

## Příloha 7

### Bezpečná společnost: Podrobná specifikace prioritní oblasti

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 škrťů a politického boje stala nezřetelnou a bezpečnostní složky 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 neomezuji:

- 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.

## 1. Struktura a cíle prioritní oblasti

Tab. 1: Struktura prioritní oblasti Bezpečná společnost

Oblasti	Podoblasti	Prioritní dílčí cíle
<b>1. Bezpečnost občanů</b>	1.1 Ochrana obyvatelstva	1.1.1 Podpora opatření a úkolů ochrany obyvatelstva
		1.1.2 Zdokonalování služeb a prostředků
		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
<b>2. Bezpečnost kritických infrastruktur a zdrojů</b>	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
<b>3. Krizové řízení a bezpečnostní politika</b>	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
	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
<b>4. Obrana, obranyschopnost a nasazení ozbrojených sil</b>	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

### 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 stříelných 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, řídicích, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.

	<p><b>Dílčí cíl 1.1.1: Podpora opatření a úkolů ochrany obyvatelstva</b></p> <p>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.</p>
	<p><b>Dílčí cíl 1.1.2: Zdokonalování služeb a prostředků ochrany obyvatelstva</b></p> <p>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.</p>
	<p><b>Dílčí cíl 1.1.3: Bezpečnost měst a obcí, informování, vzdělávání a motivace občanů</b></p> <p>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.</p>

## **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 potlačovat všechny formy závažné trestné činnosti. 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 minimalizaci 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 odvrácením 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 výpadech 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**

	<p>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.</p> <p>Účinná detekce a identifikace možných nebezpečí a interpretace informací pro ustanovení situačního přehledu (situation awareness).</p>
	<p><b>Dílčí cíl 2.1.5: Rozvoj ICT, telematiky a kybernetické ochrany KI</b></p> <p>Rozvoj ICT, telematiky a kybernetické ochrany systémů KI a ochrany citlivých informací s využitím nových technologií.</p>

### **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 velikostí 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.	
	<b>Dílčí cíl 2.2.1: Vzájemné závislosti systémů KI</b> Analýza a modelování vzájemných závislostí systémů KI s cílem prevence zesilujících negativních účinků a domino efektů a posilování pozitivních synergií.
	<b>Dílčí cíl 2.2.2: Informační podpora pro detekci možných nepříznivých ovlivňování</b> 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.

<b>Podoblast 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR</b> 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.	
<b>Stěžejní cíl 3.1:</b> Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídicích 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.	
	<b>Dílčí cíl 3.1.1: Vyhodnocení efektivity strategických řídicích a hodnotících dokumentů</b>



	<p><b>v oblasti bezpečnosti</b></p> <p>Cílem je analyzovat proces přípravy, plnění a hodnocení strategických řídicích 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.</p>
	<p><b>Dílčí cíl 3.1.2: Podpora adaptability bezpečnostního systému ČR na změny v bezpečnostním prostředí a vznikající nové bezpečnostní hrozby</b></p> <p>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).</p>

	<p><b>Podoblast 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření</b></p> <p>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 řídicích dokumentů v oblasti bezpečnosti.</p>
	<p><b>Stěžejní cíl 3.2:</b></p> <p>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 řídicích dokumentů v oblasti bezpečnosti.</p>
	<p><b>Dílčí cíl 3.2.1: Analýza bezpečnostních hrozeb a tvorba scénářů vývoje bezpečnostní situace ve světě, Evropě a ČR</b></p> <p>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 řídicích dokumentů v oblasti bezpečnosti.</p>
	<p><b>Dílčí cíl 3.2.2: Podpora specifických oblastí bezpečnosti</b></p> <p>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.</p>

**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, 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, vybavenosti 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.

	<p><b>Dílčí cíl 4.1.3: Podpora velení a řízení</b></p> <p>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.</p>
	<p><b>Dílčí cíl 4.1.4: Rozvoj KIS a kybernetická obrana</b></p> <p>Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací.</p>

## 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 řídicích 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 řídicích 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.

### **3. Indikátory pro kontrolu dosahování cílů**

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

<b>Podoblast</b>	<b>Indikátory</b>
<b>Podoblast 1.1: Ochrana obyvatelstva</b> <b>Stěžejní cíl 1.1:</b> 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, řídicích, plánovacích, kontrolních, legislativních, metodických a dalších postupů a opatření v oblasti ochrany obyvatelstva.	<ul style="list-style-type: none"> <li>• Úroveň spokojenosti občanů s ochranou obyvatelstva v případě živelních pohrom a provozních havárií (Zdroj: CVVM AV ČR);</li> <li>• Absolutní hodnoty uchráněné při požárech (Zdroj: MV-GŘ HZS ČR);</li> <li>• Podíl podniků s produkty v oblasti bezpečnostních a záchranných složek (Zdroj: ČSÚ);</li> <li>• Počet osob zachráněných jednotkami požární ochrany (Zdroj: MV-GŘ HZS ČR);</li> <li>• Početní druhové mimořádné události a krizové situace se zásahy jednotek požární ochrany (Zdroj: MV-GŘ HZS ČR);</li> <li>• Počet a rozsah realizovaných preventivních opatření v ochraně obyvatelstva (Zdroj: orgány veřejné správy);</li> </ul>
<b>Podoblast 1.2: Ochrana před kriminalitou, extremismem a terorismem</b> <b>Stěžejní cíl 1.2:</b> Stěžejním cílem této oblasti je vybudovat	<ul style="list-style-type: none"> <li>• Přijetí odpovídající legislativy a její využívání judikaturou;</li> <li>• Dotvoření bezpečnostního systému v oblasti boje proti kriminalitě, extremismu a terorismu;</li> </ul>

