle 2.1.5 jsou nezbytnou součástí systémů analýzy, prevence a obnovy na národní úrovni*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.4.1: Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací	Analyzovat a vytvářet legislativní postupy a opatření tak, aby legislativní rámec vytvářet komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje. *Je nezbytné nastavit legislativní rámec ochrany KI tak, aby byl v souladu s ostatními oblastmi národní bezpečnosti.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.4:** Legislativní a právní problémy

Dílčí cíl 4.1.4: Rozvoj KIS a kybernetická obrana	Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací. *Existuje silný překryv mezi těmito dílčími cíly v oblasti kybernetické ochrany, rozdílem je jiná aplikační oblast (civilní vs. vojenské KI). Oba cíle používají stejné, nebo koncepčně podobné metody a dá se říct, že řešení zpracované pro jednu oblast bude koncepčně aplikovatelné v oblasti druhé.*	**Oblast 4:** Obrana, obranyschopnost a nasazení ozbrojených sil **Podoblast 4.1:** Rozvoj schopností ozbrojených sil

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,0**	Ze samotné definice KI vyplývá, že spolehlivé fungování KI je nezbytným předpokladem pro každodenní chod společnosti a naopak narušení funkce KI má závažné dopady na bezpečnost a prosperitu každého občana a celé společnosti jako celku. Význam a důležitost ICT, telematiky a zvláště kybernetické ochrany systémů pro bezpečnost KI se trvale zvyšuje spolu s tím, jak roste podíl ICT technologií na řízení a provozu KI. Tento podíl ICT technologií na řízení a provozu KI se bude v budoucnosti nadále zvyšovat a tedy poroste i významnost tohoto dílčího cíle ve středně a dlouhodobém časovém horizontu. Významnost tohoto cíle obdržela v hlasování expertů vysoká hodnocení, což dokládá široké povědomí a významný přesah tohoto dílčího cíle do ostatních bezpečnostních oblastí. Dalším zaznamenáníhodným aspektem výsledků hlasování o významnosti je to, že dílčí cíl 2.1.5 obdržel podobně vysoké hodnocení významnosti jako ostatní dílčí cíle oblasti č. 2, „Bezpečnost kritických infrastruktur a zdrojů“. Tento fakt dokládá vysokou důležitost ochrany KI jako celku.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,2**	
Významnost cíle pro obranu státu:	**3,7**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Bezpečnostní vědy 2) Informační technologie
Současná úroveň a kvalita výzkumu v ČR:	**3,8**	Kvalita a úroveň výzkumu ICT pro ochranu KI odpovídá potřebám a postavení České republiky v západoevropském prostoru. Kvalita lidských zdrojů a úroveň vzdělávání vytváří předpoklady minimálně pro udržení dosavadní kvality výzkumu a jeho možné posunutí na absolutní světovou špičku v této oblasti. Jedním aspektem, který toto tvrzení dokládá je role českého vývoje a výzkumu v oblasti počítačového zabezpečení, kde české firmy dosahují významných hodnot podílu světového trhu. Vysokou dosažitelnost tohoto dílčího cíle dokládá relativně nízká finanční náročnost dosažení tohoto cíle, která plyne z faktu, že se jedná o vývoj a výzkum převážně v oblasti software, kde vybavení nutné pro tento vývoj a výzkum již existuje, nebo je možné ho pořídit jako počáteční jednorázovou investici. Absorpční kapacita aplikační sféry je vysoká, protože tento dílčí cíl naplňuje aktuální potřeby společnosti a potřeby společnosti předpokládané pro středně a dlouhodobý horizont. Tyto potřeby společnosti vytvářejí velký prostor a potenciál pro další rozvoj a růst podnikání v této oblasti na národní i na globální úrovni. Výsledky hlasování panelu expertů jsou zcela v souladu s těmito závěry a činí z dílčího cíle 2.1.5 jeden z nejdůležitějších a nejperspektivnějších oborů v bezpečnostní oblasti.
Úroveň výzkumné infrastruktury:	**3,7**	
Podpora ve státní politice a regulaci:	**3,2**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,1**	
Očekávaná finanční náročnost dosažení cíle:	**2,8**	
Absorpční kapacita aplikační sféry:	**4,0**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.2 Komunikace a vazby mezi kritickými infrastrukturami
Stěžejní cíl:	Vytvoření informační podpory a nástrojů, které umožní modelování vzájemných závislostí a interakcí nejdůležitějších systémů kritické infrastruktury. Dosažení včasnější detekce hrozeb plynoucích ze vzájemných vazeb a závislostí, přesnější a rychlejší predikce vývoje chování systémů infrastruktur a nasazení regulačních mechanismů, které minimalizují pravděpodobnost eskalace krizové situace a případného celkového kolapsu komunity s dlouhodobými následky.

Název dílčího cíle:	**2.2.1 Vzájemné závislostí systémů KI**	**2020**
Popis dílčího cíle:	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. *Charakteristika:* *Prevence disfunkce a rychlost obnovy funkce subjektů KI podmiňují úspěšnost uspokojení základních potřeb společnosti. Zabezpečení obnovy vyžaduje využití mnoha různých technických, správních a koordinačních činností prostupujících napříč systémy řízení zapojených subjektů. Činnosti jednotlivých subjektů KI jsou mezi sebou navzájem propojeny technologickými a organizačními návaznostmi. Sledování všech aspektů prolínajících se systémem a udržování kurzu směrem k zabezpečení obnovy je velice obtížné.* *Charakteristika a funkčnost jednotlivých složek/subjektů KI je popisována v plánech krizové připravenosti. Funkčnost jednotlivých systémů se opírá o šetření relativně rozsáhlou paletou rozdílných analytických nástrojů. Funkčnost KI jako celku je však závislá i na vzájemných procesních vazbách napříč systémy.* *Na KI a její evoluční vývoj působí systémy jednotlivých složek. Systém KI vnější podněty buď absorbuje, nebo neabsorbuje, v druhém případě buď vznikne nová struktura, nebo původní systém zaniká. Vzniká tak kladný/záporný dominoefekt, který v případě negativního průběhu, je vždy nežádoucí. V krátkém časovém horizontu totiž velice rychle dochází ke zkáze energetických, materiálových a informačních toků a sítí, k ničení společenské a technické infrastruktury, technologických celků, dopravních prostředků a komunikací, k poškození až kritickému zhoršení životních podmínek pro stávající formy botanického a zoologického původu.* *Opodstatněnost:* *Současný stav neumožňuje zhodnotit ohrožení a rizika vyplývající z interakcí mezi prvky KI, takže může dojít k nepředvídaným situacím, jejichž další průběh bude velmi obtížné jak predikovat, tak řídit požadovaným způsobem k obnově. Proto je třeba závislosti najít, dosáhnout jejich porozumění a vytvořit nástroje k jejich ošetření.* *Přínos:* *Výzkum zaměřený na rozvoj analytických nástrojů hodnotících synergii systémů jednotlivých subjektů směřujících k porozumění domino efektům a dalším interakcím je nezbytný. Jednou z nejdůležitějších aplikačních oblastí využití výzkumného potenciálu je možnost zkoumat dynamické procesy založené na adekvátním matematickém popisu a zvýšit kvalitativní úroveň predikce chování celého systému a možností jeho řízení v krizových situacích. To dává předpoklady nejen pro zlepšení kvality řízení procesních scénářů chování subsystémů (včetně chování v mimořádných situacích), ale i na kvalitativní zlepšení predikce a možnosti ovlivňování nežádoucího průběhu dominoefektu a odezvy celého systému. Jedná se tak o vývoj řízení systému směřující k vyšší odolnosti.*	

	Definice cíle: *Diskutovaný dílčí cíl se tématicky zaměřuje na poznání, rozbor a vyhodnocení odolnosti systému KI proti působení vnitřních i vnějších negativních vlivů. Výzkumný potenciál se zaměří na rozvoj analýz a modelování vzájemných závislostí systémů jednotlivých subjektů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. Analýzy spolehlivosti, funkčnosti a odolnosti zatížené interaktivními procesy probíhajícími mezi vzájemně propojenými subjekty KI musí směřovat k minimalizaci vzniku dominoefektů destruujících možnost obnovy. Aktualizované, rozvíjené či vyvíjené analytické nástroje musí reflektovat aktuální vývoj a změny ve vzájemných vazbách systémů KI.*

Vazba na ostatní dílčí cíle:

Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů	Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.3: Zajištění a rozvoj interoperability KI	Tvorba nástrojů pro zajištění a rozvoj interoperability KI (dopravní, energetické a dalších) s nadnárodními evropskými KI. Vazba na nadnárodní evropské síťové systémy (TEN-T, TEN-E). Modelování a výpočty sítí.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování	Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Vývoj systémů predikce a včasného varování.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami

Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.2.2: Podpora specifických oblastí bezpečnosti	Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Dílčí cíl 3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení	Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.3.4: Zdokonalení systémů pro podporu obnovy	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.4.1: Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací	Analyzovat a vytvářet legislativní postupy a opatření tak, aby legislativní rámec vytvářet komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,2**	Dílčí cíl lze považovat za velmi významný a svým způsobem zastřešující a propojující další dílčí cíle (viz výše). Nefunkčnost nebo nežádoucí odezva jednoho prvku kritické infrastruktury může způsobit kolaps dalších KI a dopady kombinovaného výpadku více infrastruktur by pro stabilitu společnosti mohly být velmi dramatické. Proto také bylo tomuto aspektu přiřazeno vysoké bodové ohodnocení. Je evidentní, že narušení funkce jedné z kritických infrastruktur je ohrožením bezpečnosti občanů a funkce společnosti, avšak současné narušení funkcí více infrastruktur bude působit synergicky a negativní efekty budou mnohem větší než prostý součet jednotlivých událostí. Stejný význam jako pro bezpečnost občanů a společnosti má navrhovaný dílčí cíl také pro obranyschopnost státu.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,3**	
Významnost cíle pro obranu státu:	**3,5**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Udržitelný rozvoj 3) Informační technologie
Současná úroveň a kvalita výzkumu v ČR: 3,4 **Úroveň výzkumné infrastruktury: 3,3** **Podpora ve státní politice a regulaci: 3,0** **Kvalita lidských zdrojů a úroveň vzdělávání: 3,8** **Očekávaná finanční náročnost dosažení cíle: 3,0** **Absorpční kapacita aplikační sféry: 3,9**	Současnou úroveň a kvalitu výzkumu v ČR lze charakterizovat jako dostatečně kvalitní s dobrým potenciálem růstu, ale ještě nikoliv špičkovou. Totéž platí o úrovni výzkumné infrastruktury a kvalitě vzdělávání a lidských zdrojů. Za klíčové je možno považovat, že bude nezbytné zapojit ČR do evropského výzkumného prostoru. Současná podpora ve státní politice a regulaci je ve fázi transformace a z minulého, spíše pasivního stavu se již začala transformovat do proaktivní podoby. Výsledky výzkumu mohou být uplatněny a využity prakticky u všech subjektů a to nejen kritické infrastruktury. Pro ověření navrhovaných opatření bude vhodné realizovat pilotní projekty. Některé z nich mohou posunout dílčí cíl do oblasti vyšší finanční náročnosti díky nutnému procesu verifikace a validace vyvinutých analytických metod a nástrojů.

