ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ
Katedra zdravotnických oborů a ochrany obyvatelstva

Možnosti dalšího směřování a rozvoje systému kritické infrastruktury v České republice

Possibilities for Future Direction and Development of Critical Infrastructure System in the Czech Republic

Diplomová práce

Studijní program:	Ochrana obyvatelstva
Studijní obor:	Civilní nouzové plánování

Autor diplomové práce:	Bc. Martin Tilcer
Vedoucí diplomové práce:	Ing. Ivan Koleňák

Kladno 2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Tilcer**	Jméno:	**Martin**	Osobní číslo:	**492533**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Možnosti dalšího směřování a rozvoje systému kritické infrastruktury v České republice

Název diplomové práce anglicky:

Possibilities for Future Direction and Development of Critical Infrastructure System in the Czech Republic

Pokyny pro vypracování:

Předmětem diplomové práce bude charakterizovat a analyzovat současné fungování systému kritické infrastruktury v České republice. Teoretická část bude obsahovat popis souvisejících právních předpisů a dalších dokumentů, vymezení základních pojmů ve zkoumané oblasti a popis systému kritické infrastruktury v České republice a jeho návaznost na evropskou kritickou infrastrukturu. V praktické části bude pomocí SWOT analýzy podrobně analyzován proces identifikace a způsob ochrany prvků kritické infrastruktury v jednotlivých odvětvích. Následně bude tento systém pomocí komparativní metody porovnán se systémy kritické infrastruktury ve vybraných zemích Evropské unie, a to zejména z pohledu jejich přístupu k identifikaci a určování prvků kritické infrastruktury. Výsledkem práce budou návrhy opatření ke zlepšení systému ochrany kritické infrastruktury v podmínkách České republiky.

Seznam doporučené literatury:

[1] HROMADA, Martin a kol. , Systém a způsoby hodnocení odolnosti kritické infrastruktury, Ostrava: Edice SPBI Spektrum, 2013, 177 s., ISBN 978-80-7385-140-8
[2] SKALICKÁ, Petra, Ochrana a obrana kritické infrastruktury: úskalí a možnosti rozvoje v České republice, The Science For Population Protection, ročník 9, číslo 2, 2017, ISSN 1803-635X
[3] SETOLA, Roberto, ROSATO, Vittorio, KYRIAKIDES, Elias, ROME, Erich, Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach, Springer International Publishing: Studies in Systems, Decision and Control, 2016, 90 s., ISBN 978-3-319-51043-9

Jméno a příjmení vedoucí(ho) diplomové práce:

Ing. Ivan Koleňák

Jméno a příjmení konzultanta(ky) diplomové práce:

kpt. Mgr. Lukáš Pidhaniuk

Datum zadání diplomové práce: **21.09.2020**
Platnost zadání diplomové práce: **18.09.2022**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

6. 5. 2021
Datum převzetí zadání

Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Možnosti dalšího směřování a rozvoje systému kritické infrastruktury v České republice vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Praze dne 12.05.2021

…….

Bc. Martin Tilcer

PODĚKOVÁNÍ

Mé poděkování patří Ing. Ivanu Koleňákovi, a to především za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval. Děkuji také kpt. Mgr. Lukášovi Pidhaniukovi za odborné konzultace k problematice evropské kritické infrastruktury.

ABSTRAKT

Diplomová práce se zabývá systémem kritické infrastruktury v České republice, kdy hlavní zkoumanou oblastí je především otázka identifikace a určování prvků kritické infrastruktury a jejich ochrana.

K hodnocení současného systému je použita SWOT analýza doplněná o multikriteriální analýzu pomocí metody AHP, kterou je provedeno párové porovnání jednotlivých identifikovaných jevů. Ty jsou poté dle výsledků získaných pomocí metody AHP posouzeny pomocí Paretova pravidla.

Systém kritické infrastruktury v České republice je následně porovnán s obdobnými systémy na Slovensku a ve Finsku, přičemž cílem tohoto porovnání a předchozí analýzy je identifikace slabých míst v současném systému a navržení odpovídajících opatření.

Tato opatření jsou navrhována ve čtyřech hlavních oblastech. Jedná se o návrh změny určujících kritérií, kdy by nově odvětvová kritéria sloužila pouze k vymezení typů objektů a služeb, jejichž narušení by mělo závažný dopad na bezpečnost státu a následné posuzování kritičnosti potenciálních prvků kritické infrastruktury by bylo prováděno pouze pomocí průřezových kritérií.

Navrhována je také úprava kompetencí s cílem posílit koordinační roli Ministerstva vnitra a to v otázce určování nových prvků kritické infrastruktury a provádění kontrol u subjektů kritické infrastruktury. Dále je navrhováno zavedení možnosti udílet sankce v případě, že subjekt kritické infrastruktury neplní povinnosti stanovené krizovým zákonem a v neposlední řadě je navrženo rozšíření ochrany kritické infrastruktury o oblast resilience a posílení spolupráce mezi veřejným a soukromým sektorem podle finského vzoru.

Klíčová slova

Kritická infrastruktura; evropská kritická infrastruktura; prvek kritické infrastruktury; subjekt kritické infrastruktury; ochrana kritické infrastruktury; SWOT analýza; komparativní metoda.

ABSTRACT

The diploma thesis deals with the system of critical infrastructure in the Czech Republic. The thesis is focused mainly on the question of identification and designation of critical infrastructure and its protection.

SWOT analysis was chosen as a main research method and is further supplemented by AHP method, in order to perform pairwise comparison of individual identified phenomena. These are then assessed by Pareto Principle according to the results of AHP method pairwise comparison. The critical infrastructure system in the Czech Republic is then compared with similar systems in Slovakia and Finland, and the aim of this comparison and previous analysis is to identify weaknesses in the current system and to propose appropriate measures.

These measures are then proposed in four main areas. First proposal aims to change the determining criteria, where the new sectoral criteria would only be used to define the types of facilities and services that could be potentially critical. The subsequent assessment of criticality of potential critical infrastructure would be then performed by cross-cutting criteria only.

Furthermore, an adjustment of competencies is proposed in order to strengthen the coordination role of the Ministry of the Interior in the area of critical infrastructure designation and in carrying out inspections of critical infrastructure operators. It is also proposed to implement sanctions to critical infrastructure operators that fail to comply with the obligations set out in the Crisis Act. Last of these measures is to extend critical infrastructure protection by implementation of resilience and strengthening of public-private cooperation according to the Finnish model.

Keywords

Critical Infrastructure; European Critical Infrastructure; Object of Critical Infrastructure; Subject of Critical Infrastructure; Protection of Critical Infrastructure; SWOT Analysis; Comparative Method.

Obsah

1 ÚVOD

Lidská společnost je již od nepaměti do jisté míry závislá na infrastrukturách zajišťujících přístup obyvatelstva k některým základním službám. V souvislosti se zkušenostmi z druhé světové války a v návaznosti na prudký technologický rozvoj se lidská společnost stala na těchto infrastrukturách silně závislá, přičemž nástup informačních technologií v posledních letech tento trend ještě více umocnil. Tyto zásadní změny s sebou přinesly řadu výzev v podobě nových, do té doby neznámých hrozeb a zranitelností, které mohou skrze narušení těchto infrastruktur ohrozit společnost jako takovou. Takové infrastruktury se začaly označovat jako kritická infrastruktura (1).

Téma týkající se systému kritické infrastruktury je pro mne zajímavé nejen z důvodu své aktuálnosti a významu pro současnou společnost, ale také z důvodu profesního, neboť se touto problematikou zabývám od roku 2016 v rámci své pracovní činnosti vyplývající z mého služebního zařazení na Ministerstvu vnitra-generálním ředitelství Hasičského záchranného sboru České republiky (dále jen „MV-GŘ HZS ČR“), odboru ochrany obyvatelstva a krizového řízení.

2 CÍLE PRÁCE A HYPOTÉZY

Cílem práce je analyzování procesu identifikace a určování prvků kritické infrastruktury (dále jen „prvek KI“) v České republice (dále jen „ČR“) a také způsob jejich ochrany. Analýza je provedena pomocí metody SWOT analýzy, která je podrobně popsána v kapitole 4. Metodika. Následně je systém kritické infrastruktury v ČR porovnán pomocí komparativní metody se systémy kritické infrastruktury ve vybraných zemích Evropské unie (dále jen „EU“), a to konkrétně na Slovensku a ve Finsku. Výsledkem práce jsou návrhy možných opatření k zefektivnění systému ochrany kritické infrastruktury v podmínkách ČR. Pro tento účel byly stanoveny následující hypotézy:

- **Hypotéza 1:** Přístup k identifikaci a určování prvků KI je v jednotlivých odvětvích rozdílný.
- **Hypotéza 2:** K ochraně prvků KI je v rámci hodnocených systémů kritické infrastruktury přistupováno srovnatelným způsobem.
- **Hypotéza 3:** Problematika kritické infrastruktury byla na základě Směrnice EKI implementována v podmínkách ČR na dostatečné úrovni.

3 PŘEHLED SOUČASNÉHO STAVU

V prostředí ČR se problematika kritické infrastruktury začala poprvé řešit v návaznosti na teroristický útok na budovy Světového obchodního centra ve Spojených státech amerických dne 11. září 2001. K legislativnímu ukotvení této problematiky však došlo až o deset let později, a to v souvislosti s přijetím *směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu* (dále jen „Směrnice EKI"), která členským státům EU stanovila povinnost implementovat problematiku ochrany kritické infrastruktury do národní legislativy v termínu do 12. ledna 2011.

3.1 Kritická infrastruktura před rokem 2011

Základ celého systému kritické infrastruktury v ČR byl vytvořen již před teroristickými útoky v roce 2001. Stěžejním krokem v této věci bylo přijetí usnesení vlády ČR k definici a rozsahu základních funkcí státu, kdy se jednalo o jeden z prvních oficiálních dokumentů, jež řešil otázky zabezpečení základních funkcí státu během mimořádných událostí či krizových situací, které nebyly vojenského charakteru. Na toto usnesení bylo dále navázáno v roce 2002, kdy tehdejší ministr vnitra předložil k projednání v Bezpečnostní radě státu v souvislosti s řešením problematiky zajištění základních funkcí státu ucelenou informaci o kritické infrastruktuře. Navazujícím krokem po této informaci bylo stanovení úkolu zpracovat celou problematiku kritické infrastruktury a projednat vzniklý materiál na schůzi Výboru pro civilní nouzové plánování, k čemuž došlo dne 24. září 2002. Tímto materiálem byly v ČR poprvé stanoveny oblasti, které spadaly do národní kritické infrastruktury (2). Jednalo se o

- systém dodávky energií,
- systém dodávky vody,
- systém odpadového hospodářství,
- přepravní síť,
- komunikační a informační systémy,
- bankovní a finanční sektor,
- nouzové služby,
- veřejné služby,
- státní správu a samosprávu.

V roce 2007 byla vládou přijata *Zpráva o řešení problematiky kritické infrastruktury v České republice*, konkrétně usnesením vlády ze dne 21. března 2007 č. 244, která konstatovala nutnost zpracování komplexní strategie a národního programu k řešení problematiky ochrany kritické infrastruktury, přičemž celý proces byl nastaven v *Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národní program ochrany kritické infrastruktury*, který byl přijat usnesením vlády ze dne 25. února 2008 č. 170 (3).