<p>v rámci komplexního bezpečnostního systému takovou politiku s odpovídajícími nástroji, která bude schopna v maximální možné míře potlačovat 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.</p>	<ul style="list-style-type: none"> <li>• Prevence násilného extremismu a terorismu, odhalování a případné zvládnutí následků teroristických útoků (Zdroj: ad hoc analýzy srovnávajícího potenciál a reálné pokusy o útoky);</li> <li>• Pokles trestné činnosti a zvýšení její objasněnosti (Zdroj: Zpráva o bezpečnostní situaci na základě evidence kriminality);</li> <li>• Zvýšení pocitu bezpečnosti občanů (Zdroj: Výzkumy CVVM);</li> <li>• Pokles extremistických akcí a deliktů (Zdroj: Zpráva o problematice extremismu v ČR na základě údajů bezpečnostních složek);</li> <li>• Zvýšení pocitu bezpečnosti u skupin ohrožených extremismem (Zdroj: ad hoc sociologická šetření, údaje specializovaných úřadů, např. Vládní agentury pro sociální začleňování apod.);</li> <li>• Statistiky teroristických útoků (Zdroj: vyhodnocení vládní Strategie boje proti terorismu);</li> </ul>
<p><b>Podoblast 2.1: Ochrana, odolnost a obnova kritických infrastruktur</b>  <b>Stěžejní cíl 2.1:</b>  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</p>	<ul style="list-style-type: none"> <li>• Počet organizací – dodavatelů nezbytných výrobků prací a služeb – s certifikovaným systémem managementu kontinuity (Zdroj: krizové plány);</li> <li>• Snížení velikosti dopadu krize se zahrnutím KI a počet odvrácených hrozeb;</li> <li>• Snížení počtu a rozsahu selhání (i dílčích nebo krátkodobých) prvků KI;</li> </ul>



<p>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 výpadech informační infrastruktury.</p>	
<p><b>Podoblast 2.2: Komunikace a vazby mezi kritickými infrastrukturami</b>  <b>Stěžejní cíl 2.2:</b>  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.</p>	<ul style="list-style-type: none"> <li>• Počet případů, kdy byla na základě informační podpory provedena adekvátní preventivní nebo represivní opatření, a rozsah těchto opatření;</li> <li>• Počet a velikost aplikovaných databází, map a metodik;</li> <li>• Snížení velikosti dopadu krize se zahrnutím KI a počet odvrácených hrozeb;</li> </ul>
<p><b>Podoblast 3.1: Rozvoj bezpečnostní politiky státu a bezpečnostního systému ČR</b>  <b>Stěžejní cíl 3.1:</b>  Zdokonalit mechanismus pro tvorbu a realizaci bezpečnostní politiky, vycházející z jasně definované struktury, úlohy a místa strategických řídicích 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</p>	<ul style="list-style-type: none"> <li>• Optimalizace finančních prostředků vydávaných na zajištění bezpečnosti a obrany, fungování bezpečnostního systému;</li> <li>• Stav zajištění bezpečnosti/bezpečí občanů (např. pokles/zvýšení kriminality, akceschopnost při zajišťování zdraví a majetku občanů, při zajišťování ochrany kritické infrastruktury, apod.);</li> <li>• Schopnost plnit spojenecké závazky vůči EU a NATO;</li> </ul>

<p>prostředí a na vznikající nové hrozby. Z tohoto důvodu je potřeba ho vnímat jako otevřený a dynamicky se vyvíjející systém.</p>	
<p><b>Podoblast 3.2: Hodnocení hrozeb a rizik, tvorba a rozvíjení scénářů, postupů a opatření</b>  <b>Stěžejní cíl 3.2:</b>  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 řídicích dokumentů v oblasti bezpečnosti.</p>	<ul style="list-style-type: none"> <li>• Počet a kvalita obsahu nově zpracovaných strategických a řídicích dokumentů v oblasti bezpečnosti;</li> <li>• Počet a kvalita nových opatření k eliminaci hrozeb;</li> <li>• Míra připravenosti složek bezpečnostního systému čelit širšímu spektru hrozeb a rizik;</li> </ul>
<p><b>Podoblast 3.3: Systémy analýzy, prevence, odezvy a obnovy</b>  <b>Stěžejní cíl 3.3:</b>  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, 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.</p>	<ul style="list-style-type: none"> <li>• Míra připravenosti složek bezpečnostního systému čelit širšímu spektru hrozeb a rizik;</li> <li>• Stav zajištění bezpečnosti/bezpečí občanů (akceschopnost při zajišťování zdraví a majetku občanů, při zajišťování ochrany kritické infrastruktury apod.);</li> </ul>

<p><b>Podoblast 3.4: Legislativní a právní problémy</b>  <b>Stěžejní cíl 3.4:</b>  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.</p>	<ul style="list-style-type: none"> <li>• 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);</li> <li>• Úroveň spokojenosti obyvatel a dalších subjektů se stavem legislativy;</li> </ul>
<p><b>Podoblast 4.1: Rozvoj schopností ozbrojených sil</b>  <b>Stěžejní cíl 4.1:</b>  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.</p>	<ul style="list-style-type: none"> <li>• Doba plné funkčnosti IS pod kybernetickou ochranou za rok v odpovědnosti NBÚ (Zdroj: NBÚ a jednotlivé ministerské CIRC);</li> <li>• 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);</li> <li>• 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);</li> </ul>