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	2 Bezpečnost kritických infrastruktur a zdrojů
Podoblast:	2.2 Komunikace a vazby mezi kritickými infrastrukturami
Stěžejní cíl:	Vytvoření informační podpory a nástrojů, které umožní modelování vzájemných závislostí a interakcí nejdůležitějších systémů kritické infrastruktury. Dosažení včasnější detekce hrozeb plynoucích ze vzájemných vazeb a závislostí, přesnější a rychlejší predikce vývoje chování systémů infrastruktur a nasazení regulačních mechanismů, které minimalizují pravděpodobnost eskalace krizové situace a případného celkového kolapsu komunity s dlouhodobými následky.

Název dílčího cíle:	**2.2.2 Informační podpora pro detekci možných nepříznivých ovlivňování**	**2020**
Popis dílčího cíle:	Zajištění Informační podpory subjektů krizového řízení pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI. Vývoj systémů predikce a včasného varování. *Prvky kritické infrastruktury nejsou na sobě nezávislé, ale tvoří spolu a ve vztahu ke společnosti vzájemně propojený komplex, zahrnující různé formy ovlivňování a zpětných vazeb. Některé z nich mohou být pozitivní, ale v mnoha případech hrozí nepříznivá vzájemná interakce. Typickou ukázkou jednoduché interakce je ohrožení dodávek vody či funkce komunikací při selhání energetické infrastruktury nebo ohrožení dodávek potravin při dlouhotrvajícím suchu, tyto interakce však mohou být mnohem složitější. Ačkoliv existuje a dále se rozvíjí systém monitoringu funkčnosti jednotlivých prvků KI s ohledem na detekci možných mimořádných stavů, bylo dosud jen málo pozornosti věnováno vzájemným interakcím mezi kritickými infrastrukturami a mezi KI a společností (komunitou).* *Tento dílčí cíl je zaměřen na zajištění informační podpory subjektů krizového řízení a celé společnosti pro detekci možných nepříznivých ovlivňování funkce KI v důsledku vzájemných závislostí systémů KI, pro modelování možností dalšího vývoje včetně chování KI v krizových stavech a pro vyhledávání efektivních nástrojů a metod prevence a zmírňování následků disfunkcí KI. Rozvíjeny by měly být hlavně tyto typy informační podpory:* • *Sběr a vyhodnocování dat o vzájemných vlivech kritických infrastruktur v nestandardních stavech; analýzy interakcí založené na statistických rozborech a případových studiích;* • *Vytváření map a databází možných interakcí KI;* • *Vytvoření a rozvíjení informační báze metod predikce a detekce mimořádných stavů, zahrnující také efektivní systém včasného varování, a to včetně analýz využitelnost;* • *Informační podpora pro rozhodovací proces v rámci krizovém řízení v případě vzniku krize vznikající interakcemi KI nebo tyto interakce zahrnující.*	

Vazba na ostatní dílčí cíle:		
Stěžejní cíl 2.1: Zajištění funkčnosti KI	Celý stěžejní cíl 2.1, zahrnující dílčí cíle • **Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů,** • **Dílčí cíl 2.1.2: Zvyšování odolnosti KI,** • **Dílčí cíl 2.1.3: Zajištění a rozvoj interoperability KI,** • **Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb,** • **Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI,** vytváří vazby na dílčí cíl 2.2.2, který bude pomáhat řešit případy zahrnující více než jednu KI.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých. *Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích způsobených selháním kritických infrastruktur ve vzájemné interakci.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Bezpečnost měst a obcí je závislá na reakcích společnosti na stresující faktory. Připravenost obyvatel a komunit na možné krize výrazně zvyšuje resilienci společnosti. V tomto cíli budou rozvíjeny také metody a nástroje připravenosti měst a obcí, ale i jednotlivců na krize způsobené selháním funkce více kritických infrastruktur. Výzkum bude obsahovat i možnosti poskytování informační podpory těmto subjektům.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.2.2: Podpora specifických oblastí bezpečnosti	Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků *V rámci rozvoje nástrojů k zajištění specifických oblastí bezpečnosti bude prováděn výzkum potřeb informační podpory v rámci interakcí mezi kritickými infrastrukturami a ostatními bezpečnostními aspekty s vazbou na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle bude nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, a potřeb informační podpory. Součástí bude i rozvoj informační podpory rozhodovacích modelů pro řešení protichůdných nároků a požadavků.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,0**	Tento dílčí cíl má vysokou významnost pro fungování infrastruktur, protože dobrá informační podpora poskytuje potenciál zabránit vzniku domino efektu mezi kritickými infrastrukturami v případě selhání některé z nich a umožní včasnou přípravu na případný krizový stav. Významná je také informační podpora rozhodování v případech složitých vazeb mezi kritickými infrastrukturami. Zvýšení odolnosti systému kritických infrastruktur se pozitivně promítá i do obranyschopnosti státu.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,1**	
Významnost cíle pro obranu státu:	**3,4**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Bezpečnostní vědy 2) Udržitelný rozvoj 3) Informační technologie
Současná úroveň a kvalita výzkumu v ČR:	**3,4**	Současná úroveň a kvalita výzkumu v ČR je na dobré úrovni, avšak s ohledem na řešení tohoto cíle schází výzkumné týmy i programy zaměřené na velmi širokou komplexní problematiku vazeb mezi infrastrukturami. Lidský potenciál i technické zázemí výzkumných organizací však dávají dobrou šanci tuto mezeru vyplnit a výzkum může být na velmi dobré úrovni, bude však třeba překonat resortní pohled a nahradit jej komplexním přístupem. Absorpční kapacita aplikační sféry je vysoká, finanční náročnost střední.
Úroveň výzkumné infrastruktury:	**3,7**	
Podpora ve státní politice a regulaci:	**3,1**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**	
Očekávaná finanční náročnost dosažení cíle:	**3,3**	
Absorpční kapacita aplikační sféry:	**3,9**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.1 Rozvoj bezpečnostní politiky státu a bezpečnostního sytému ČR
Stěžejní cíl:	Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídících a hodnotících dokumentů v oblasti bezpečnosti, které je nutno pravidelně aktualizovat v závislosti na vývoji bezpečnostního prostředí a v závislosti na strategických prioritách bezpečnostní politiky NATO a EU. Prioritou bezpečnostní politiky je zajištění připravenosti a akceschopnosti celého bezpečnostního systému ČR (zejména IZS a AČR) za krizových situací a krizových stavů a to jak samostatně, tak i v součinnosti se spojenci v NATO a EU, a dále při řešení mimořádných událostí, přírodních a antropogenních krizových situací. Bezpečnostní systém tak musí být připraven reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.

Název dílčího cíle:	**3.1.1 Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti**	**2030** (průběžně)
Popis dílčího cíle:	Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Bílá kniha o obraně, Koncepce zahraniční politiky, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda, ministerstva) a Parlament ČR (výbory) jak přistupovat k tomuto procesu.	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých. *Dílčí cíl se přímo promítá do zajišťování koncepčního rámce pro ochranu obyvatelstva.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR. *Dílčí cíl významně souvisí se zajišťováním akceschopnosti Integrovaného záchranného systému.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva

Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému). *Implementace dílčího cíle se bezprostředně promítá do efektivního fungování bezpečnostního systému ČR*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Realizace dílčího cíle se musí opírat na relevantní identifikaci klíčových trendů vývoje bezpečnostní situace ve střednědobém i dlouhodobém horizontu.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,0**	Kvalita zpracování strategických řídících a hodnotících dokumentů v oblasti bezpečnosti má značný význam pro praktickou implementaci bezpečnostní politiky České republiky. Bezprostředně se to bude promítat do fungování bezpečnostního systému ČR, zajištění obrany země, zajištění odpovídajícího právního rámce pro ochranu kritické infrastruktury a zajištění bezpečnosti občanů na celostátní, regionální i lokální úrovni. Závěry obsažené v těchto dokumentech mají zajišťovat, aby bezpečnostní politika ČR měla jasně definovaný dlouhodobější koncepční rámec navázaný na cíle a úkoly bezpečnostní politiky EU a NATO a nebyla ovlivňována, resp. měněna v důsledku krátkodobě působících vlivů. Zároveň ale musí být brána v potaz současná vysoká dynamika vývoje bezpečnostního prostředí, což bude klást vyšší nároky na analýzu plnění strategických řídících a hodnotících dokumentů v oblasti bezpečnosti. Z analýzy musí vyplynout i formulování doporučení a návrhů k jejich aktualizaci a k metodice zpracovávání.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,8**	
Významnost cíle pro obranu státu:	**4,1**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Veřejná politika 2) Bezpečnostní vědy 3) Strategická studia 4) Sociologie
Současná úroveň a kvalita výzkumu v ČR:	**3,6**	Výzkum v uvedené oblasti je v rámci ČR dosud řešen odpovídajícím způsobem i když v uvedené oblasti působí omezený počet relevantních výzkumných pracovišť. Určitým problémem je využitelnost výsledků výzkumu pro státní správu - z její strany je patrná určitá nárazovost poptávky po výstupech v návaznosti na konkrétní přípravu strategických řídících a hodnotících dokumentů v oblasti bezpečnosti.
Úroveň výzkumné infrastruktury:	**3,6**	
Podpora ve státní politice a regulaci:	**3,5**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,7**	
Očekávaná finanční náročnost dosažení cíle:	**3,1**	
Absorpční kapacita aplikační sféry:	**3,9**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.1 Rozvoj bezpečnostní politiky státu a bezpečnostního sytému ČR
Stěžejní cíl:	Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídících a hodnotících dokumentů v oblasti bezpečnosti, které je nutno pravidelně aktualizovat v závislosti na vývoji bezpečnostního prostředí a v závislosti na strategických prioritách bezpečnostní politiky NATO a EU. Prioritou bezpečnostní politiky je zajištění připravenosti a akceschopnosti celého bezpečnostního systému ČR (zejména IZS a AČR) za krizových situací a krizových stavů a to jak samostatně, tak i v součinnosti se spojenci v NATO a EU, a dále při řešení mimořádných událostí, přírodních a antropogenních krizových situací. Bezpečnostní systém tak musí být připraven reagovat na měnící se podmínky a změny v bezpečnostním prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.

Název dílčího cíle:	**3.1.2 Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby**	**2030** (průběžně)
Popis dílčího cíle:	Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR. *Pro realizaci dílčího cíle je to mimořádně důležité s ohledem na to, že při zdokonalování služeb a prostředků obrany má zásadní význam Integrovaný záchranný systém, jenž je také jádrem bezpečnostního systému*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.1.1: Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti	Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda) a Parlament ČR jak přistupovat k tomuto procesu. *Pro realizaci dílčího cíle je mimořádně důležitá úroveň a vyhodnocování strategických řídících dokumentů v oblasti bezpečnosti - přímo to ovlivňuje strukturu a efektivitu bezpečnostního systému.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. R*ealizace dílčího cíle se musí opírat o Identifikaci klíčových trendů vývoje bezpečnostní situace, což určuje i podobu bezpečnostního systému.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,0**	Nástrojem pro realizaci bezpečnostní politiky a její implementaci do života je bezpečnostní systém. Jeho parametry -jednotlivé prvky , jejich funkce a vztahy mezi nimi a vztahy bezpečnostního systému s jeho okolím -musejí odpovídat potřebě zajištění bezpečnosti v dynamicky se měnícím bezpečnostním prostředí. Úroveň fungování bezpečnostního systému, jeho adaptabilita a rozvoj se přímo promítá na zajištění fungování státu, zajištění jeho obrany a bezpečnosti občanů.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,8**	
Významnost cíle pro obranu státu:	**4,3**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		**1)** Prognostika 2) Strategická studia **3)** Bezpečnostní vědy
Současná úroveň a kvalita výzkumu v ČR:	**3,4**	Daná problematika je předmětem výzkumu jak ve státní správě (především HZS), tak i v akademické sféře (relevantních výzkumných pracovištích). Výzkum je řešen odpovídajícím způsobem, složitost dané problematiky ovšem vyžaduje užší propojení akademické sféry a státní správy (společné výzkumné projekty, týmy, apod.).
Úroveň výzkumné infrastruktury:	**3,7**	
Podpora ve státní politice a regulaci:	**3,3**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,8**	
Očekávaná finanční náročnost dosažení cíle:	**3,0**	
Absorpční kapacita aplikační sféry:	**3,9**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.2 Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Stěžejní cíl:	Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik v dlouhodobém horizontu (2020-2030), který funguje následujícím způsobem: Pravidelně se zpracovávají prognostické studie a scénáře vývoje bezpečnostní situace, které jsou předmětem expertního posuzování. Následně se vytváří soubor opatření pro eliminaci hrozeb podpořený i tvorbou (variantních) scénářů bezpečnostního vývoje. Závěry se promítají do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Název dílčího cíle:	**3.2.1 Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR**	**2030** (průběžně)
Popis dílčího cíle:	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků obrany	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR. *Výzkumné úkoly plněné v rámci dílčího cíle mohou být využity k identifikaci hrozeb a rizik souvisejících s ochranou obyvatelstva, majetku a životního prostředí a s přijímáním opatření k jejich eliminaci.*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.1.1: Vyhodnocení efektivity strategických řídících a hodnotících dokumentů v oblasti bezpečnosti	Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídících a hodnotících dokumentů v oblasti bezpečnosti (Bezpečnostní strategie, Obranná strategie, Zpráva o stavu zajištění bezpečnosti atd.), jejich vliv na implementaci bezpečnostní politiky a formulovat doporučení pro příslušné orgány státní správy (vláda) a Parlament ČR jak přistupovat k tomuto procesu. *Výsledky dílčího cíle se budou bezprostředně promítat do přípravy a tvorby strategických řídících a hodnotících dokumentů v oblasti bezpečnosti.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému). *Výsledky dílčího cíle budou mít vliv na proces zdokonalování a zpřesňování struktury, úkolů a cílů bezpečnostního systému.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Dílčí cíl 3.2.2: Podpora specifických oblastí bezpečnosti	Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků *Dílčí cíl je propojen s identifikováním obsahu a předpokládaných dopadů specifických oblastí bezpečnosti (environmentální, energetická, surovinová, potravinová, finanční).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,9**	Dynamika vývoje bezpečnostního prostředí vyžaduje zvýšit úroveň metod a nástrojů identifikace vývoje a trendů bezpečnostního vývoje ve světě, Evropě a ČR a to i prostřednictvím kontinuálně zpracovávaných prognostických studií a scénářů a promítnutí získaných poznatků/závěrů do tvorby(příprava strategických, řídících a hodnotících dokumentů v oblasti bezpečnosti) a realizace (implementace dokumentů v bezpečnostní politice na celostátním regionální i místní úrovni) bezpečnostní politiky.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,7**	
Významnost cíle pro obranu státu:	**4,2**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Prognostika 2) Ochrana obyvatelstva 3) Bezpečnostní vědy 4) Strategická studia
Současná úroveň a kvalita výzkumu v ČR:	**3,8**	Daná problematika je předmětem výzkumu především na akademické úrovni, jeho výstupy jsou ale využívány státní správou v rozdílné míře. Klíčovým faktorem pro zvýšení úrovně výzkumu je užší propojení kapacit státní správy a výzkumných akademických institucí (zajištění zpětné vazby) a kontinuální spolupráce (nikoliv nárazově pouze při přípravě strategických, řídících a hodnotících dokumentů v oblasti bezpečnosti).
Úroveň výzkumné infrastruktury:	**3,9**	
Podpora ve státní politice a regulaci:	**3,4**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,8**	
Očekávaná finanční náročnost dosažení cíle:	**3,2**	
Absorpční kapacita aplikační sféry:	**3,9**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.2 Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření
Stěžejní cíl:	Vytvoření mechanismu vyhledávání a identifikace bezpečnostních hrozeb a rizik v dlouhodobém horizontu (2020-2030), který funguje následujícím způsobem: Pravidelně se zpracovávají prognostické studie a scénáře vývoje bezpečnostní situace, které jsou předmětem expertního posuzování. Následně se vytváří soubor opatření pro eliminaci hrozeb podpořený i tvorbou (variantních) scénářů bezpečnostního vývoje. Závěry se promítají do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.

Název dílčího cíle:	**3.2.2 Podpora specifických oblastí bezpečnosti**	**2020**
Popis dílčího cíle:	Cílem je vytvoření a rozvoj nástrojů k zajištění specifických oblastí bezpečnosti s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné vypracovat modely vzniku možných krizí, vytvořit systém indikátorů, preventivních a mitigačních nástrojů a vzájemných interakcí. Tvorba rozhodovacích modelů pro řešení protichůdných nároků a požadavků. *Velká část cílů výzkumu v oblasti bezpečnosti je zaměřena na konkrétní rizika s rychlou dynamikou a vedoucí víceméně bezprostředně ke vzniku krize. Významné bezpečnostní problémy se však mohou vyvíjet zvolna a svým charakterem pak nezahrnují jen krizové řízení, ale také celkovou stabilitu společnosti a dlouhodobý, stabilní a nepřerušovaný přístup ke zdrojům včetně zdrojů obnovitelných. Stejně tak existuje řada oblastí bezpečnosti, které nespadají jednoznačně do jednotlivého prioritního cíle, avšak jsou z hlediska celkové bezpečnosti významné. Pro bezpečnost a stabilitu společnosti jsou důležité i prvky veřejného zdraví a kvality života a zde je prostor pro spolupráci s výzkumem připravovaným v rámci jiných panelů.* *Cílem podpory specifických oblastí bezpečnosti je rozvoj poznání zaměřený cíleně na bezpečnostní aspekty v těchto oblastech, dále pak vytvoření a rozvoj metod a nástrojů prevence a ochrany s důrazem na environmentální, energetickou, surovinovou, potravinovou a finanční bezpečnost v kontextu udržitelného rozvoje a pro zajištění stability společnosti a dlouhodobé bezpečnosti obyvatel. K dosažení tohoto cíle je nezbytné provést relevantní analýzy vztahů a vazeb uvnitř těchto specifických oblastí a mezi nimi a vypracovat modely vzniku možných krizí včetně modelů zahrnujících dlouhodobé změny a jejich dopady. Dále je cílem vytvořit systém dlouhodobých indikátorů nežádoucího vývoje a krátkodobých indikátorů blížící se krize, systém preventivních a mitigačních nástrojů a zahrnutí vzájemných interakcí do vytvářených systémů. Dalším cílem je vytvoření modelů pro řešení protichůdných nároků a požadavků a nástrojů pro podporu rozhodovacích procesů ve všech fázích vývoje bezpečnostních situací, tedy od prevence negativního vývoje přes zmírňování krize až po optimalizaci nápravných opatření ve fázi po skončení krize.*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability (předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného	**Oblast** 1: Bezpečnost občanů **Podoblast** 1.1: Ochrana obyvatelstva