Zásadním materiálem, který definoval celý způsob implementace Směrnice EKI, byla *Komplexní strategie ČR k řešení problematiky Kritické infrastruktury* a na ní navázaný *Národní program ochrany kritické infrastruktury*. Oba uvedené materiály byly schváleny usnesením vlády ze dne 22. února 2020 č. 140. V materiálech byl popsán způsob řešení problematiky kritické infrastruktury, jejího určování a ochrany a také byl stanoven způsob implementace v rámci právního řádu ČR.

V případě řešení této problematiky byly uvažovány dvě varianty, kdy první z nich byla implementace formou samostatného zákona o ochraně kritické infrastruktury, což byla cesta, kterou zvolily některé členské státy EU, např. Slovenská republika. Druhou možnou variantou bylo zapracování do některého

z existujících právních předpisů, a zde se pochopitelně nabízel *zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů* (dále jen „krizový zákon“), ve znění pozdějších předpisů, a prováděcí právní předpisy k němu.

Po diskusích v odborných kruzích, zejména na MV-GŘ HZS ČR a dalších dotčených resortech byla v podmínkách ČR nakonec zvolena právě druhá varianta. Důvodem, mimo jiné, byla i skutečnost, že kritická infrastruktura a její ochrana bezesporu patří do oblasti zachování základních funkcí státu a v případě jejího narušení budou velice pravděpodobně přijímána krizová opatření. Veškeré povinnosti a kompetence tak jsou provázány a uvedeny v rámci jednoho zákona a dvou prováděcích právních předpisů k němu (4).

3.2 Systém kritické infrastruktury v ČR

Systém ochrany kritické infrastruktury tedy prošel významnou proměnou až v souvislosti s novelizací krizového zákona. Nejednalo se však o jediný právní předpis, který byl v rámci tohoto procesu přijat, resp. novelizován. Problematika kritické infrastruktury v ČR tak byla řešena i novelizovanými či nově přijatými prováděcími právními předpisy ke krizovému zákonu. Tento balík právních předpisů vytváří celkový rámec systému kritické infrastruktury v ČR, který je předmětem této kapitoly.

3.2.1 Právní předpisy

Jak bylo uvedeno výše, problematika ochrany kritické infrastruktury je na národní úrovni řešena krizovým zákonem, konkrétně byla tato problematika implementována pomocí *zákona č. 430/2010 Sb., kterým se kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů*. Novelizace definovala základní pojmy, které jsou popsány

v podkapitole 3.2.2, stanovila povinnosti jednotlivým orgánům státní správy a provozovatelům prvků KI. V neposlední řadě byl tímto zákonem stanoven postup pro identifikaci a určování prvků KI v jednotlivých odvětvích (viz kapitola 3.2.6).

Na novelizaci krizového zákona navazovala novelizace *nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)*, kdy se konkrétně jednalo o doplnění specifikace a náležitostí plánu krizové připravenosti subjektu kritické infrastruktury. Základní právní rámec systému kritické infrastruktury uzavírá *nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů*, kterým byla stanovena průřezová a odvětvová kritéria (více o těchto kritériích v podkapitole 3.2.4).

Základní právní rámec poté doplňují další právní předpisy, které se systémem kritické infrastruktury přímo či nepřímo souvisí. Jedním z těchto zákonů je například *zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů*, kterým byla definována kritická informační infrastruktura (dále jen „KII“).

3.2.2 Nelegislativní dokumenty

V případě nelegislativních dokumentů je potřeba zmínit zejména *Bezpečnostní strategii ČR* z roku 2015, která byla schválena usnesením vlády č. 79 ze dne 4. února 2015. Bezpečnostní strategie je základním dokumentem bezpečnostní politiky ČR, který dále rozvíjejí další navazující strategické a koncepční dokumenty. Bezpečnostní strategie zároveň navazuje na předchozí bezpečnostní strategie z roku 2003 a 2011, ale zároveň reflektuje postupný vývoj a proměnu vnějšího a vnitřního bezpečnostního prostředí ČR. Právě Bezpečnostní strategie z roku 2015 zdůrazňuje zvyšující s význam ochrany kritické infrastruktury,

přičemž na základě analýzy bezpečnostního prostředí, bylo mezi bezpečnostní hrozby zahrnuto i ohrožení funkčnosti kritické infrastruktury (5).

Na bezpečnostní strategii ČR navazuje *Koncepce ochrany obyvatelstva ČR do roku 2020 s výhledem do roku 2030*, která definovala ochranu kritické infrastruktury jako jednu ze strategických priorit v oblasti ochrany obyvatelstva. Konkrétně se jedná o *„zvýšení odolnosti a ochrany prvků KI proti možným rizikům a zajištění širšího zapojení subjektů kritické infrastruktury do procesu přípravy na mimořádné události a krizové situace a jejich řešení.“* (6).

K naplnění této priority byl zároveň Ministerstvu vnitra stanoven úkol precizovat systém ochrany kritické infrastruktury, a to například revidováním odvětví kritické infrastruktury (dále jen „odvětví KI“) či formou stanovení standardů ochrany prvků KI (6). Vyhodnocování plnění tohoto úkolu je součástí Zpráv o stavu ochrany obyvatelstva v České republice (zpracovány v roce 2015 a 2018), které jsou předkládány vládě za účelem informování o současném stavu ochrany obyvatelstva a o plnění úkolů stanovených koncepcí (7).

V souvislosti s implementací výše uvedené Směrnice EKI byly usnesením vlády ze dne 22. února 2010 č. 140 schváleny *Komplexní strategie ČR k řešení problematiky kritické infrastruktury* (dále jen „Komplexní strategie“) a *Národní program ochrany kritické infrastruktury* (dále jen „Národní program ochrany KI“). Komplexní strategie vychází z výsledků posouzení situace v oblasti ochrany kritické infrastruktury a zároveň navazuje na předchozí dokumenty řešící tuto oblast. Cílem Komplexní strategie bylo především stanovení dalšího postupu v úpravě systému kritické infrastruktury ve vazbě na Směrnici EKI (8). Stejným usnesením vlády byl také schválen Národní program ochrany kritické infrastruktury, který více rozpracovává návrhy uvedené v Komplexní strategii. V Národním programu ochrany kritické infrastruktury je tak rozpracován postup legislativního ukotvení problematiky ochrany kritické infrastruktury, stanovení klíčových aktérů či finanční zabezpečení (9).

3.2.3 Základní pojmy v oblasti kritické infrastruktury

Klíčové definice využívané v systému kritické infrastruktury jsou obsahem krizového zákona, konkrétně v § 2. Dle tohoto zákona se kritickou infrastrukturou rozumí prvek KI nebo systém prvků KI, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. V kontextu evropské kritické infrastruktury (dále jen „EKI“) se potom jedná o kritickou infrastrukturu na území ČR, jejíž narušení by mělo závažný dopad i na další členský stát EU. Prvek KI je dle současné úpravy chápán jako stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek KI součástí EKI, považuje se za prvek EKI (10).

Prvky KI jsou provozovány subjekty kritické infrastruktury (dále jen „subjekt KI“), které jsou chápány jako provozovatel prvku KI, přičemž jde-li o provozovatele prvku EKI, považuje se tento za subjekt EKI. V neposlední řadě je pro oblast kritické infrastruktury důležitá definice ochrany kritické infrastruktury, jež je chápána jako opatření zaměřená na snížení rizika narušení funkce prvku KI (10). Dle současného pojetí je tak systém kritické infrastruktury zaměřen z právního hlediska pouze na problematiku ochrany prvků KI ve smyslu snižování rizika jejich narušení. V posledních letech se však v souvislosti s ochranou kritické infrastruktury hovoří také o zajištění její resilience, tedy schopnosti prvku KI *absorbovat, adaptovat se a rychle obnovit činnost prvku z důsledků působení nežádoucí události* (1). Tento přístup v současné době není v národním systému zohledněn, ačkoliv subjekty KI v rámci své ochrany tento aspekt řeší také.

Specifikem české úpravy ve vztahu ke Směrnici EKI je také rozlišování mezi kritickou infrastrukturou a prvkem KI, kdy česká úprava více specifikuje zaměření systému ochrany kritické infrastruktuře směrem ke konkrétním objektům. Naproti tomu definice použitá ve Směrnici EKI pojímá kritickou

infrastrukturu jako *prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí*, tedy s větším důrazem na systém než na jednotlivé objekty (11).

3.2.4 Průřezová a odvětvová kritéria

Kromě naplnění definice kritické infrastruktury musí potenciální prvek KI naplňovat průřezová a odvětvová kritéria, která jsou obsahem výše uvedeného nařízení vlády o kritériích pro určení prvku KI. K určení musí potenciální prvek KI splňovat alespoň jedno z průřezových a jedno z odvětvových kritérií. Průřezovými kritérii jsou:

- *„oběti s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
- *ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo*
- *dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob“* (12).

Odvětvovými kritérii, která jsou uvedena v příloze nařízení vlády o kritériích pro určení prvku KI, se naopak rozumí technické či organizační parametry v odvětvích energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby, veřejná správa (12). Konkrétní odvětvová kritéria jsou uvedena v příloze 1.

Odvětvová kritéria byla od doby jejich stanovení několikrát upravována. První velká novelizace proběhla v roce 2014, kdy byla přidána oblast

kybernetické bezpečnosti v rámci odvětví komunikační a informační systémy. Zároveň bylo doplněno odvětví nouzových služeb o kritérium pro určení stanic Hasičského záchranného sboru ČR. Poslední úprava byla přijata v souvislosti s řešením krizové situace spojené s výskytem koronaviru SARS-CoV-2, kdy bylo rozšířeno odvětví zdravotnictví o oblast výroby léčivých prostředků (12).

3.2.5 Aktéři v systému kritické infrastruktury

Aktéři v systému kritické infrastruktury na národní úrovni jsou vymezeni v krizovém zákoně, přičemž dle Národního programu ochrany kritické infrastruktury je lze rozdělit na čtyři hlavní skupiny (9). Jedná se o

- vládu ČR,
- Ministerstvo vnitra,
- ministerstva a ústřední správní úřady (dále jen „ÚSÚ“), v jejichž gesci jsou jednotlivá odvětví kritické infrastruktury,
- subjekty KI.

Vláda ČR v souladu s krizovým zákonem k ochraně kritické infrastruktury stanovuje průřezová a odvětvová kritéria pro určení prvku KI (za tímto účelem přijala nařízení vlády o kritériích pro určení prvku kritické infrastruktury) a zároveň rozhoduje na základě seznamu předloženého Ministerstvem vnitra o určení prvků KI, jejichž provozovatelem je organizační složka státu (tento postup je podrobněji popsán v kapitole 3.2.6).

Ministerstvo vnitra (konkrétně MV-GŘ HZS ČR v souladu s § 10 odst. 4 krizového zákona) plní v systému kritické infrastruktury zejména koordinační roli, kdy koordinuje ve spolupráci s ostatními gesčními a spolu gesčními ministerstvy a ÚSÚ řešení problematiky kritické infrastruktury, a to na národní i evropské úrovni (10). Mezi další úkoly svěřené do kompetence MV-GŘ HZS ČR spadá navrhování průřezových kritérií, zpracovávání a aktualizace seznamu

prvků KI, jejichž provozovatelem je organizační složka státu a v neposlední řadě plnění úkolů vyplývajících z členství ČR v EU. S tím souvisí zabezpečování výměny informací, plnění funkce kontaktního místa ČR pro problematiku EKI a podávání zpráv o plnění úkolů vyplývajících z úkolů stanovených Směrnicí EKI. Konkrétně se jedná o každoroční informování Evropské komise o počtu prvků EKI na území ČR a o jejich vlivu na ostatní členské státy a předkládání souhrnné zprávy se všeobecnými údaji o typech zranitelnosti, hrozbách a rizicích zjištěných v jednotlivých odvětvích EKI každé dva roky (10).