	systému a civilního nouzového plánování. *Dílčí cíl 1.1.3 zahrnuje také bezpečnostní aspekty identifikované v rámci dílčího cíle 3.2.2 jako prioritní. Znalostní báze z dílčího cíle 3.2.2 bude využita ke zvýšení a informovanosti občanů o rizicích ve specifických oblastech bezpečnosti (environmentální, energetická, surovinová, potravinová a finanční bezpečnost) a o možnostech jejich prevence a zvládání a ke zvýšení připravenosti měst, obcí i jednotlivců na možné bezpečnostní hrozby.*	
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Cílem je zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému). *Dílčí cíl 3.2.2 má charakter spíše analytický, poznávací a přípravný, a výstupy z něj budou zařazeny do realizace dílčího cíle 3.1.2 tak, aby specifické oblasti bezpečnosti (environmentální, energetická, surovinová, potravinová a finanční bezpečnost) byly efektivně zahrnuty do podpory adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby*	**Oblast** 3: Krizové řízení a bezpečnostní politika **Podoblast** 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti. *Výzkum v rámci dílčího cíle 3.2.1 bude využívat výstupy z dílčího cíle 3.2.2 jako jeden ze vstupů.*	**Oblast** 3: Krizové řízení a bezpečnostní politika **Podoblast** 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,1**	Dílčí cíl má vysokou významnost pro fungování státu a infrastruktur a tato významnost se odvíjí mimo jiné z toho, že dílčí cíl zahrnuje posouzení jak krátkodobých, tak střednědobých a dlouhodobých aspektů bezpečnosti v hraničních oblastech, kde by jinak mohly hrozby a rizika a jejich vývoj být podceněny. Důležitý je také interdisciplinární přístup a vazby s ostatními výzkumnými směry, včetně vazeb mimo úzkou oblast bezpečnosti. Významnost cíle pro bezpečnost občanů a pro bezpečnost občanské společnosti vyplývá z významnosti pro fungování státu a infrastruktur; individuální bezpečnost také závisí na přístupu jedinců a komunity v jeho blízkosti ke zdrojům a na stabilitě společnosti jako celku. Významnost cíle pro obranu státu je také vysoká a souvisí nejen s vnitřní bezpečností související se specifickými aspekty environmentální, energetické, surovinové, potravinové a finanční bezpečnosti, ale také s mezinárodní stabilitou, konflikty a migračními vlnami odvíjejícími se od těchto bezpečnostních aspektů
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,5**	
Významnost cíle pro obranu státu:	**3,5**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Mezioborové transdisciplinární interakce s možnými negativní účinky 3) Nové přístupy k soběstačnosti ČR ve zdrojích energie, vody a v potravinách

Současná úroveň a kvalita výzkumu v ČR:	**3,1**
Úroveň výzkumné infrastruktury:	**3,2**
Podpora ve státní politice a regulaci:	**2,6**

Kvalita lidských zdrojů a úroveň vzdělávání:	**3,7**	kvalitě lidských zdrojů a úrovni vzdělávání. Cíl patří mezi méně finančně náročné, kapacita aplikační sféry je relativně vysoká.
Očekávaná finanční náročnost dosažení cíle:	**3,4**	
Absorpční kapacita aplikační sféry:	**3,7**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.3 Systémy analýzy, prevence, odezvy a obnovy
Stěžejní cíl:	Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Název dílčího cíle:	**3.3.1 Zlepšení systémů získávání a třídění bezpečnostních informací**	**2020**
Popis dílčího cíle:	Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací	Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům. *Metody a techniky boje s kybernetickou kriminalitou velmi úzce souvisejí i se schopností včasného rozpoznání hrozeb, jejich analýzy, prevence – a v případě nutnosti i účinného zotavení. Velmi důležitá je v této oblasti mezinárodní spolupráce s bezpečnostními složkami jiných států*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem
Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb ,	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness). *Systémy analýzy, prevence, odezvy a obnovy mohou výraznou měrou pomoci při ochraně KI*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. *Systémy analýzy, prevence, odezvy a obnovy mohou výraznou měrou pomoci při ochraně KI*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

Dílčí cíl 3.3.2: Analýza bezpečnostních informací	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. *Systému pro získávání a třídění bezpečnostních informací jsou těsně provázány s metodami a technikami pro jejich zpracování a analýzu. Vzhledem ke globálnímu charakteru hrozeb je pak naprosto klíčová i mezinárodní spolupráce*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,8**	Vzhledem k neustále se zdokonalujícím technikám kybernetických a jiných forem útoků a jejich rostoucí globalizaci je pro ochranu kritických infrastruktur, ale obecně všech systemů naprosto zásadní předcházení hrozbám, případně jejich včasné rozpoznání. To je nemyslitelné bez dostatečného rozvoje systémů pro získávání a třídění bezpečnostních informací a – vzhledem ke globálnímu charakteru útoků – také bez dostatečně účinné mezinárodní spolupráce. Tato problematika je velmi důležitá i z hlediska branně-bezpečnostního, obranné zpravodajství může být jedním z hlavních odběratelů výsledků výzkumu v této oblasti.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,2**	
Významnost cíle pro obranu státu:	**3,7**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Informační technologie 2) Technická kybernetika 3) Manažerské systémy řízení
Současná úroveň a kvalita výzkumu v ČR:	**3,5**	Současná úroveň především aplikačního výzkumu v České republice je na poměrně vysoké úrovni, mimo jiné díky několika firmám, které v této oblasti patří ke světové špičce. Také základní výzkum je zejména v některých oblastech (např. zpracování řeči) na poměrně dobré úrovni. S tím souvisí i velmi dobrá personální základna. Přesto je pro udržení kroku s bezpečnostními hrozbami a pro úspěšný boj s kybernetickou kriminalitou nutné dále do výzkumu v této oblasti investovat, jak v oblasti základního, tak i aplikačního výzkumu. Očekávaná absorpční kapacita aplikační sféry je vysoká, jen minimálně ovlivněna možnou úzkou orientací některých výzkumných projektů na branně-bezpečnostní problematiku
Úroveň výzkumné infrastruktury:	**3,5**	
Podpora ve státní politice a regulaci:	**2,9**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,9**	
Očekávaná finanční náročnost dosažení cíle:	**3,0**	
Absorpční kapacita aplikační sféry:	**3,8**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.3 Systémy analýzy, prevence, odezvy a obnovy
Stěžejní cíl:	Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Název dílčího cíle:	**3.3.2 Analýza bezpečnostních informací**	**2020**
Popis dílčího cíle:	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč) pomocí data mining, knowledge engineering, odvozování znalostí (reasoning) a strojového učení (machine learning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. *Vyvinuté metody budou aplikovatelné na informace získávané v rámci boje proti konvenční a organizované kriminalitě ve všech oblastech a terorismu. Bude se vztahovat i na informace získávané v rámci mezinárodní bezpečnostní a vojenské spolupráce. Vytvořené metody budou zaměřeny jak na operativní využití získaných informací (vyšetřování, prevence bezprostředně hrozícího nebezpečí), tak na dlouhodobé využití (prevence do budoucna, plánování, sledování, podpora rozhodovacích procesů).* *Stěžejní pro splnění tohoto cíle je využití výzkumných výsledků v oblasti moderních ICT technologií (za pomoci fundamentálních matematických, statistických a lingvistických metod a metod umělé inteligence) pro zpracování informací v klíčových modalitách a jejich kombinace pro bezpečnostní účely. Předpokládá se, že analyzované informace budou přicházet jak z otevřených, tak utajovaných zdrojů v různé kvantitě a kvalitě. Řešení musí tedy zahrnovat také třídění a prioritizaci analyzovaných informací z hlediska přesnosti a relevance (snížení objemu práce analytiků, nalezení obtížně dohledatelných souvislostí). Důležitou součástí řešení bude rovněž adekvátnost a škálovatelnost implementace vyvinutých metod a algoritmů z časového hlediska s ohledem na danou aplikaci (práce v reálném čase pro operativní účely, naopak možnost zvýšení přesnosti na úkor času při plnění dlouhodobých informačních cílů).*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací	Cílem je vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům. *Dílčí cíl 1.2.2 se podobně jako cíl 2.1.6 zabývá kybernetickou kriminalitou; cíl 3.3.2 je širší, zabývá se analýzou informací, které mohou vést k odhalení kriminálního činu jakéhokoli druhu nebo k prevenci takových činů. Oba cíle sdílejí pouze metody (ICT).*	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem
Dílčí cíl 2.1.4: Účinná detekce a identifikace hrozeb	Předpovědi a scénáře možného vývoje hrozeb (a jejich dynamiky) z pohledu funkčnosti KI. Metody a postupy vyhodnocování zranitelnosti a odolnosti (dostatečnosti stávající ochrany a zabezpečení funkce) systémů KI. Účinná detekce a identifikace možných nebezpečí a interpretace	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

	informací pro ustanovení situačního přehledu (situation awareness). *Cíl 2.1.4 se zabývá detekcí a identifikací hrozeb proti kritickým infrastrukturám. S cílem 3.3.2. sdílí důraz na odhalení možných útoků (prevenci) a jejich identifikaci. Cíl 3.3.2 se přitom do hloubky zaměřuje na analýzu informací (avšak pro veškeré bezpečnostní účely, nejen pro ochranu KI), zatímco cíl 2.1.4 řeší tuto otázku na obecné rovině.*	
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií. *Informační technologie zabezpečení KI, které jsou zadáním cíle 2.1.5 budou i součástí systémů analýzy informací cíle 3.3.2 týkajících se KI.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací	Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů. *V rámci podoblasti 3.3 spolu první tři dílčí cíle úzce souvisí. Zatímco zde popisovaný dílčí cíl 3.3.2 je zaměřen primárně na analýzu informací dostupných v elektronické formě metodami ICT, způsob získávání a (před)třídění těchto informací je součástí cíle 3.3.1, a oba tyto cíle pak ovlivňují nastavení bezpečnostního systému a systému krizového řízení jako celku (dílčí cíl 3.3.3).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy
Dílčí cíl 3.3.3: Zdokonalování účinnosti bezpečnostního systému a krizového řízení	Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti. *V rámci podoblasti 3.3 spolu první tři dílčí cíle úzce souvisí. Zatímco zde popisovaný dílčí cíl 3.3.2 je zaměřen primárně na analýzu informací dostupných v elektronické formě metodami ICT, způsob získávání a (před)třídění těchto informací je součástí cíle 3.3.1, a oba tyto cíle pak ovlivňují nastavení bezpečnostního systému a systému krizového řízení jako celku (dílčí cíl 3.3.3).*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,8**	Informace jsou v 21. století kriticky důležitou složkou každého rozhodovacího procesu, a tím více je jejich včasná dostupnost klíčová pro veškeré aspekty bezpečnosti občanů, kritických infrastruktur i obrany. Při množství informací všech typů a modalit je naprosto nezbytné mít prostředky pro jejich analýzu a třídění z hlediska relevance pro bezpečnost. Stejně tak důležité je i nalezení souvislostí mezi těmito relevantními informacemi, ze kterých lze vyvodit podstatné a nové informace; často teprve kombinace informací z různých zdrojů a modalit umožní dojít k relevantním závěrům. V této oblasti přitom již nelze spoléhat jen na lidskou sílu (tj. analytiky, manažery, vyšetřovatele, státní správu), je třeba pro ně zajistit technologickou podporu (ICT) na nejvyšší možné úrovni pomocí matematických, statistických a jazykově-analytických metod a postupů, implementovaných v systémech prevence, operativy a řešení následků na administrativní i technologické rovině.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,4**	
Významnost cíle pro obranu státu:	**3,6**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Informační technologie 2) Technická kybernetika 3) Jazykověda 4) Matematika 5) Umělá inteligence
Současná úroveň a kvalita výzkumu v ČR: 4,0 **Úroveň výzkumné infrastruktury: 3,7** **Podpora ve státní politice a regulaci: 2,9** **Kvalita lidských zdrojů a úroveň vzdělávání: 4,1** **Očekávaná finanční náročnost dosažení cíle: 3,1** **Absorpční kapacita aplikační sféry: 3,9**	Výzkum a vývoj v uvedených relevantních oblastech je v ČR na vysoké úrovni (i z mezinárodního hlediska). Výzkum je prováděn na několika vysokých školách (ČVUT, UK, ZČU, VUT, MU, TUL), pracovištích AV ČR (ÚI, ÚTIA) i firmách (např. Retia, SpeechTek, Phonexia, CaptaWorks). Výzkum v oblasti ICT a dalších vyjmenovaných oborech má relativně dobrou infrastrukturu (internet / CESNET, instalovaná výpočetní síla) a mezinárodní zkušenosti a kontakty, nicméně je třeba ji posílit (v tomto směru bude přínosem vybudování HPC centra IT4U v Ostravě) a rovněž posílit mezinárodní zapojení do projektů, jako je PRACE (vysokokapacitní HPC) nebo EUDAT (datová infrastruktura pro vědecké a výzkumné výpočty). Lidský potenciál a úroveň vzdělávání je rovněž na vysoké úrovni, od škol s bakalářskými obory pro základních potřeby znalosti ICT technologií po špičková pracoviště v uvedených oborech, která průběžně připravují magistry a doktorandy na práci v těchto oborech a jejich kombinacích. Finanční náročnost je kromě průběžných investic do obnovy výpočetní a síťové infrastruktury průměrná, neboť se jedná převážně o mzdové náklady při vývoji softwarových prostředků a systémů. ICT a vyjmenované související obory a technologie jsou přitom nezbytným předpokladem rozvoje společnosti i v dalších oblastech života, a specificky zaměření dílčího cíle 3.3.2 odpovídá potřebám mnoha odvětví hospodářství a státní správy v dnešní „znalostní společnosti“. Řešení tohoto cíle tedy bude mít pozitivní vliv na ekonomiku i mimo bezpečnostní oblast a oblast obrany, jak tomu již mnohokrát v minulosti bylo.

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.3 Systémy analýzy, prevence, odezvy a obnovy
Stěžejní cíl:	Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Název dílčího cíle:	**3.3.3 Zdokonalování účinnosti bezpečnostního systému a krizového řízení**	**2030** (průběžně)
Popis dílčího cíle:	Průběžná analýza informačních potřeb. Nastavení rozhodovacích a informačních procesů a zodpovědností všech složek. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému, analýza průběhu krizových situací, hodnocení dopadů dostupnosti informací. Opatření pro odstranění nedostatků a zvýšení odolnosti informačního systému v technologické i organizační oblasti. *Cílem je optimalizace rozhodovacích a informačních procesů a zodpovědností všech složek směřující k zavedení manažerského způsobu řízení ve dvou základních úrovních – strategické a operační. Strategická úroveň řízení zajišťování bezpečnosti státu má za úkol trvale vytvářet komplexní podmínky pro včasné vytváření a udržování adekvátních nezbytných bezpečnostních schopností v rámci bezpečnostního systému státu. Operační úroveň řízení zajišťování bezpečnosti státu má za úkol trvale vytvářet komplexní podmínky pro včasné účelné a efektivní nasazení existujících bezpečnostních schopností v rámci bezpečnostního systému státu k eliminaci bezpečnostních rizik – tj. zajistit efektivní fungování krizového systému státu.* *K naplnění dílčího cíle je třeba provést zejména následující kroky a činnosti: Vytváření manažerského informačního systému pro podporu rozhodování v rámci bezpečnostního systému státu. Průběžná analýza informačních potřeb. Zabezpečení informačních toků při prevenci i v krizových situacích. Propojení technologií a rozhodovacích procesů státní správy. Návaznost informačního systému na složky krizového řízení. Analýza účinnosti preventivních opatření vzhledem k informačnímu systému. Analýza průběhu krizových situací, Hodnocení dopadů dostupnosti informací. Formulace opatření pro odstranění nedostatků. Zvýšení odolnosti informačního systému v technologické i organizační oblasti. Vytváření interního normativního rámce pro činnost bezpečnostního systému státu. Monitoring aktuálního stavu bezpečnostního systému státu.*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací	Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce, interoperabilita. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

	Bez relevantních informací, poskytovaných v dostatečné kvalitě i kvantitě, nelze smysluplně naplnit cíle zdokonalení účinnosti bezpečnostního systému a krizového řízení.	
Dílčí cíl 3.3.2: Analýza bezpečnostních informací	Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning). Hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu. Identifikace vhodných příjemců analyzovaných a agregovaných výstupů. *Naplnění dílčího cíle zdokonalení účinnosti bezpečnostního systému a krizového řízení výrazně usnadní vývoj nových metod analýzy informací bezpečnostního charakteru, a hodnocení aktuálnosti a relevance informací a to i v mezinárodním kontextu.*	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.3:** Systémy analýzy, prevence, odezvy a obnovy

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,6**	Výsledky hlasování členů panelu potvrdily předpokládanou relativně vysokou významnost dílčího cíle pro fungování státu a kritických infrastruktur, na kterých úzce závisí bezpečnost občanů a bez nichž lze v dnešní době jen těžko realizovat obranu státu jako takovou. Ačkoliv lze konstatovat, že IZS v ČR je v současnosti na relativně dobré úrovni, je třeba zajistit, aby nedošlo k zhoršení tohoto stavu vlivem nedostatečného zdrojového zabezpečení, nedostatečné reflexe neustálého vývoje bezpečnostních hrozeb a pokroku ve vývoji nových technologií. Při řízení bezpečnostního systému navíc není doposud v ČR uplatňován manažerský způsob řízení v obou základních úrovních – strategické a operační. Dílčí cíl je proto klíčový pro zajištění optimálního fungování Integrovaného záchranného systému ČR a jeho jednotlivých složek, stejně jako pro optimalizaci řídících a informačních procesů nutných pro zajištění managementu bezpečnosti jako celku. Protože v současné době není ČR sama schopna zajistit svoji obranu a bezpečnost svých občanů, je tento dílčí cíl důležitý i z hlediska mezinárodní spolupráce v případě krizových událostí v ČR. Zároveň také přispěje k tomu, aby ČR byla spojencem schopným nabídnout účinnou pomoc při krizových událostech mimo naše území.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**3,2**	
Významnost cíle pro obranu státu:	**3,7**	

Dosažitelnost dílčího cíle		
Související obory výzkumu a vývoje:		1) Ekonomika 2) Manažerské systémy řízení 3) Informační technologie
Současná úroveň a kvalita výzkumu v ČR:	**3,1**	Z výsledků hlasování členů panelu vyplývá, že současná úroveň výzkumu a výzkumné infrastruktury potřebná k naplnění tohoto dílčího cíle je spíše průměrná, což může být i důsledkem v současnosti pouze průměrné podpory ve státní politice. Kvalitu lidských zdrojů naopak členové panelu považují za relativně dobrou, což je důležitým předpokladem k úspěšnému naplnění tohoto dílčího cíle. Podobně pozitivně byla hodnocena i absorpční kapacita aplikační sféry, což je dalším signálem o naplnitelnosti a důležitosti dílčího cíle.
Úroveň výzkumné infrastruktury:	**3,2**	
Podpora ve státní politice a regulaci:	**2,8**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,6**	
Očekávaná finanční náročnost dosažení cíle:	**3,1**	
Absorpční kapacita aplikační sféry:	**3,5**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.3 Systémy analýzy, prevence, odezvy a obnovy
Stěžejní cíl:	Pro odvrácení bezpečnostních hrozeb ve všech oblastech (kriminalita včetně organizované, terorismus, bezpečnost a ochrana životů a zdraví, předcházení následkům živelních a přírodních katastrof, související zdravotní problematika, ochrana infrastruktur) je nutné zajistit vysokou úroveň znalostí a informací dlouhodobého i operativního charakteru. Stejně tak je třeba držet krok s moderními informačními a znalostními technologiemi i v oblasti zásahové, nouzového režimu a odstraňování následků, pokud k nežádoucí situaci dojde. Předpokládá se zapojení všech složek bezpečnosti a ochrany (policie, státní správa na všech úrovních, ZZS, HZS, BIS, ozbrojené síly). Relevantní technologie musí odpovídat standardům, případně nezbytným certifikacím, a být interoperabilní v rámci závazků ČR v EU a NATO.