Věcně příslušná ministerstva a jiné ÚSÚ jsou v případě systému kritické infrastruktury stanovena v souladu se *zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR*, přehled všech věcně příslušných ministerstev a ÚSÚ (včetně České národní banky, která je příslušným orgánem krizového řízení) ve vztahu k jednotlivým odvětvím a oblastem je uveden v příloze 2. Zde se konkrétně jedná o tyto resorty:

- Ministerstvo průmyslu a obchodu,
- Ministerstvo dopravy,
- MV-GŘ HZS ČR,
- Ministerstvo zemědělství,
- Ministerstvo zdravotnictví,
- Ministerstvo financí,
- Ministerstvo práce a sociálních věcí
- Ministerstvo životního prostředí,
- Národní úřad pro kybernetickou a informační bezpečnost,
- Správu státních hmotných rezerv,
- Státní úřad pro jadernou bezpečnost a
- Českou národní banku.

Věcně příslušná ministerstva a jiné ÚSÚ zajišťují veškeré potřebné informace a součinnost s MV-GŘ HZS ČR v této oblasti a zároveň připravují návrhy

odvětvových kritérií v rámci své působnosti (10). Stejně tak v rámci své působnosti vyžadují od provozovatelů potenciálních prvků KI informace nezbytné k určení těchto prvků, a to včetně údajů, u kterých je nutné zachovat mlčenlivost, pokud požadované informace nelze získat jiným způsobem. Zároveň určují opatřením obecné povahy prvky KI, jejichž provozovatelem není organizační složka státu a o tomto určení bez zbytečného odkladu informují MV-GŘ HZS ČR. Do kompetence těchto ministerstev a jiných ÚSÚ dále spadá oprávnění vykonávat kontrolu subjektů KI, a to zejména se zaměřením na plnění jejich povinností stanovených krizovým zákonem (10).

Neméně důležitou skupinou aktérů jsou subjekty KI, tedy její provozovatelé či vlastníci. Jejich role v systému a povinnosti, které musí plnit v souladu s krizovým zákonem a jeho prováděcími právními předpisy jsou uvedeny v podkapitole 3.2.7.

3.2.6 Proces identifikace a určování prvků kritické infrastruktury

Krizový zákon stanovil v případě procesu identifikace a určování prvků kritické infrastruktury dvojí způsob určování těchto prvků, přičemž tento proces se řídí podle toho, zda je subjektem kritické infrastruktury organizační složka státu či nikoliv (10).

Pojem organizační složka státu je definován *zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích*, a to tak, že se jedná o „*ministerstva a jiné správní úřady státu, Ústavní soud, soudy, státní zastupitelství, Nejvyšší kontrolní úřad, Kancelář prezidenta republiky, Úřad vlády České republiky, Kancelář Veřejného ochránce práv, Akademie věd České republiky, Grantová agentura České republiky a jiná zařízení, o kterých to stanoví zvláštní právní předpis anebo tento zákon; obdobné postavení jako organizační složka státu má Kancelář Poslanecké sněmovny a Kancelář Senátu*“ (13).

To, že je nějaký subjekt uvedený v definici organizační složkou státu samozřejmě neznamená, že se automaticky jedná o subjekt kritické infrastruktury. Rozdělení slouží zejména k vydefinování, jaký způsob určování bude použit u konkrétního prvku KI.

V případě prvků KI, jejichž provozovatelem je organizační složka státu, provádí určování těchto prvků vláda ČR, a to na základě Seznamu prvků KI, jejichž provozovatelem je organizační složka státu (dále jen „Seznam prvků KI"), který zpracovává MV-GŘ HZS ČR na základě podkladů předložených věcně příslušnými ministerstvy a jinými ÚSÚ (10).

Seznam prvků KI byl poprvé schválen usnesením vlády ze dne 14. prosince 2011 č. 934, přičemž jeho poslední (v pořadí osmá) aktualizace byla schválena usnesením vlády ze dne 21. prosince 2020 č. 1359. Aktualizace nemá ze zákona stanovenou periodičnost, ale probíhá zpravidla jedenkrát ročně. Výjimkou byl rok 2015, kdy byla z důvodu novelizace nařízení vlády o kritériích pro určení prvku kritické infrastruktury aktualizace provedena dvakrát, a také aktualizaci za rok 2020 stihla vláda projednat ještě v prosinci toho roku (většinou býval tento materiál zařazen na program jednání vlády počátkem následujícího kalendářního roku).

V rámci procesu určování jsou nejprve ze strany MV-GŘ HZS ČR oslovena všechna věcně příslušná ministerstva a jiné ÚSÚ, které následně zasílají návrhy pro určení nových prvků kritické infrastruktury, či změnu, nebo vyškrtnutí již stávajících prvků KI. Souhrnný Seznam prvků KI je poté postoupen k projednání Výboru pro civilní nouzové plánování a následně Bezpečnostní radě státu. Po tomto projednání je návrh předložen k projednání a schválení vládou ČR. Přehledy prvků a subjektů kritické infrastruktury po jednotlivých odvětvích za léta 2011 až 2020 je uveden v příloze 3.

V případě druhého způsobu, tedy určování prvků KI, jejichž provozovatelem není organizační složka státu, je celý proces více decentralizovaný, kdy

zodpovědnost za určování prvků mají věcně příslušná ministerstva a jiné ÚSÚ. Ty určují prvky KI postupem podle správního řádu, konkrétně opatřením obecné povahy, přičemž o tomto určení následně informují MV-GŘ HZS ČR, a to bez zbytečného odkladu (10).

Opatření obecné povahy je vydáváno v souladu se zákonem č. 500/2004 Sb., Správní řád, kdy dotčené ministerstvo a jiný ÚSÚ vyvěsí po dobu 15 dnů příslušný návrh opatření obecné povahy na své úřední desce na úředních deskách obecních úřadů v obcích, jejichž správních obvodů se má opatření obecné povahy týkat, a vyzve dotčené osoby, aby k tomuto návrhu podávaly připomínky. Po uplynutí této lhůty se na uvedených úředních deskách zveřejní konečný návrh opatření obecné povahy, který uplynutím doby 15 dnů nabývá účinnosti (14).

3.2.7 Subjekt kritické infrastruktury a jeho povinnosti

Subjektem KI se dle krizového zákona rozumí provozovatel prvku KI, přičemž jde-li o provozovatele prvku EKI, považuje se takový provozovatel za subjekt EKI (10). Tato definice je navázána na definici stanovenou ve Směrnici EKI, která však oproti národní úpravě pracuje s dvěma pojmy, a to vlastník/provozovatel EKI. Vlastníkem/provozovatelem EKI se následně rozumí subjekty odpovídající za investice do konkrétního prostředku, systému nebo jeho části, které jsou podle výše uvedené směrnice označeny za EKI, nebo se jedná o subjekty odpovídající za každodenní provoz těchto prostředků (11).

Rozdělení na vlastníka a provozovatele prvku KI má ve vztahu k národní legislativě význam zejména ve vazbě na zákon o kybernetické bezpečnosti. Ten ve vazbě na systém kritické infrastruktury definoval pojem KII, kterou se rozumí prvek nebo systém prvků KI v odvětví komunikační a informační systémy, v oblasti kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti dále

definuje správce a provozovatele informačního nebo komunikačního systému KII, přičemž správcem informačního nebo komunikačního systému KII se rozumí provozovatel prvku kritické infrastruktury, tedy subjekt kritické infrastruktury podle krizového zákona (15).

Povinnosti subjektu KI jsou uvedeny v krizovém zákoně, konkrétně jsou obsahem ustanovení § 29a, 29b a 29c. Subjekt KI je v tomto smyslu povinen vypracovat plán krizové připravenosti subjektu KI (dále jen „PKP subjektu KI“), a to do jednoho roku od určení prvku kritické infrastruktury. Účelem PKP subjektu KI je identifikace možných ohrožení funkce prvku KI a stanovení opatření na jeho ochranu. V případě že subjekt KI plní jinou veřejnoprávní povinnost, na jejímž základě zpracovává jinou plánovací, organizační nebo technickou dokumentaci, lze náležitosti PKP subjektu KI zapracovat do této dokumentace (10).

Další povinností je umožnění kontroly PKP subjektu KI a ochrany prvku KI věcně příslušnému ministerstvu nebo jinému ÚSÚ, a to včetně umožnění vstupu a vjezdu na pozemky a do prostorů, kde se tento prvek nachází.

Následuje povinnost subjektu KI určit styčného bezpečnostního zaměstnance. Jeho určení musí subjekt KI bez zbytečného odkladu oznámit věcně příslušnému ministerstvu nebo jinému ÚSÚ. Do doby určení styčného bezpečnostního zaměstnance plní jeho povinnosti sám subjekt KI (jeho statutární zástupce). Hlavním úkolem styčného bezpečnostního zaměstnance je poskytování součinnosti při plnění úkolů stanovených krizovým zákonem (10).

V neposlední řadě má subjekt KI ohlašovací povinnost, kdy musí věcně příslušnému ministerstvu nebo jinému ÚSÚ oznámit jakékoliv informace o organizační, výrobní nebo jiné změně, která může mít vliv na určení prvku KI (10).

3.2.8 Ochrana kritické infrastruktury

Ochranou kritické infrastruktury se, jak je již výše uvedeno, rozumí opatření zaměřená na snížení rizika narušení funkce prvku KI. V současné právní úpravě je za ochranu kritické infrastruktury zodpovědný jeho provozovatel, tedy subjekt KI, který v souladu s požadavky stanovenými v krizovém zákoně zpracovává PKP subjektu KI a určuje styčného bezpečnostního zaměstnance (viz podkapitola 3.2.7). Tímto však otázka ochrany kritické infrastruktury nekončí. Jak bylo také výše uvedeno, v současné právní úpravě je řešena pouze problematika ochrany kritické infrastruktury, kdy je opomíjen koncept její resilience. Ten je však ze strany subjektů KI řešen v rámci jejich snahy o zajištění kontinuity poskytování svých služeb.

Základní rámec ochrany je obsahem PKP subjektu KI, jehož náležitosti jsou stanoveny v nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 krizového zákona, přičemž jeho rozpracování je dále specifikováno v Metodice zpracování plánů krizové připravenosti podle § 17 až 18 výše uvedeného nařízení vlády.

V **základní části** PKP subjektu KI je zejména vymezení předmětu činnosti subjektu KI, důvody pro zpracování tohoto plánu, charakteristika krizového řízení subjektu KI včetně definování vazeb na příslušné orgány krizového řízení a krizové štáby, se kterými by subjekt KI spolupracoval, a v neposlední přehled hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost tohoto subjektu. Přehled možných zdrojů rizik a analýza ohrožení se zpracovává s využitím podkladů, které poskytne příslušný hasičský záchranný sbor kraje a dalších analýz, které si subjekt KI zpracuje ve své působnosti (16).

V **operativní části** PKP subjektu KI je řešen zejména způsob zabezpečení akceschopnosti subjektu KI včetně stanovení opatření určených na ochranu prvku KI, postupy řešení krizových situací, které byly identifikovány v analýze ohrožení, dále přehled spojení na příslušné orgány krizového řízení

a v neposlední řadě je v této části uveden přehled všech plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací (16).