Název dílčího cíle:	**3.3.4 Zdokonalení systémů pro podporu obnovy**	**2030** (průběžně)
Popis dílčího cíle:	Analýza potřeb při krátkodobé i dlouhodobé obnově škod z mimořádných situací a krizových stavů. Komplexní informační a infrastrukturní podpora obnovy. *Kategorie „obnovy" je chápána v širším a užším slova smyslu. Obecně a v širším slova smyslu jde o „zajištění návratu posuzovaného systému do stabilizovaného stavu a o iniciování dalšího rozvoje v rozumném čase a za přijatelných nákladů". Takto chápaný koncept obnovy nerozlišuje příčinu nerovnováhy, která může být přírodního (např. pohroma typu povodně, zemětřesení aj.), nebo antropogenního původu (např. technologická havárie, teroristický útok apod.). V užším slova smyslu jde o obnovu blíže specifikovaných systémů, které jsou výrazně horizontálně a vertikálně diferencovány (např. obnova majetku různé povahy, obnova informačních systémů, obnova infrastruktury v územním regionu, obnova provozu obchodních společností nebo průmyslových podniků apod.).* *Z hlediska rozvoje je třeba obnovu nechápat jen jako prostou obnovu poškozeného majetku a rozvrácených funkcí, ale je ji třeba dělat podle scénáře takového, aby v budoucnu dopady stejně silné pohromy byly menší. Proto je třeba vycházet z hodnocení ohrožení od pohromy, analýzy rizik a přihlížet k požadavkům udržitelného rozvoje a principu předběžné opatrnosti – tj. používat nástroj řízení bezpečnosti.* *Cílem by proto měla být kvalitní příprava scénáře obnovy po pohromách velkého rozsahu, jehož cílem je minimalizace času na návrat k normálnímu stavu a minimalizace škod.* *Důležitým prvkem scénáře obnovy je propojenost opatření ve všech oblastech postižených pohromou, společné postupy při návratu kritických infrastruktur a technologií do provozu,* *Scénář obnovy navazuje na scénář obrany proti nekontrolovatelnému šíření pohrom a krizových stavů . Tento scénář musí být pravidelně aktualizován , aby odpovídal vždy současnému platnému systému. (V souladu s evropskou legislativou jsou takové scénáře zpracovány a ročně aktualizovány pro přenosovou soustavu –Plán proti šíření velkých systémových poruch - Defence plan a Plán obnovy provozu přenosové soustavy po velké systémové poruše - Plan of the restoration. Tyto plány byly jednou z podmínek pro připojení soustavy ČR do evropské elektrizační soustavy v roce 1996.).*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a	Rozvíjet a zdokonalovat metodiky a postupy směřující ke zvyšování úrovně procesního řízení při mimořádných a krizových situacích; zvyšování úrovně bezpečnosti měst a obcí, mechanismů a civilního nouzového plánování v rámci bezpečnosti státu, regionu, obce, podniku, objektu, organizace apod. v dynamicky proměnném okolí s cílem systematického zajišťování stability	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva

motivace občanů	(předcházení krizím) a vytváření podmínek pro další rozvoj; zvyšování úrovně připravenosti orgánů státní správy a samosprávy; nové formy výchovy a vzdělávání v oblasti ochrany obyvatelstva, integrovaného záchranného systému a civilního nouzového plánování. *Zdokonalení systémů pro podporu obnovy vede ke zvyšování integrální bezpečnosti a udržitelného rozvoje lidského systému a jeho chráněných zájmů: životy, zdraví a bezpečí lidí; majetek a veřejné blaho; životní prostředí; infrastruktura a technologie.*	
Dílčí cíl 2.1.1: Rozvoj alternativních a nouzových krizových procesů	Rozvoj alternativních nouzových a krizových procesů umožňujících nezbytnou úroveň provozu i při nefunkčnosti nadřazených soustav KI (např. vytváření dynamických ostrovních systémů, schopnost startu funkce KI „ze tmy“). Podpora zajištění nezbytné funkčnosti (Minimum Service Level) KI v případě stavu nouze a kritických situací. Zajišťování diverzifikace vzhledem ke zdrojům a kontinuity vzhledem k uživatelům služeb KI. *Zdokonalení systémů pro podporu obnovy souvisí úzce se zajištěním o kontinuity provozu kritické infrastruktury a kritických technologií v území.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.1.2: Zvyšování odolnosti KI	Rozvoj metodik a aplikačních postupů rizikových analýz (stanovení relevantních hrozeb, analýza a kvantifikace rizik), metodik a aplikačních postupů navrhování a výběru preventivních opatření (včetně analýzy nákladů a užitků) k odvrácení hrozeb pro jednotlivé druhy kritické infrastruktury, ke zvyšování ochrany a odolnosti KI. Metody a nástroje pro modelování (simulace) rizik, zranitelnosti a scénářů dopadů. *Souvislost odolnosti KI a obnovy je zcela zásadní. Reálný život může překonat předpokládané bezpečnostní bariéry. O to důležitější je poučení z pohrom a z hlediska rozvoje je třeba obnovu chápat nejen jako prostou obnovu poškozeného majetku a rozvrácených funkcí, ale je ji třeba uskutečňovat tak, aby v budoucnu dopady stejně silné pohromy byly menší.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur
Dílčí cíl 2.2.1: Vzájemné závislosti systémů KI	Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování positivních synergií. *Při obnově a zvyšování odolnosti území je zcela zásadní řešit a zohledňovat vzájemnou závislost systémů KI, která může způsobovat zesilující negativní účinky mimořádných událostí a domino efekty a naopak posilovat účinky pozitivní.*	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.2:** Komunikace a vazby mezi kritickými infrastrukturami

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**4,4**	Procesy obnovy zásadním způsobem ovlivňují dobu trvání krizové situace. Mají kritický význam pro zajišťování základních fyziologických potřeb a zajištění bezpečnosti občanů, majetku a životního prostředí.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**4,0**	
Významnost cíle pro obranu státu:	**4,0**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Manažerské systémy řízení 2) Informační technologie 3) Ekonomika

Současná úroveň a kvalita výzkumu v ČR:	**3,8**	Současná výzkumná infrastruktura je schopna tyto zásady v rámci aplikovaného výzkumu adaptovat na jednotlivé oblasti kritické infrastruktury. V řadě případů se bude jednat o „soft“ opatření, která nemusí být ekonomicky příliš náročná. Prevence zakomponované do obnovy pro zabránění opakování krizové situace bývá řádově méně nákladná, než obnova po opakující se pohromě.
Úroveň výzkumné infrastruktury:	**3,8**	
Podpora ve státní politice a regulaci:	**3,6**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,0**	
Očekávaná finanční náročnost dosažení cíle:	**2,8**	
Absorpční kapacita aplikační sféry:	**4,0**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	3 Krizové řízení a bezpečnostní politika
Podoblast:	3.4 Legislativní a právní problémy
Stěžejní cíl:	Rozvíjet legislativní postupy a navrhovaná legislativní opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů a složek, aby dynamicky reagoval na nově vznikající potřeby bezpečnostního systému ČR s preferencí krizových situací spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) nebo vnitřní bezpečnosti státu a dále pak při přírodních (živelních) a antropogenních (tj. lidmi nebo lidskou činností způsobených) pohromách.

Název dílčího cíle:	**3.4.1 Legislativní postupy a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací**	**2030** (průběžně)
Popis dílčího cíle:	Analyzovat a vytvářet legislativní postupy a opatření tak, aby legislativní rámec vytvářet komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách s preferencí problematiky krizového řízení, ochrany obyvatelstva, ochrany kritické infrastruktury, civilního nouzového plánování, integrovaného záchranného systému, požární ochrany, ochrany veřejného zdraví, udržitelného rozvoje. *Začlenit rovinu bezpečnosti do koncepčních dokumentů na národní i regionální úrovni rozvoje v souladu se Strategickým rámcem udržitelného rozvoje ČR.* *Rozvíjet legislativní postupy a opatření tak, aby legislativní rámec vytvářel komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničení životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnější bezpečnosti státu (stav ohrožení státu a válečný stav) včetně vazeb na krizové situace související s ohrožením vnitřní bezpečnosti státu a při přírodních a antropogenních pohromách.* *Analyzovat relevantní legislativní akty EU a strategické dokumenty NATO a navrhovat způsoby jejich implementace do legislativy České republiky tak, aby legislativní rámec vytvářející komplexní prostor pro efektivní činnost příslušných orgánů, organizací, složek a obyvatelstva při mimořádných a krizových situacích spojených s ohrožením životů a zdraví obyvatelstva, ničením životního prostředí, majetkových a kulturních hodnot, ke kterým dochází v souvislosti s ohrožením vnitřní bezpečnosti státu, při přírodních a antropogenních pohromách a v souvislosti s vnějším ohrožením státu (stav ohrožení státu a válečný stav), byl plně v souladu s legislativou EU.*	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat organizační, technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná, následná a dlouhodobá opatření na ochranu obyvatel – ukrytí, evakuaci/přesídlení, zdravotní péči postiženým, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití prostředků/zbraní hromadného ničení (CBRNE) a na ochranu před	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva

	nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování a, komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.	
Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva	Rozvíjet a zdokonalovat metody, metodiky a postupy pro zvyšování efektivnosti a účinnosti organizační, technické a technologické úrovně relevantních prostředků a služeb zabezpečujících ochranu obyvatelstva, majetku a životního prostředí při mimořádných a krizových situacích s důrazem na připravenost a akceschopnost integrovaného záchranného systému ČR.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby	Zajistit na základě kvantitativní a kvalitativní analýzy bezpečnostních hrozeb a predikce vývoje bezpečnostních rizik přijímání opatření majících za cíl zvýšit adaptabilitu bezpečnostního systému na změny v bezpečnostním prostředí (struktura, nástroje, vazby bezpečnostního systému).	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.1:** Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR
Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR	Zajišťování kvantitativní a kvalitativní analýzy bezpečnostních hrozeb, predikce vývoje bezpečnostních rizik, monitoring nově se objevujících dosud neznámých rizik a to i prostřednictvím pravidelně zpracovávaných prognostických studií a scénářů (normativní, explorační, prediktivní) vývoje bezpečnostní situace ve světě, Evropě a ČR. Následné promítnutí do tvorby a realizace strategických a řídících dokumentů v oblasti bezpečnosti.	**Oblast 3:** Krizové řízení a bezpečnostní politika **Podoblast 3.2:** Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření

Významnost dílčího cíle	
Významnost pro fungování státu a infrastruktur: 4,3	Tento dílčí cíl je expertně velmi výrazně hodnocený cíl v rámci prioritní oblasti 6 Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR. To potvrzuje významnost a prioritu dílčího cíle pro fungování státu, infrastruktur, bezpečnost občanů, občanské společnosti a pro obranu státu. Systém ochrany životů, zdraví a majetkových hodnot, jakož i působnost při výkonu státní správy v jednotlivých oblastech státem chráněných zájmů je kodifikován právním řádem České republiky. Základním principem tohoto systému je vytváření a rozvíjení podmínek pro přípravu na vznik mimořádných událostí a krizových stavů a pro poskytování účinné pomoci v případě, že takové situace nastanou. Přitom platí, že významnou součástí předpisové základny v oblasti ochrany životů, zdraví a majetkových hodnot je předcházení rizikům, tedy prevence. Zvláštními právními předpisy jsou v rámci vymezených působností státním orgánům a orgánům územních samosprávných celků stanoveny povinnosti a pravomoci tak, aby byla v uvedených oblastech zabezpečována ochrana životů, zdraví a majetkových hodnot na potřebné úrovni. Činnosti příslušných orgánů probíhají koordinovaně, avšak systém je koncipován tak, aby jeho jednotlivé součásti byly schopny plnit stanovené úkoly samostatně. V daných souvislostech jsou samozřejmě práva a povinnosti stanoveny také právnickým osobám a fyzickým osobám. Veškeré právní předpisy je nutno připravovat a koncipovat v duchu sbližování právních předpisů České republiky s právem Evropských společenství. V oblasti požární ochrany, krizového řízení, ochrany obyvatelstva a integrovaného záchranného systému je, podle kompetenčního zákona (zákon č. 2/ 1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů) působným ústředním orgánem státní správy Ministerstvo vnitra, přičemž úkoly státu na příslušných úrovních zabezpečují také ostatní ministerstva a jiné státní orgány, hasičské záchranné sbory krajů a v přenesené působnosti také orgány krajů a orgány obcí.
Významnost cíle pro bezpečnost občanů a občanské společnosti: 3,9	
Významnost cíle pro obranu státu: 4,0	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Ochrana obyvatelstva 3) Ekonomika 4) Právní věda

Současná úroveň a kvalita výzkumu v ČR: 3,7 **Úroveň výzkumné infrastruktury: 3,8** **Podpora ve státní politice a regulaci: 3,7** **Kvalita lidských zdrojů a úroveň vzdělávání: 3,9** **Očekávaná finanční náročnost dosažení cíle: 3,0** **Absorpční kapacita aplikační sféry: 3,9**	Česká republika disponuje vysoce erudovanými odborníky s praktickými zkušenostmi, kteří mají schopnosti definovat obsahové zaměření legislativních postupů a opatření vnitřní bezpečnosti státu, přírodních a antropogenních mimořádných událostí a krizových situací. Úroveň výzkumné infrastruktury je z pohledu obsahu na vysoké úrovni. Horší situace je při aplikaci obsahové stránky do paragrafového znění. Stát tuto oblast systematicky, komplexně a dlouhodobě koordinuje na odpovídající úrovni. Důležitá je implementace doporučení a nařízení EU. Finanční prostředky vynaložené na výzkum, experimentální vývoj a inovace pro tento dílčí cíl je nezbytné považovat za základní vklad pro zvyšování úrovně připravenosti ČR na zvládání mimořádných událostí a krizových situací. Z tohoto pohledu lze považovat dosažené bodové hodnocení za nadhodnocené. V reálném odhadu je náročnost úrovně 4,5 bodového hodnocení. Absorpční kapacita aplikační sféry je vysoká a nezbytná. Uživatelem výsledků výzkumu a vývoje v oblasti ochrany obyvatelstva budou instituce státní správy a samosprávy, prvky Bezpečnostního systému ČR, bezpečnostní složky a podnikatelské subjekty působící v oblasti zajišťování bezpečnosti, odborná i laická veřejnost, kdy je třeba akcentovat a legislativně zakotvit i prvek sebeochrany obyvatel a jejich participaci na likvidaci následků.

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	4 Obrana, obranyschopnost a nasazení ozbrojených sil
Podoblast:	4.1 Rozvoj schopností ozbrojených sil
Stěžejní cíl:	Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.

Název dílčího cíle:	**4.1.1 Vývoj nových zbraňových a obranných systémů**	**2030** (průběžně)
Popis dílčího cíle:	Cílem je hledání a realizace vhodného konceptu ochrany a obrany prostoru ČR, a to ať už vlastními silami a prostředky a nebo zapojením se do mezinárodních projektů, které zejména přinesou úsporu personálu a zvýší efektivnost schopností ozbrojených sil.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva	Rozvíjet a zdokonalovat technické, technologické, metodické a kontrolní postupy a opatření ochrany obyvatelstva směřující k zabránění vzniku, respektive k minimalizaci následků mimořádných a krizových situací. Důraz je kladen na systémy varování, vyrozumění a monitorování vzniku a hodnocení vývoje a dopadů dané situace, na neodkladná a dlouhodobá opatření na ochranu obyvatel – evakuaci, kolektivní a individuální ochranu, záchranné a likvidační práce, zabezpečení nouzového přežití, humanitární pomoc - dále na specifická opatření při použití zbraní hromadného ničení (CBRNE) a na ochranu před nebezpečnými chemickými látkami, biologickými agens a zdroji ionizujícího záření, na informování obyvatelstva, na komunikaci s obyvatelstvem, na motivaci občanů k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti spoluobčanů a blízkých.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.1:** Ochrana obyvatelstva
Dílčí cíl 4.1.2: Přeprava, mobilita a udržitelnost sil	Cílem je rozvíjet a zdokonalovat metody, postupy, technická a jiná řešení, která povedou k vyšší mobilitě a dlouhodobé udržitelnosti sil v operacích. Ta je zejména spojena s ochrannou živé síly. Proto je cílem i vývoj a zdokonalování prostředků aktivní i pasivní ochrany živé síly a vojenské techniky v celém spektru operací, jako např. výstroj, výzbroj, prostředky balistické ochrany, individuální i kolektivní prostředky ochrany proti ZHN a maskování.	**Oblast 4:** Obrana, obranyschopnost a nasazení ozbrojených sil **Podoblast 4.1:** Vývoj nových zbraňových a obranných systémů

Významnost dílčího cíle	
Významnost pro fungování státu a infrastruktur:	**3,2**
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**2,5**

Významnost cíle pro obranu státu: 2,3	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Strategická studia 3) Technické vědy 4) Bezpečnostní technologie 5) Právo 6) Matematika
Současná úroveň a kvalita výzkumu v ČR: 3,0	Česká republika zdědila po Československo velmi kvalitní výzkumnou a vývojovou základnu v oblasti zbrojních technologií. To je zejména dlouholetou tradicí. Tato základna byla dříve soustředěna v působnosti Ministerstva obrany (akademická pracoviště, výzkumné technické ústavy, opravárenské podniky), ale v důsledku přeměny ČR na otevřenou ekonomiku orientovanou na export se postupně začala etablovat špičková pracoviště mimo působnost ministerstva. To dokazuje např. exkluzivní spolupráce ČVUT s armádou Spojených států. V ČR dokonce existují studijní obory specializující se na problematiku vojenských technologií. Technický výzkumu a vývoj byl a je však ze své podstaty finančně velmi náročný z důvodu požadavku vytvoření prototypů, funkčních vzorků a nákladům na jejich testování. Navzdory určitému ústupu, existuje v České republice stále vysoká absorpční kapacita výsledků vojenského technického výzkumu a vývoje.
Úroveň výzkumné infrastruktury: 4,0	
Podpora ve státní politice a regulaci: 3,0	
Kvalita lidských zdrojů a úroveň vzdělávání: 4,0	
Očekávaná finanční náročnost dosažení cíle: 1,0	
Absorpční kapacita aplikační sféry: 4,0	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	4 Obrana, obranyschopnost a nasazení ozbrojených sil
Podoblast:	4.1 Rozvoj schopností ozbrojených sil
Stěžejní cíl:	Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.