V **pomocné části** je pak uveden přehled všech právních předpisů využitelných při přípravě na mimořádné události či krizové situace a jejich řešení, zásady manipulace s tímto plánem, geografické podklady a další dokumenty související s připraveností na mimořádné události či krizové situace (16).

Konkrétní náležitosti objektové, režimové, či kybernetické ochrany prvků KI jsou pro každé odvětví stanoveny ve specifických předpisech. Jedná se např. o právní předpisy, které stanovují konkrétní náležitosti ochrany prvků KI v konkrétním odvětví, kde lze uvést třeba oblast kybernetické bezpečnosti, jejíž ochrana je specifikována ve *vyhlášce Národního úřadu pro kybernetickou a informační bezpečnost č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat*, která je kromě náležitostí ochrany provozovatelů základních služeb a významným informačních systémů zaměřena i na ochranu KII, tedy kritické infrastruktury v oblasti kybernetické bezpečnosti. Další skupinou specifických předpisů jsou technické normy nebo přímo podnikové normy, jako např. *ČSN P 73 4450-1 Fyzická ochrana prvku kritické infrastruktury – Část 1: Obecné požadavky*, která je technickou normou, jež stanovuje obecné požadavky na systém fyzické ochrany prvků KI a je využívanou mj. v odvětví energetiky.

V současné době zároveň nabývá na významu nové pojetí ochrany kritické infrastruktury, které vychází z pojmu tzv. resilience, tedy odolnosti kritické infrastruktury.

Ta je determinována ve dvou oblastech, které lze charakterizovat jako technologickou a fyzickou ochranu prvků a management organizace, přičemž technologická a fyzická ochrana jednotlivých prvků je označována jako

technická resilience a je determinována robustností a obnovitelností jednotlivých prvků. Posilování této resilience je realizováno ve vztahu ke konkrétnímu prvku nebo skupině stejných či velmi podobných prvků. Například v elektroenergetice je robustnost a obnovitelnost zajišťována odlišnými způsoby a prostředky u zařízení pro výrobu elektrické energie a u zařízení pro jeho přenos či distribuci. Technická resilience je tvořena mírou robustnosti a obnovitelnosti jednotlivých prvků KI, přičemž u každého prvku jsou tyto komponenty technické resilience ovlivňovány třemi faktory, jimiž jsou technologická struktura prvku, bezpečnostní opatření prvku a nežádoucí události, kterými je resilience ovlivňována (1).

Naproti tomu management organizace je označován jako **organizační resilience** a její míra je určována úrovní vnitřních procesů organizace, které jsou nezbytné ve fázi adaptace prvků KI s použitím zkušeností získaných při likvidačních a obnovovacích pracích v minulosti (1).

Resilience kritické infrastruktury probíhá v rámci jednotlivých cyklů, přičemž prvním z těchto cyklů je prevence, kdy se prováděním preventivní činnosti provozovatel připravuje na budoucí nežádoucí události. Zde potom platí, že připravenost je výsledným stavem prevence. V okamžiku, kdy již dojde k působení negativních vlivů či událostí na kritickou infrastrukturu, přechází resilience z fáze prevence do fáze absorpce (1).

Absorpce začíná v okamžiku působení nežádoucích událostí a vlivů a je určována celkovou robustností prvku KI. Podstatou této robustnosti je poté schopnost prvku KI absorbovat působení nežádoucí události, aniž by došlo k výraznějším výkyvům či k přerušení poskytovaných služeb (1).

Po ukončení působení nežádoucích událostí nastává fáze obnovy, která je charakterizována schopností prvku KI obnovit svou činnost do původní, nebo alespoň minimálně požadované, úrovně výkonu. Délka fáze obnovy se odvíjí od

dostupných zdrojů využitelných pro navrácení se k požadovanému výkonu a času nutného pro realizaci jednotlivých procesů obnovy (1).

Poslední fází cyklu resilience kritické infrastruktury je fáze adaptace, kde se jedná se o schopnost organizace adaptovat provozovaný prvek KI na případné další opakování již proběhlé nežádoucí události. Adaptace tak představuje schopnost organizace adaptovat se na změněnou situaci. Adaptace je určována vnitřními procesy organizace souvisejícími s posilováním resilience, kdy se jedná o management rizik, inovační procesy a vzdělávací a rozvojové procesy. K posilování resilience však může docházet již ve fázi obnovy např. formou výměny komponent nebo úpravy procesů jejich fungování (1).

3.3 Možnosti dalšího rozvoje

V případě národního systému kritické infrastruktury je pro další vývoj stěžejním materiálem Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, která v rámci jedné ze svých pěti priorit stanovila další směřování a rozvoj problematiky kritické infrastruktury v ČR (6).

Ve vztahu ke kritické infrastruktuře tak byla v rámci dalšího rozvoje konstatována potřeba precizování systému ochrany kritické infrastruktury formou revize stanovených určujících kritérií a stanovení standardů ochrany prvků KI z hlediska objektové, technologické, personální či kybernetické bezpečnosti. Koncepce také reflektovala otázku provázanosti jednotlivých odvětví KI, prohloubení spolupráce se subjekty KI a výměnu informací mezi všemi zainteresovanými subjekty (6).

V rámci vymezeného období platnosti koncepce byly některé ze stanovených úkolů splněny. Zde se jedná především o revizi určujících kritérií, jež jsou uvedena v podkapitole 3.2.4. Ve věci provázanosti jednotlivých odvětví KI pak

bylo dosaženo dílčího posunu ve vazbě na problematiku identifikace a kategorizace strategických objektů, jejichž součástí je také kritická infrastruktura, která se přímo dotýká otázky provázanosti prvků kritické infrastruktury v odvětví energetiky s prvky kritické infrastruktury z ostatních odvětví KI. V rámci této činnosti byl Ministerstvem průmyslu a obchodu zpracován *Postup pro vytvoření seznamu strategických objektů a určení jejich priorit a pro definici scénářů výpadku dodávek elektrické energie* (dále jen „Postup"), jež byl schválen usnesením vlády ze dne 8. října 2019 č. 710. Uvedený materiál vychází z původně připravovaného *Národního programu energetické odolnosti*, jehož zpracování bylo jedním z úkolů *Státní energetické koncepce* z roku 2015. Cílem materiálu je vytvoření kategorizovaného seznamu strategických objektů na území ČR, který bude sloužit zejména provozovatelům distribučních soustav k prioritizaci vytipovaných strategických objektů v rámci jejich vypínacích plánů. Uvedený seznam bude zároveň součástí krizových plánů krajů (17).

Snaha o řešení některých úkolů stanovených v koncepci však poukázala na některé skutečnosti, jež významným způsobem ztěžují jejich realizaci. Zde se jedná především o úkol týkající se stanovení jednotných a závazných standardů ochrany prvků KI, který je v současné době v podstatě nerealizovatelný, neboť rozdíly mezi prvky KI v jednotlivých odvětvích jsou natolik rozsáhlé, že je stanovení jednotných standardů pro všechna odvětví KI velice obtížné (6).

Systém kritické infrastruktury také podléhá vývoji této problematiky na evropské úrovni, kde jsou již od roku 2018 patrné výrazné snahy o revizi fungování celého systému, které se vztahují k výše uvedené Směrnici EKI. Vzhledem k tomu, že od přijetí směrnice v roce 2008 nedošlo k žádným výrazným změnám v systému EKI, byl zahájen proces její revize. V roce 2018 byla zahájena veřejná konzultace k hodnocení fungování aktuálně platné Směrnice EKI, jejímž prostřednictvím si Evropská komise vyžádala od všech zainteresovaných subjektů hodnocení současného stavu. Na základě této

konzultace bylo v červenci 2019 Evropskou komisí vydáno hodnocení této směrnice a navržena doporučení, která by vedla k posílení a zefektivnění systému EKI napříč všemi členskými státy EU (18).

Poslední vývoj v této oblasti nastal na konci roku 2020, kdy byl v návaznosti na vydaná doporučení představen nový návrh *směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů* (dále jen „Směrnice CER"). Návrh směrnice přináší několik zásadních změn, které v případě, že dojde k přijetí této směrnice, mohou mít výrazný dopad na podobu systému kritické infrastruktury nejen v ČR, ale i v dalších evropských státech.

Nejviditelnější změnou je zejména rozšíření počtu odvětví řešených na evropské úrovni z původních dvou (energetika a doprava) na nově navrhovaných deset. Jedná se tak o odvětví energetiky, dopravy, bankovnictví, infrastruktury finančního trhu, zdravotnictví, pitné vody, odpadového hospodářství, digitální infrastruktury, veřejné správy a vesmíru. Kromě změny rozsahu je významnou navrhovanou změnou také zavedení nového chápání kritické infrastruktury, kdy by měl být nově kladen důraz na určování tzv. kritických subjektů, které poskytují základní služby. Nejedná se tak o určování jednotlivých prvků ve smyslu objektů, ale o identifikaci základních služeb a subjektů, které je poskytují. V tomto pojetí tak návrh Směrnice CER přímo navazuje na *směrnici Evropského parlamentu a Rady 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*, která je v současné době rovněž revidována. Kromě těchto úprav je také zásadním bodem návrhu Směrnice CER definování resilience v rámci systému ochrany kritické infrastruktury spolu se stanovením nových povinností pro členské státy a kritické subjekty, jejichž účelem je právě posílení resilience infrastruktury kritických subjektů (19). Finální podoba směrnice však ještě bude předmětem jednání mezi Evropskou komisí a členskými státy a případné změny by se národního pojetí dotkly až v příštích letech.

4 METODIKA

V diplomové práci budou použity dvě metody pro hodnocení současného systému ochrany kritické infrastruktury. Systém kritické infrastruktury bude jednak analyzován pomocí SWOT analýzy a následně bude pomocí komparativní metody srovnán se systémy kritické infrastruktury Slovenska a Finska, přičemž důvod výběru těchto dvou států bude blíže uveden v podkapitole 4.5.

4.1 SWOT analýza

První metodou použitou v této práci použita je SWOT analýza, tedy analýza silných stránek (Strengths), slabých stránek (Weaknesses), příležitostí (Opportunities) a hrozeb (Threats). Jedná se o analytickou metodu, jež primárně používána při analýzách na strategické úrovni (ale dá se použít i v rámci taktického a operačního řízení) a v základu spočívá v identifikaci výše uvedených silných a slabých stránek systému jeho příležitostí a hrozeb, přičemž takto identifikované klíčové faktory jsou poté slovně charakterizovány či případně ohodnoceny (20).

Pomocí SWOT analýzy je systém hodnocen jak z pohledu jeho vnitřního fungování a procesů, které jeho sílu a robustnost určují, tak i z pohledu vnějších faktorů, které mají na systém pozitivní či naopak negativní vliv, respektive mohou svou existencí vést ke zlepšení současného stavu systému, nebo naopak mohou tento systém ohrozit. Z pohledu vnitřních procesů se tak hodnotí výše uvedené silné a slabé stránky systému, kdežto vnější vlivy jsou hodnoceny v rámci kategorií příležitosti a hrozby.

Ač se v jádru jedná o vcelku jednoduchý analytický nástroj je v případě SWOT analýzy potřeba dodržet několik základních zásad, které zaručí relevantnost

a využitelnost provedené SWOT analýzy. Zaprvé by měla být SWOT analýza zaměřena pouze na podstatná fakta a jevy, to znamená, že po identifikaci všech jevů souvisejících s fungováním systému by měla být provedena jejich redukce pouze na ty nejzásadnější jevy. Důvodem je fakt, že příliš velké množství identifikovaných jevů významným způsobem redukuje využitelnost analýzy při formulování vhodných opatření k posílení hodnoceného systému (20). Zároveň by identifikované jevy a jejich řešení měly svým významem odrážet úroveň, pro kterou byla SWOT analýza zpracována, to znamená, že pokud byla SWOT analýza prováděna na strategické úrovni, měly by problémy a s tím korespondující řešení být také strategického významu.

V neposlední řadě je podstatné u SWOT analýzy zajistit objektivitu výsledků a analýza by tak neměla pouze vyjadřovat subjektivní názory zpracovatele analýzy ale objektivně popisovat vlastnosti systému. V tomto ohledu je tak vhodné poskytnout prvotní návrh analýzy k posouzení dalším expertům na uvedenou problematiku a jejich připomínky a návrhy v konečném návrhu analýzy zohlednit. Alternativním postupem je provedení identifikace všech jevů v rámci expertní skupiny tzv. metodou brainstormingu (20).

4.2 Paretovo pravidlo

V kontextu této diplomové práce je selekce identifikovaných významných jevů zajištěna pomocí tzv. Paretova principu, které je taktéž známé jako pravidlo 80/20. Toto pravidlo spočívá ve skutečnosti, že 80 % důsledků pramení z 20 % příčin, přičemž tento princip lze nalézt v mnoha odlišných oblastech. V kontextu SWOT analýzy toto pravidlo znamená, že identifikací nejvýznamnějších příčin, v tomto případě identifikovaných jevů, jsme schopni cílit na 80 % všech důsledků, které se s těmito příčinami pojí (21).

4.3 Metoda AHP

K samotné identifikaci těch nejvýznamnějších jevů byla použita metoda tzv. párového porovnávání, kdy jsou jednotlivé identifikované jevy mezi sebou vzájemně porovnávány. Pro tuto diplomovou práci byla zvolena metoda AHP, která se také nazývá jako tzv. Saatyho metoda. Jedná se o metodu, která se používá k vícekriteriálnímu hodnocení kritérií a možných variant. V tomto případě jsou kritéria, tedy jevy, identifikovaná ve SWOT analýze párově porovnávána mezi sebou, kdy cílem je mezi jednotlivými jevy určit preference. Výhodou metody AHP je to, že umožňuje u každého párového porovnání dvou jevů stanovit tzv. váhu těchto jevů, tedy v jaké míře je jeden jev významnější než jev druhý, a to na hodnotící škále 1 až 9. Přehled použitých vah a jejich význam je uveden v tabulce 1. Výslednou hodnotou jsou geometrické průměry jednotlivých jevů a výsledné váhy těchto prvků, přičemž pro ověření správnosti výpočtu musí být výsledná hodnota součtu všech geometrických průměrů rovna číslu 1 (22).

Tabulka 1 - přehled použitých vah (22)

Body	Popis významnosti
1	Kritéria jsou stejně významná
2	Kritérium je velmi slabě významnější než druhé
3	Kritérium je slabě významnější než druhé
4	Kritérium je docela o dost významnější než druhé
5	Kritérium je o dost významnější než druhé
6	Kritérium je téměř prokazatelně významnější jak druhé
7	Kritérium je prokazatelně významnější jak druhé
8	Kritérium je o hodně významnější než druhé
9	Kritérium je podstatně významnější než druhé

Finálním krokem je ověření konzistentnosti provedeného párového porovnání. U stanovování významnosti jednotlivých jevů totiž může dojít k situaci, kdy u většího počtu hodnocených jevů mohou být jednotlivé jevy porovnávány odlišným způsobem, resp. přidělení jednotlivých vah nemusí být

konzistentní. Nejjednodušším příkladem je situace, kdy jevu A je přidělena váha významnosti 4 oproti jevu B, následně je jevu B přidělena váha významnosti 2 oproti jevu C, ale při porovnávání jevu A s jevem C je jevu A přidělena váha významnosti pouze v hodnotě 1. To vede k situaci, kdy je jev A významnější než jev B a mírně významnější než jev C, nicméně jev B je zároveň významnější než jev C.

Tato nekonzistentnost se dá celkem snadno odhalit v případě nízkých počtů hodnocených jevů, ale v případě, většího počtu jevů už je posouzení konzistentnosti obtížné. Proto k jeho ověření slouží tzv. konzistenční poměr, který by měl mít hodnotu menší než 0,1 (22).

Jelikož k výpočtu konzistenčního poměru je nutné znát maximální vlastní číslo matice, je potřeba k ověření použít speciální software. K ověření konzistentnosti v této práci tak je použit program MCA7.

Tento program je k dispozici volně ke stažení a slouží k provádění multikriteriální analýzy a dále k provedení výpočtu vah metodou Fullerova trojúhelníku a Saatyho metodou, přičemž součástí propočtu Saatyho metody je zároveň ověření konzistentnosti (23).

Po tomto párovém porovnání jsou identifikované jevy seřazeny podle jejich významnosti. Aplikací Paretova pravidla jsou následně vyselektovány ty jevy, které systém kritické infrastruktury ovlivňují nejvíce. Konkrétně se číselné ohodnocení jednotlivých jevů převede na procentuální vyjádření podílu celkového podílu v dané kategorii. Následně budou procentuální kumulací identifikovány nejvýznamnější jevy, které souhrnně tvoří 80 % podíl v dané kategorii.

4.4 Komparativní metoda

Ke zhodnocení systému kritické infrastruktury a identifikování slabých stránek a adekvátních opatření využitelných ke zlepšení současného stavu tohoto systému bude využita metoda komparace, tedy srovnávání, kdy v tomto případě se bude jednat o komparativní případovou studii, kdy na jedné straně je případ systém kritické infrastruktury v ČR, který bude komparován se systémy kritické infrastruktury jiných států.

V rámci komparace bude využita analytická metoda, tedy princip hodnocení systému jako celku skrze identifikaci a hodnocení jeho jednotlivých částí. Analýza tak umožňuje odhalit různé vlastnosti jevů a procesů, oddělovat podstatné od nepodstatného či odlišit trvalé vztahy a vazby od nahodilých tendencí (24).

Při komparaci bude v případě systému kritické infrastruktury v ČR vycházeno především z kapitoly č. 3. Komparace bude prováděna v následujících oblastech:

- právní ukotvení,
- definice,
- kompetence aktérů,
- určující kritéria,
- identifikace a určování kritické infrastruktury,
- ochrana kritické infrastruktury,
- kontrola plnění opatření.

Systém kritické infrastruktury v ČR bude komparován se dvěma jinými systémy kritické infrastruktury, a to konkrétně Slovenské republiky a Finské republiky. Důvodem výběru těchto dvou systému je především několik

společných znaků, které všechny systémy vykazují. Zde se jedná především o skutečnost, že všechny tři státy jsou členskými státy Evropské unie, a tudíž jejich systémy kritické infrastruktury jsou stejnou měrou regulovány směrnicí EKI a budou stejným způsobem regulovány případnou novou Směrnicí CER. V případě Slovenska se dále jedná o geograficky i kulturně blízký stát s podobnou právní praxí. V případě Finska se naopak jedná o stát se specifickým přístupem k této problematice, který je charakteristický úzkou spoluprací mezi veřejným a soukromým sektorem.

5. VÝSLEDKY

Cílem této kapitoly je zejména provedení analýzy v souladu s metodikou uvedenou v předchozí kapitole. Nejprve je hodnocen systém kritické infrastruktury v ČR pomocí SWOT analýzy, přičemž jednotlivé identifikované jevy jsou následně hodnoceny pomocí metody AHP a následně z nich jsou s využitím Paretova pravidla vyselektovány ty nejzásadnější jevy, které jsou na konci této kapitoly použity k navržení možných zlepšení celého systému.

Před navržením vhodných opatření ke zlepšení současného stavu však je ještě systém kritické infrastruktury v ČR porovnán se systémy ochrany kritické infrastruktury Slovenska a Finska.

5.1 Hodnocení Systému kritické infrastruktury v ČR (SWOT analýza)

V následující části práce jsou nejprve představeny v rámci čtyř podkapitol jednotlivé identifikované jevy týkající se silných a slabých stránek, příležitostí a hrozeb. U každého jevu je uvedeno vysvětlení o jeho zařazení do konkrétní kategorie. Po identifikaci všech jevů je v další podkapitole provedeno jejich hodnocení, které má za úkol identifikovat ty nejvýznamnější jevy, které mají vliv na současný systém kritické infrastruktury v ČR a jejichž řešení či využití může vést ke zlepšení současného stavu.

V tabulce 2 jsou uvedeny závěry z provedené SWOT analýzy systému kritické infrastruktury v ČR.

Tabulka 2 - SWOT analýza „Systém kritické infrastruktury v ČR“ [zdroj vlastní]

SILNÉ STRÁNKY	SLABÉ STRÁNKY
- Legislativní ukotvení systému KI - Jednoznačně stanovené gesce a role všech aktérů - Systém identifikace a určování prvků KI - Stanovení odbornosti styčných bezpečnostních zaměstnanců - Provázání systému KI se systémem krizového řízení - Připravenost na krizové situace pomocí plánovací dokumentace - Aktivní přístup na evropské úrovni - Řešení systému KI na strategické úrovni	- Decentralizace systému v případě nestátních prvků KI - Špatně nastavená kritéria pro určování prvků KI - Absence sankcí - Neexistence standardů ochrany - Vzdělávání styčných bezpečnostních zaměstnanců - Zaměření pouze na ochranu - Absence komunikačních nástrojů pro spolupráci se subjekty KI - Nedostatečná ochrana informací o KI
PŘÍLEŽITOSTI	**HROZBY**
- Nové přístupy - Nové technologie - Nové hrozby - Příznivá změna evropské legislativy - Možnosti financování z ISF či jiných fondů - Zapojení akademického sektoru - Rozšíření odvětví KI	- Nepodchycení všech relevantních odvětví - Nepříznivá změna evropské legislativy - Odsunutí problematiky na okraj zájmu - Tendenční přístup k řešení ochrany KI - Populistické či neodborné zásahy do systému - Výskyt domino a kaskádových efektů

5.1.1 Silné stránky

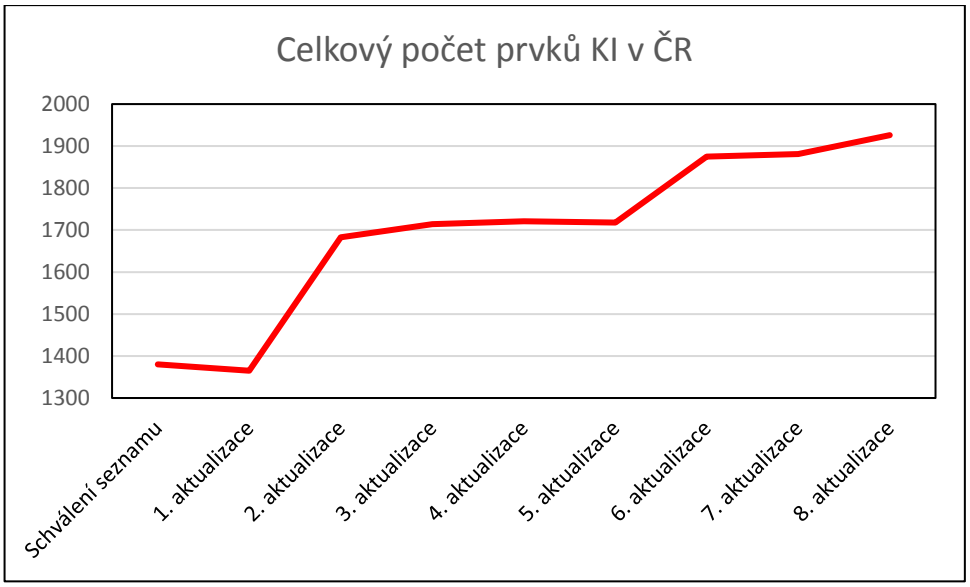
Legislativní ukotvení systému kritické infrastruktury (S1) – systém kritické infrastruktury je v současné době legislativně ukotven v rámci právního řádu ČR spolu s jednoznačně stanovenými kompetencemi a povinnostmi všech věcně

příslušných aktérů včetně zákonem stanovených úkolů, které se musí v souladu se zákonem plnit. V tomto smyslu je tak legislativní ukotvení silnou stránkou, neboť neumožňuje všem dotčeným subjektům konat v rozporu s tím, co je zákonem stanoveno.