Název dílčího cíle:	**4.1.2 Přeprava, mobilita a udržitelnost sil**	**2030** (průběžně)
Popis dílčího cíle:	Cílem je rozvíjet a zdokonalovat metody, postupy, technická a jiná řešení, která povedou k vyšší mobilitě a dlouhodobé udržitelnosti sil v operacích. Ta je zejména spojena s ochrannou živé síly. Proto je cílem i vývoj a zdokonalování prostředků aktivní i pasivní ochrany živé síly a vojenské techniky v celém spektru operací, jako např. výstroj, výzbroj, prostředky balistické ochrany, individuální i kolektivní prostředky ochrany proti ZHN a maskování.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 4.1.1: Vývoj nových zbraňových a obranných systémů	Cílem je hledání a realizace vhodného konceptu ochrany a obrany prostoru ČR, a to ať už vlastními silami a prostředky a nebo zapojením se do mezinárodních projektů, které zejména přinesou úsporu personálu a zvýší efektivnost schopností ozbrojených sil.	**Oblast 4:** Obrana, obranyschopnost a nasazení ozbrojených sil **Podoblast 4.1:** Rozvoj schopností ozbrojených sil

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,8**	Obranyschopnost státu je přímo spojena se schopnostmi ozbrojených sil. Vzhledem k tomu, že ČR je součástí systému kolektivní obrany a jako taková musí být schopna nasadit a po určitou dobu udržet v operaci své ozbrojené síly jsou schopnosti českých ozbrojených sil budovány jako expediční a nasaditelné pro celé spektrum operací. Stejně jako spojenců ČR si tento koncept vyžaduje soustavné zdokonalování těchto schopností tak, aby byla zajištěna konvergence kvality nasazovaných sil a prostředků. Jejím výchozím bodem je interoperablita sil a prostředků a cílovým standardem stav popsaný prostřednictvím Force Goals a Force Proposals.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**2,2**	
Významnost cíle pro obranu státu:	**4,3**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Bezpečnostní vědy 2) Technické vědy 3) Vojenské vědy 4) Ochrana obyvatelstva 5) Technologie 6) Chemie 7) Technická kybernetika 8) Biologie 9) Medicína

Současná úroveň a kvalita výzkumu v ČR: **3,0**	Otázka naplnění standardů sil a prostředků zajišťující interoperabilitu a v krajnosti shodnost sil je záležitostí aplikační. Z toho úhlu pohledu cíl navazuje na dílčí cíl 4.1.1. To určuje i očekávanou nižší finanční náročnost cíle. Absorpční kapacita je však zpravidla omezována jen na české ozbrojené síly, nelze však vyloučit její rozšíření i na jiné ozbrojené síly v rámci nového konceptu NATO SMART Defence. Výzkumná infrastruktura je stejnou infrastrukturou, jako v případě dílčího cíle 4.1.1.
Úroveň výzkumné infrastruktury: **4,0**	
Podpora ve státní politice a regulaci: **3,0**	
Kvalita lidských zdrojů a úroveň vzdělávání: **3,0**	
Očekávaná finanční náročnost dosažení cíle: **2,0**	
Absorpční kapacita aplikační sféry: **3,0**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	4 Obrana, obranyschopnost a nasazení ozbrojených sil
Podoblast:	4.1 Rozvoj schopností ozbrojených sil
Stěžejní cíl:	Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.

Název dílčího cíle:	**4.1.3 Podpora velení a řízení**	**2030** (průběžně)
Popis dílčího cíle:	Cílem je rozvoj systémů velení a řízení v operacích umožňujících získání společného přehledu o vývoji situace s aliančními partnery a informační převahy nad protivníkem. Rozvoj technických a jiných řešení, která povedou ke zvýšení efektivnosti řízení rezortu MO, zejména k personálním úsporám. Modernizace a rozvoj zpravodajského, geografického a hydrometeorologického zabezpečení s důrazem na implementaci systému Intelligence, Surveillance, and Reconnaissance.	
Vazba na ostatní dílčí cíle:		
Dílčí cíl 4.1.2: Přeprava, mobilita a udržitelnost ozbrojených sil	Cílem je rozvíjet a zdokonalovat metody, postupy, technická a jiná řešení, která povedou k vyšší mobilitě a dlouhodobé udržitelnosti sil v operacích. Ta je zejména spojena s ochrannou živé síly. Proto je cílem i vývoj a zdokonalování prostředků aktivní i pasivní ochrany živé síly a vojenské techniky v celém spektru operací, jako např. výstroj, výzbroj, prostředky balistické ochrany, individuální i kolektivní prostředky ochrany proti ZHN a maskování.	**Oblast 4:** Obrana, obranyschopnost a nasazení ozbrojených sil **Podoblast 4.1:** Rozvoj schopností ozbrojených sil

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**2,4**	Schopnost ozbrojených sil dosáhnout požadovaného výsledku v jejich nasazení je vždy podmíněna schopností zajistit přístup a zpracování adekvátních informací. To je funkcí velení a řízení, jako specifické schopnosti ozbrojených sil a ministerstva odpovědného za organizaci odvětví obrany ČR. Od 70. let 20. století se v této oblasti projevuje stále silněji trend automatizace a zlepšování kvalitativní a komplexnosti informace používané pro potřeby rozhodování. Tato schopnost je specifickou schopností příznačnou pro vojensky organizované organizace.
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**1,5**	
Významnost cíle pro obranu státu:	**3,0**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Vojenské vědy 2) Manažerské systémy řízení 3) Ekonomie 4) Informační technologie 5) Informatika 6) Umělá inteligence
Současná úroveň a kvalita výzkumu v ČR: **3,0**	

Úroveň výzkumné infrastruktury:	**2,0**	řízení chápáno spíše jako rozšiřování počítačů i na úlohy, které byly řešeny jiným, z hlediska životního cyklu, hospodárnějším způsobem. Příkladem jsou informační systémy dodávané na klíč. Takto však nedochází k nárůstu produktivity personálu obecně spojované s nasazením nových technologií.
Podpora ve státní politice a regulaci:	**3,0**	
Kvalita lidských zdrojů a úroveň vzdělávání:	**3,0**	
Očekávaná finanční náročnost dosažení cíle:	**3,0**	
Absorpční kapacita aplikační sféry:	**4,0**	

IDENTIFIKAČNÍ LIST PRIORITNÍHO DÍLČÍHO CÍLE

Prioritní oblast:	**Rostoucí komplexita hrozeb, rizik a adaptace bezpečnostního systému ČR**
Oblast:	4 Obrana, obranyschopnost a nasazení ozbrojených sil
Podoblast:	4.1 Rozvoj schopností ozbrojených sil
Stěžejní cíl:	Zajistit rozvoj schopností ozbrojených sil ČR v klíčových oblastech, které jsou nezbytné k zajištění obrany země a k dosažení deklarovaných politicko-vojenských ambicí České republiky a naplnění rolí a funkcí ozbrojených sil České republiky.

Název dílčího cíle:	**4.1.4 Rozvoj KIS a kybernetická obrana**	**2020**
Popis dílčího cíle:	Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací.	

Vazba na ostatní dílčí cíle:		
Dílčí cíl 1.2.2: Minimalizace kybernetické kriminality a zneužívání informací	Vytvoření systému pro trvalé zlepšování schopnosti rozpoznávat a čelit novým formám kybernetické kriminality a zneužívání informací; koordinovaná inovace, vytváření a zavádění organizačních, technických a legislativních nástrojů pro boj proti těmto fenoménům.	**Oblast 1:** Bezpečnost občanů **Podoblast 1.2:** Ochrana před kriminalitou, extremismem a terorismem
Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI	Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.	**Oblast 2:** Bezpečnost kritických infrastruktur a zdrojů **Podoblast 2.1:** Ochrana, odolnost a obnova kritických infrastruktur

Významnost dílčího cíle		
Významnost pro fungování státu a infrastruktur:	**3,2**	Současné schopnosti ozbrojených sil jsou charakteristické aplikací komunikačních a informačních technologií. To je patrné zejména u systémů velení a řízení. Nasazení těchto technologií na jedné straně přináší výhodu jednodušší obsluhy, na druhé straně tu vzniká určitý druh zranitelnosti. To v případě závislosti schopností na těchto technologiích. Ochrana proti kybernetickým hrozbám a zajištění utajeného přenosu informací je životním zájmem zajištění obranyschopnosti České republiky. Zároveň jde o jednu z priorit NATO. Proto lze očekávat existenci společných mezinárodních projektů
Významnost cíle pro bezpečnost občanů a občanské společnosti:	**2,7**	
Významnost cíle pro obranu státu:	**3,7**	

Dosažitelnost dílčího cíle	
Související obory výzkumu a vývoje:	1) Informační technologie 2) Informatika 3) Bezpečnostní vědy 4) Bezpečnostní technologie 5) Umělá inteligence
~~Současná úroveň a~~	Česká republika disponuje množstvím soukromých subjektů zabývajících se vývojem

kvalita výzkumu v ČR:	**3,0**
Úroveň výzkumné infrastruktury:	**3,0**
Podpora ve státní politice a regulaci:	**3,0**
Kvalita lidských zdrojů a úroveň vzdělávání:	**4,0**
Očekávaná finanční náročnost dosažení cíle:	**3,0**
Absorpční kapacita aplikační sféry:	**3,0**

prodejem software pro oblast kybernetické obrany. Otázky vytváření symbiózy těchto firem se státem doposud stály poněkud stranou. Tomu odpovídá i snaha o zastřešení otázek kybernetické bezpečnosti ne úrovni některého z ústředních orgánů státní správy a sjednocení jejich přístupu v otázkách společné strategie.
S ohledem na požadavek mobility vojenských schopností je žádoucí, aby část problematiky kybernetické ochrany u mobilních KIS byla řešena samostatně. Tomuto přístupu doposud odpovídá i existence vlastních výzkumných a vývojových kapacit v působnosti Ministerstva obrany. Personál zabývající se kybernetickými hrozbami má přístup ke kapacitám NATO soustředěným v NATO Cooperative Cyber Defence Centre of Excellence v Tallinnu.