Jednoznačně stanovené gesce a role všech aktérů (S2) – systém kritické infrastruktury má stanoveného gestora a spolugestory za tuto problematiku, která je vymezená zákonem. Hlavní gesci, koordinační roli a roli kontaktního bodu pro oblast EKI zastává MV-GŘ HZS ČR. Spolugesci za celý systém a gesci v rámci jednotlivých odvětví zastávají věcně příslušná ministerstva a jiné ÚSÚ, a to po podle působnosti stanové kompetenčním zákonem či jinými specifickými právními předpisy upravujícími působnost orgánů státní správy.

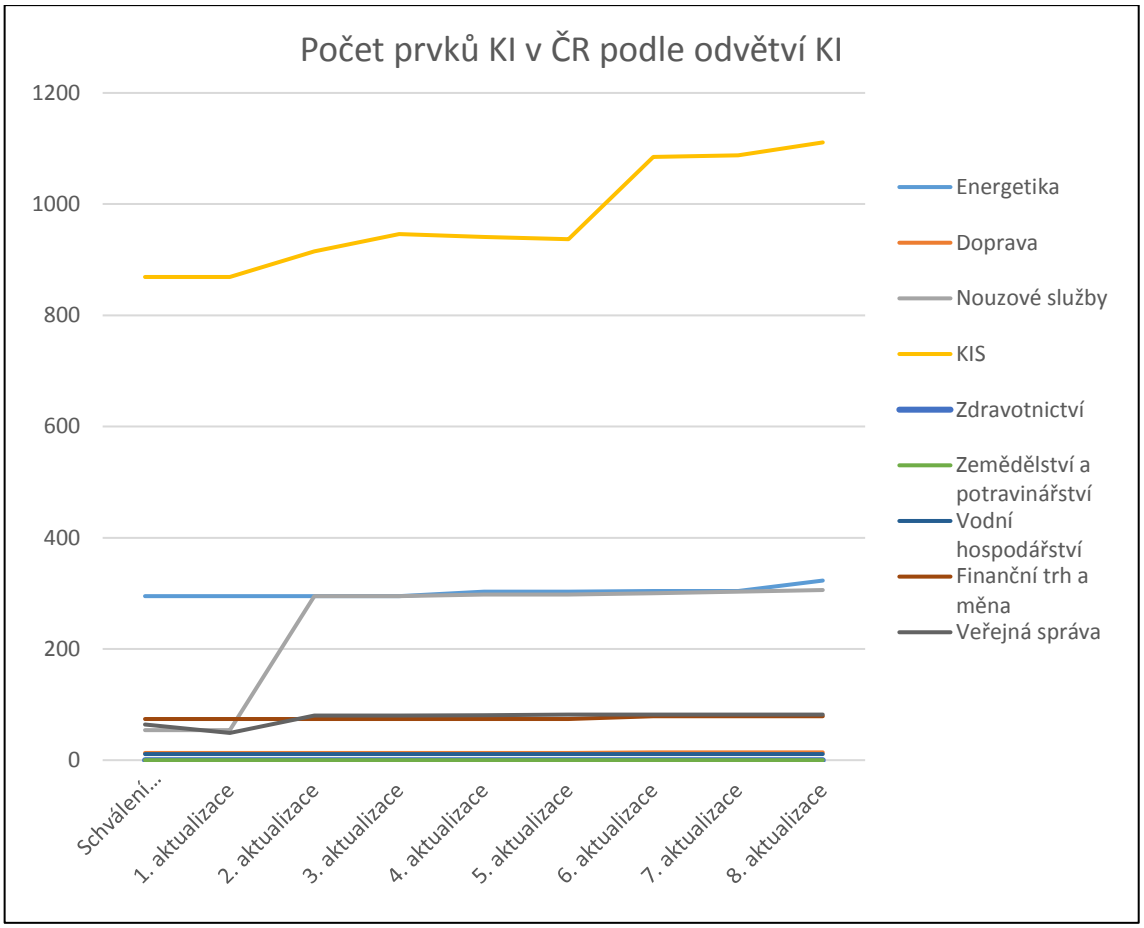
Systém identifikace a určování prvků KI (S3) – určování prvků KI probíhá po dvou liniích, jenž se liší podle toho, zda se v případě jeho provozovatele jedná o organizační složku státu či nikoliv. V případně organizačních složek státu probíhá určování zpravidla v pravidelných ročních cyklech[1] a relevantnost seznamu všech těchto prvků je během tohoto procesu posuzována Výborem pro civilní nouzové plánování, Bezpečnostní radou státu a vládou ČR. Od přijetí novely v roce 2011 bylo provedeno celkem osm aktualizací Seznamu prvku kritické infrastruktury, jejichž provozovatelem je organizační složka státu a souběžně s tím byla přijímána opatření obecné povahy gestory za jednotlivá odvětví. Od přijetí novely lze pozorovat kontinuální nárůst celkového počtu prvků KI se skokovým navýšením v roce 2015. Tento vývoj je znázorněn na grafu, viz obrázek 1.

[1] S výjimkou roku 2015, kdy došlo vlivem novelizace nařízení vlády o kritériích pro určení prvku kritické infrastruktury ke dvěma aktualizacím.



Obrázek 1 - počet prvků KI v ČR od roku 2011 [Zdroj MV-GŘ HZS ČR]

Tento kontinuální nárůst počtu určených prvků KI však není přítomný u všech definovaných odvětví KI, jak lze pozorovat na grafu viz obrázek 2. Určování nových prvků KI tak nejčastěji proběhlo zejména v odvětvích energetika (nárůst oproti roku 2011 je o celkem 28 prvků KI), nouzové služby (nárůst o 252 prvků KI) a komunikační a informační systémy (nárůst o 247 prvků KI). Stagnaci v některých odvětvích KI v případě identifikace a určování nových prvků KI lze pak přičíst jednak specifické povaze každého odvětví, kde neprobíhají časté změny samotných prvků KI, jako například v případě vodního hospodářství, kde jsou určeny především významná vodní díla, ale pak také nastavení určujících kritérií, jež jsou v jednotlivých odvětvích nastavena rozdílným způsobem.



Obrázek 2 - počet prvků KI v ČR od roku 2011 po odvětvích [Zdroj MV-GŘ HZS ČR]

Stanovení odbornosti styčných bezpečnostních zaměstnanců (S4) – v současné době jsou zákonem o krizovém řízení stanoveny podmínky pro výkon funkce styčného bezpečnostního zaměstnance, které zajišťují, že tuto funkci bude vykonávat osoba, která má vysokoškolské vzdělání v oblasti zajišťování bezpečnosti ČR, ochrany obyvatelstva nebo v oblasti krizového řízení, nebo má alespoň v jedné z těchto oblastí tříletou praxi.

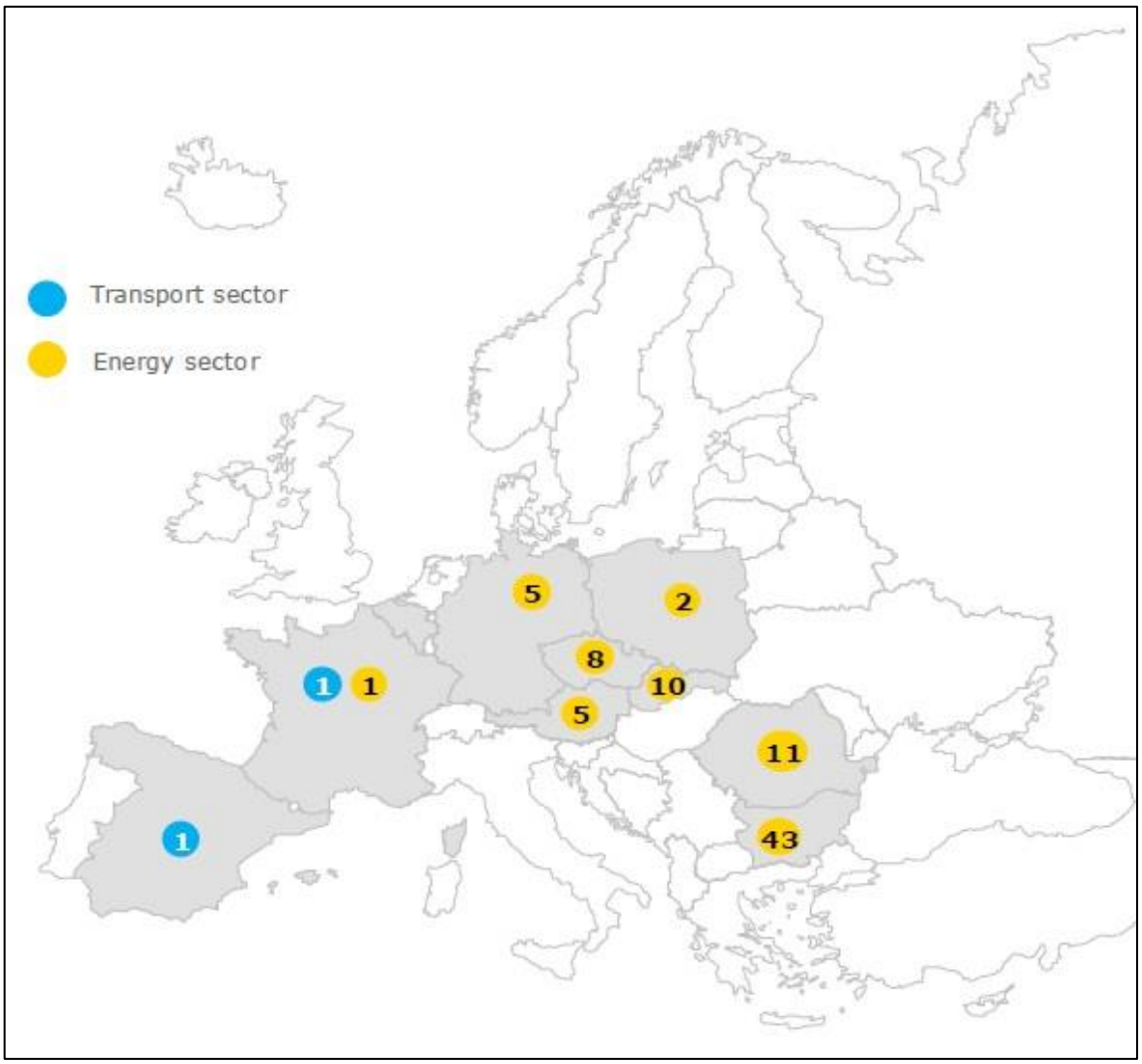
Provázání systému kritické infrastruktury se systémem krizového řízení (S5) – je umožněno implementací problematiky v rámci zákona o krizovém řízení. V tomto kontextu se jedná zejména o zahrnutí narušení kritické infrastruktury do situací, jež mohou vést k vyhlášení některého z krizových

stavů, dále provázání kritické infrastruktury s krizovými opatřeními zejména ve vztahu k přednostnímu zásobování a také stanovení povinnosti zpracovávat krizovou plánovací dokumentaci, jejíž struktura vychází z dokumentace zpracovávané právnickými či podnikajícími fyzickými osoby v případě že zajišťují plnění opatření vyplývajících z krizového plánu.

Připravenost na krizové situace pomocí plánovací dokumentace (S6) – jedná se především o povinnost subjektů KI zpracovat PKP subjektu KI do jednoho roku od určení prvku KI, což přispívá ke zvýšení připravenosti subjektu KI na řešení mimořádných událostí či krizových situací, které by mohly vést k narušení funkce prvku KI, stejně tak ke zvýšení schopnosti reakce tohoto subjektu na nastalou mimořádnou událost či krizovou situaci stanovením konkrétních opatření směřujících k obnovení funkce prvku KI v případě jeho narušení.

Aktivní přístup na evropské úrovni (S7) – ČR se zapojila do řešení problematiky kritické infrastruktury na úrovni EU, a to především skrze efektivní implementaci Směrnice EKI, pomocí které došlo na území ČR k určení osmi prvků EKI z odvětví energetiky. V tomto ohledu je tak ČR jednou z mála zemí EU, kde byl záměr Směrnice EKI naplněn, a to zejména ve vazbě na implementaci Směrnice EKI v jiných členských státech, kde byla tato implementace provedena pouze na papíře a reálně nevedla k žádnému určení prvků EKI v těchto státech. Tento stav je dokreslen na obrázku 3, kde je patrný výrazný nepoměr mezi členskými státy západní Evropy a členskými státy střední a východní Evropy. Kromě toho ČR skrze činnost svého kontaktního místa v rámci EKI podává zprávy Evropské komisi o plnění úkolů stanovených ve Směrnici EKI. Zde se jedná zejména o podávání zpráv o určených prvcích EKI a o souhrnnou zprávu se všeobecnými údaji o typech zranitelnosti, hrozbách a rizicích zjištěných v jednotlivých odvětvích (10). Zároveň se aktivně účastní pravidelných jednání pracovní skupiny kontaktních bodů pro EKI, jíž předsedá

zástupce Evropské komise, konkrétně zástupce z Generálního ředitelství pro migraci a vnitřní věci.



Obrázek 3 - Počet určených prvků EKI v členských státech EU (18).

Řešení systému kritické infrastruktury na strategické úrovni (S8) – problematika kritické infrastruktury je řešena a dále rozvíjena pomocí strategických materiálů, a to jak těch základních – tedy Bezpečnostní strategií ČR, tak i koncepčními dokumenty, kdy se v tomto případě jedná o Koncepci ochrany obyvatelstva do roku 2020 s výhledem do roku 2030, kterou je oblast kritické infrastruktury vymezena jako jedna z pěti priorit a spolu se systémem

krizového řízení je dále rozvíjena. Plnění úkolů a opatření koncepce je průběžně vyhodnocováno zprávami o stavu ochrany obyvatelstva v ČR (poslední je z roku 2018).

5.1.2 Slabé stránky

Decentralizace systému v případě nestátních prvků KI (W1) – v případě určování prvků KI, jejichž provozovatelem není organizační složka státu, probíhá určování pomocí opatření obecné povahy, které vydávají jednotlivá věcně příslušná ministerstva nebo jiné ÚSÚ, přičemž MV-GŘ HZS ČR, je o tomto určení pouze bez zbytečného odkladu pouze informováno. V případě tohoto určování tak neexistuje žádný mechanismus kontroly určování prvků KI, jako v případě státních prvků, které jsou při určování posuzovány Výborem pro civilní nouzové plánování a Bezpečnostní radou státu.

Špatně nastavená kritéria pro určování prvků KI (W2) – u odvětvových kritérií existují výrazné rozdíly v konkrétních hodnotách u odvětví KI. To má za následek situaci, kdy jsou v rámci některých odvětví určovány prvky KI, které mají pouze regionální význam a na druhé straně jsou odvětví, u kterých nedošlo k určení žádných prvků KI. Zde se jedná zejména o nedostatečně řešené odvětví zdravotnictví a zemědělství a potravinářství, kde jsou stanovená kritéria nastavena takovým způsobem, že je nesplňuje žádná infrastruktura tohoto typu v ČR. Naproti tomu v odvětví nouzových služeb jsou určovány jednotlivé stanice HZS ČR, které však mohou ve většině případů být pouze regionálního významu.

Absence sankcí (W3) – v krizovém zákoně jsou řešeny sankce, respektive přestupky, fyzických osob a přestupky podnikajících fyzických osob a právnických osob, které se však netýkají ustanovení souvisejících s povinnostmi v oblasti ochrany kritické infrastruktury. V současné době tak sice probíhají dle krizového zákona kontroly subjektů KI z pohledu plnění jejich

povinností stanovených v tomto zákoně, ale jakákoliv vymahatelnost zákonem stanovených požadavků je nemožná, neboť za jejich nesplnění nehrozí žádný postih.

Neexistence specifických standardů ochrany (W4) – v současné době je otázka ochrany prvku KI plně v kompetenci subjektu KI, neboť dle krizového zákona subjekt KI odpovídá za ochranu provozovaných prvků KI. Ačkoliv zákon stanovuje pro subjekty povinnost zpracovat PKP subjektu KI či určit styčného bezpečnostního zaměstnance, konkrétní náležitosti ochrany jednotlivých prvků (nebo jednotlivých částí prvků) KI stanoveny nejsou. Nelze tak v současné době jednoznačně určit, zda je ochrana konkrétního prvku KI řešena dostatečně či nikoliv, resp. zdali určení prvku KI vede k posílení jeho ochrany oproti jiné infrastruktuře obdobného typu, jež kritéria pro určení nenaplňuje. Posuzování míry ochrany je tak na zodpovědnosti jednotlivých ministerstev a ÚSÚ.

Vzdělávání styčných bezpečnostních zaměstnanců (W5) – v současné době jsou stanoveny podmínky pro výkon činnosti styčných bezpečnostních zaměstnanců, ale již neexistuje mechanismus k prověřování jejich reálných znalostí v oblasti ochrany obyvatelstva, krizového řízení či zajišťování bezpečnosti ČR ani systém jejich průběžného vzdělávání či školení pro potřeby kooperace a koordinace s orgány krizového řízení, přičemž pracovníci orgánů krizového řízení řešící problematiku krizového řízení způsob průběžného školení a prověření jejich znalostí nastavený mají.

Ochrana kritické infrastruktury je zaměřena pouze na ochranu (W6) – současná právní úprava je zaměřena pouze na ochranu kritické infrastruktury a řeší se pouze otázka připravenosti a reakce na nastalou mimořádnou událost či krizovou situaci spolu s obnovou provozu do původního stavu. Není však již řešena otázka posilování odolnosti jednotlivých prvků, tedy schopnosti odolat

působící mimořádné události či krizové situace bez nutnosti vynakládání velkého množství prostředků na návrat do původního stavu.

Absence komunikačních nástrojů pro spolupráci se subjekty KI (W7) – neexistence platformy či mechanismu pro koordinaci či kooperaci se subjekty kritické infrastruktury a orgány státní správy v oblasti kritické infrastruktury. Komunikace probíhá odděleně v rámci jednotlivých odvětví a na různé úrovni bez koordinace gestora.

Nedostatečná ochrana informací o kritické infrastruktuře (W8) – v současné době není k informacím o prvcích KI a jejich subjektech přistupováno jako k utajovaným informacím. Informace jsou považovány za neveřejné, nicméně jejich ochrana není nijak legislativně či nelegislativně upravena a jednotliví gestoři k ochraně informací přistupují rozdílným způsobem. V tomto kontextu je využíván mimo jiné institut zvláštních skutečností podle krizového zákona, kterým někteří gestoři chrání konkrétnější a citlivější údaje o kritické infrastruktuře a s ostatními orgány státní správy poté sdílejí pouze údaje nezbytné k plnění povinností stanovených krizovým zákonem. Neutajovanost informací o kritické infrastruktuře se poté nejvíce projevuje zejména v případě žádostí o poskytnutí informací podle *zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů*.

5.1.3 Příležitosti

Nové přístupy (O1) – aplikace nových přístupů k řešení identifikace a určování nových prvků KI, nebo v oblasti ochrany prvků KI. Patří zde mj. otázka rozšíření ochrany jednotlivých prvků KI i na řešení problematiky ochrany dodavatelských řetězců těchto subjektů, hodnocení či mapování vzájemných závislostí aj.

Nové technologie (O2) – výskyt či aplikace nových technologií jak v oblasti ochrany jednotlivých prvků KI na úrovni subjektů KI, tak také na úrovni technologií, které využívají gestoři za jednotlivá odvětví v oblasti sběru či sdílení dat o kritické infrastruktuře, či v oblasti nových komunikačních nástrojů využitelných pro koordinaci činností se subjekty KI, dalšími gestory za jednotlivá odvětví či s dalšími aktéry státní správy či samosprávy.

Nové hrozby (O3) – výskyt nových hrozeb, které mohou vést k rozšíření ochrany kritické infrastruktury v nových, dosud neřešených oblastech, a tím umožnit celkový rozvoj problematiky.

Příznivá změna evropské legislativy (O4) – změna legislativy na úrovni EU formou přijetí nové směrnice nebo novelizace té stávající, která umožní prosadit rozsáhlejší změny v systému kritické infrastruktury jednotlivých členských států a přinese aplikaci nových postupů či směrů.

Možnosti financování z ISF či jiných fondů (O5) – v současné době je otázka financování opatření na zajištění ochrany určených prvků KI ponechána dle krizového zákona v kompetenci samotných subjektů KI, kteří dle tohoto zákona zajišťují ochranu prvků KI, které provozují. K posílení systému kritické infrastruktury by tak mohlo přispět financování i z jiných zdrojů. Zde se především nabízí finanční prostředky z evropských fondů, využitelným by v této věci mohl být např. fond pro vnitřní bezpečnost (dále jen „ISF“). Jedním z cílů ISF je zlepšování schopností řízení rizik a krizí, a to skrze posilování kapacit členských státu EU ke zvládání bezpečnostních rizik ve vztahu k přípravě na ochranu obyvatelstva ochranu kritických infrastruktur proti teroristickým útokům či jiným s bezpečností souvisejícím událostem (25). Zároveň lze do této příležitosti zahrnout financování opatření, které souvisí s možným přijetím nové

Směrnice CER, jejímž cílem je zavedení nových povinnosti pro členské státy i pro kritické subjekty (19).

Zapojení akademického sektoru (O6) – zapojení akademického sektoru do úpravy systému kritické infrastruktury, a to formou přímého podílení se na přípravě změn stávajícího systému nebo formou podpory bezpečnostního výzkumu v této oblasti.

Rozšíření odvětví kritické infrastruktury (O7) – rozšíření stávajících odvětví či pododvětví KI o nové oblasti, které jsou řešeny v systémech jiných zemí. Jedná se například o odvětví odpadového hospodářství, či o odvětví spojené s vězeňstvím a zajištěním veřejného pořádku.

5.1.4 Hrozby

Nepodchycení všech relevantních odvětví (T1) – výskyt stávajících či nových potenciálních odvětví KI, která nejsou v současné době v systému řešena, a jejichž narušení může mít významný dopad na bezpečnost těchto prvků a s tím související bezpečnost ČR.

Nepříznivá změna evropské legislativy (T2) – taková změna legislativy řešící problematiku KI, která by výrazným způsobem narušovala národní přístup k ochraně kritické infrastruktury, případně by vedla ke značnému administrativnímu nebo finančnímu zatížení orgánů řešících tuto problematiku či subjektů KI, které by nevedlo k úměrnému posílení ochrany kritické infrastruktury.

Odsunutí problematiky na okraj zájmu (T3) – situace, kdy se problematika kritické infrastruktury dostane na okraj politického a odborného zájmu a vývoj jejího řešení tak ustrne a nebude dále rozvíjen o nové postupy a přístupy.

Tendenční přístup k řešení ochrany kritické infrastruktury (T4) – zaměření pouze na některé oblasti systému kritické infrastruktury a přehlížení jiných oblastí, které však mají neméně důležitý význam pro komplexní řešení této problematiky.

Populistické či neodborné zásahy do systému (T5) – necitlivé zásahy do systému kritické infrastruktury bez předchozí znalosti problematiky za účelem zisku politických bodů nebo s cílem rychlého a razantního řešení problému. Z nedávné doby lze například uvést situaci, kdy bylo během první vlny onemocnění COVID-19 vládou ČR vydáno usnesení ze dne 30. března 2020 č. 332, které definovalo tzv. kritické zaměstnance, jako zaměstnance, kteří se v rámci plnění svých pracovních úkolů podílejí na zajištění funkce prvku KI a stanovilo jim specifické povinnosti a omezení. Toto opatření tak mj. zakazovalo čerpání dovolené, či omezovalo pohyb těchto zaměstnanců mimo své bydliště a zaměstnání (26). To však vedlo k situaci, kdy se uvedené povinnosti týkaly i zaměstnanců, u kterých bylo zavedení těchto povinností zbytečné či kontraproduktivní (27). Následně tak muselo být vydáno nové usnesení vlády ze dne 1. dubna 2020 č. 377, které pravomoc určit kritické zaměstnance, na které se dotčené povinnosti vztahovaly, stanovilo samotným subjektům KI (28).

Výskyt domino a kaskádových efektů (T6) – efekt, kdy narušení jedné infrastruktury vede k následnému narušení dalších infrastruktur, které jsou na této prvotní infrastruktuře závislé. V tomto kontextu se pak jedná o hrozbu vzniku těchto efektů v případě infrastruktury, která v současné době není řešena

v systému kritické infrastruktury, ale svým narušením již povede ohrožení infrastruktury zahrnuté do kritické infrastruktury.

5.2 Párové porovnání metodou AHP

V této podkapitole jsou výše uvedené identifikované jevy párově porovnány pomocí metody AHP za účelem stanovení jejich významnosti. Tento krok je důležitý zejména pro následné stanovení vhodných a efektivních návrhů opatření, jež by mohla vést ke zlepšení celkového stavu.

Párové porovnání pomocí metody AHP je provedeno v rámci jednotlivých kategorií SWOT analýzy. Přičemž jak je uvedeno v kapitole 4, jednotlivé jevy jsou hodnoceny pomocí hodnotící škály v rozmezí hodnot 1 až 9. V tomto případě pak hodnota 1 značí vztah, kdy jsou oba jevy stejně významné, nebo je rozdíl v jejich významnosti zanedbatelný. Naproti tomu v případě hodnoty 9 se jedná o situaci, kdy je první jev totálně významnější než jev druhý. Pokud by v rámci párového porovnání byl první jev naopak méně významný, než jev druhý použije se pro vyjádření tohoto stavu převrácená hodnota 1/x, kde x vyjadřuje hodnotu o kolik je druhý jev významnější, jak jev první.

Konzistentnost výsledků párového porovnání potom je ověřena pomocí programu MCA7, tak jak je uvedeno v kapitole 4.

5.2.1 Párové porovnání silných stránek

Výsledky párového porovnání jsou uvedeny v tabulce 3. Následným vydělením prvků každého sloupce matice součtem všech prvků tohoto sloupce

byla získána sloupcově normalizovaná Saatyho matice, která je uvedena v tabulce 4. Následně je stejný postup aplikován na řádky Saatyho matice, čímž jsou identifikovány váhy jednotlivých jevů.

Tabulka 3 - párové porovnání silných stránek [zdroj vlastní]

Silné stránky		J							
		S1	S2	S3	S4	S5	S6	S7	S8
I	S1	1	3	2	7	3	4	5	4
	S2	1/3	1	1	4	2	5	4	3
	S3	1/2	1	1	5	2	3	5	2
	S4	1/7	1/4	1/5	1	1/5	1/4	1/3	1/3
	S5	1/3	1/2	1/2	5	1	2	4	3
	S6	1/4	1/5	1/3	4	1/2	1	3	1/2
	S7	1/5	1/4	1/5	3	1/4	1/3	1	1/3
	S8	1/4	1/3	1/2	3	1/3	2	3	1
Suma		3,00952381	6,533333333	5,733333333	32	9,283333333	17,58333333	25,33333333	14,16666667

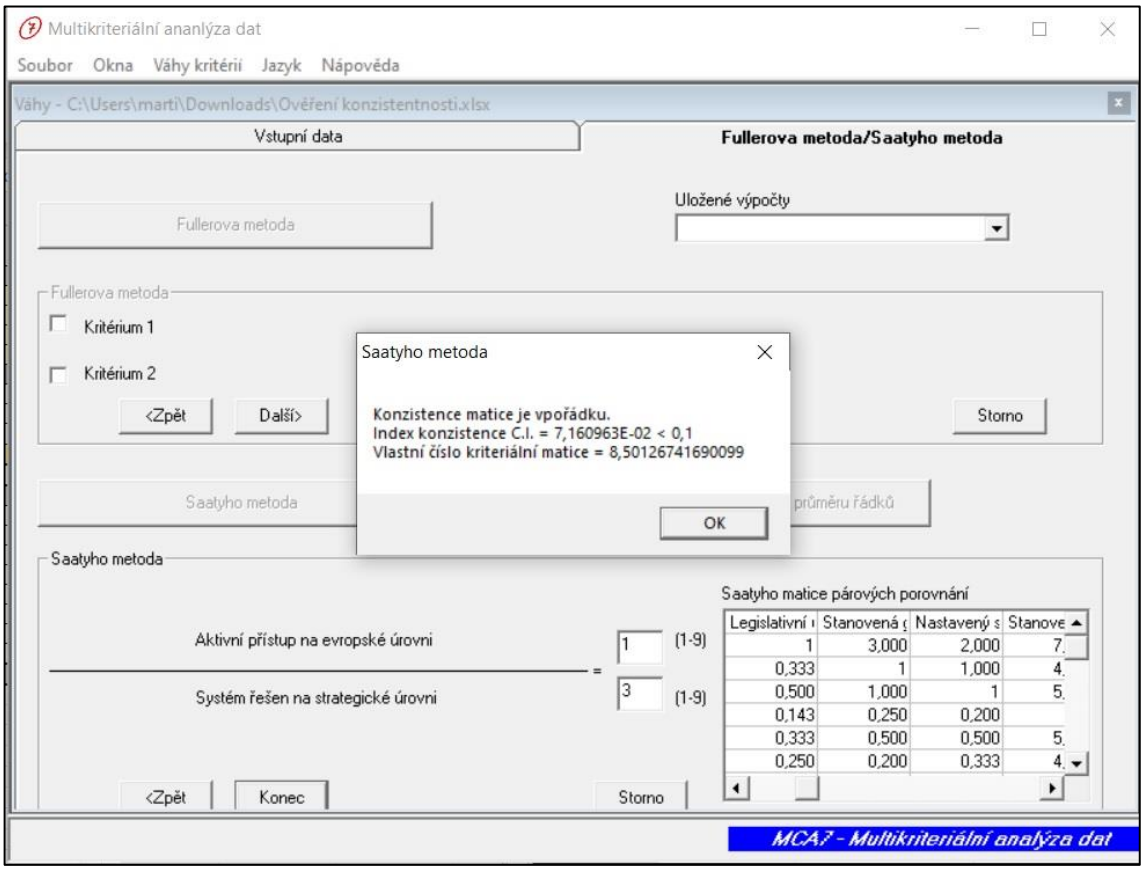
Tabulka 4 - výpočet vah silných stránek [zdroj vlastní]

	S1	S2	S3	S4	S5	S6	S7	S8	Skóre
S1	0,332278481	0,459183673	0,348837209	0,21875	0,323159785	0,227488152	0,197368421	0,282352941	0,298677333
S2	0,110759494	0,153061224	0,174418605	0,125	0,215439856	0,28436019	0,157894737	0,211764706	0,179087351
S3	0,166139241	0,153061224	0,174418605	0,15625	0,215439856	0,170616114	0,197368421	0,141176471	0,171808741
S4	0,047468354	0,038265306	0,034883721	0,03125	0,021543986	0,014218009	0,013157895	0,023529412	0,028039585
S5	0,110759494	0,076530612	0,087209302	0,15625	0,107719928	0,113744076	0,157894737	0,211764706	0,127734107
S6	0,08306962	0,030612245	0,058139535	0,125	0,053859964	0,056872038	0,118421053	0,035294118	0,070158572
S7	0,066455696	0,038265306	0,034883721	0,09375	0,026929982	0,018957346	0,039473684	0,023529412	0,042780643
S8	0,08306962	0,051020408	0,087209302	0,09375	0,035906643	0,113744076	0,118421053	0,070588235	0,081713667
Součet									1

Výsledné váhy jednotlivých silných stránek zaokrouhlené na dvě desetinná místa jsou následující:

- legislativní ukotvení – 0,30;
- stanovená gesce a role – 0,18;
- nastavený systém identifikace a určování prvků KI – 0,17;
- stanovení odbornosti styčných bezpečnostních zaměstnanců – 0,03;
- provázání se systémem krizového řízení – 0,13;
- připravenost na krizové situace pomocí plánovací dokumentace – 0,07;
- aktivní přístup na evropské úrovni – 0,04;
- systém řešen na strategické úrovni – 0,08.

Následně je ověřena konzistentnost párového porovnání pomocí programu MCA7, kdy výsledný indikátor konzistentnosti dosahuje (po zaokrouhlení na dvě desetinná místa) hodnoty 0,072, jak lze pozorovat na obrázku 4.



Obrázek 4 - ověření konzistentnosti párového porovnání silných stránek programem MCA7 [zdroj vlastní]

5.2.2 Párové porovnání slabých stránek

Výsledky párového porovnání slabých stránek jsou uvedeny v tabulce 5. Následně je použitý stejný postup jako v případě silných stránek, viz tabulka 6.

Tabulka 5 - párové porovnání slabých stránek [zdroj vlastní]

Slabé stránky		J							
		W1	W2	W3	W4	W5	W6	W7	W8
I	W1	1	1	4	3	6	4	6	5
	W2	1	1	5	4	7	5	7	6
	W3	1/4	1/5	1	1	4	3	4	3
	W4	1/3	1/4	1	1	5	3	5	3
	W5	1/6	1/7	1/4	1/5	1	1/2	1/4	1/5
	W6	1/4	1/5	1/3	1/3	2	1	1/2	1/3
	W7	1/6	1/7	1/4	1/5	4	2	1	1/2
	W8	1/5	1/6	1/3	1/3	5	3	2	1
Suma		3,366666667	3,102380952	12,16666667	10,06666667	34	21,5	25,75	19,03333333

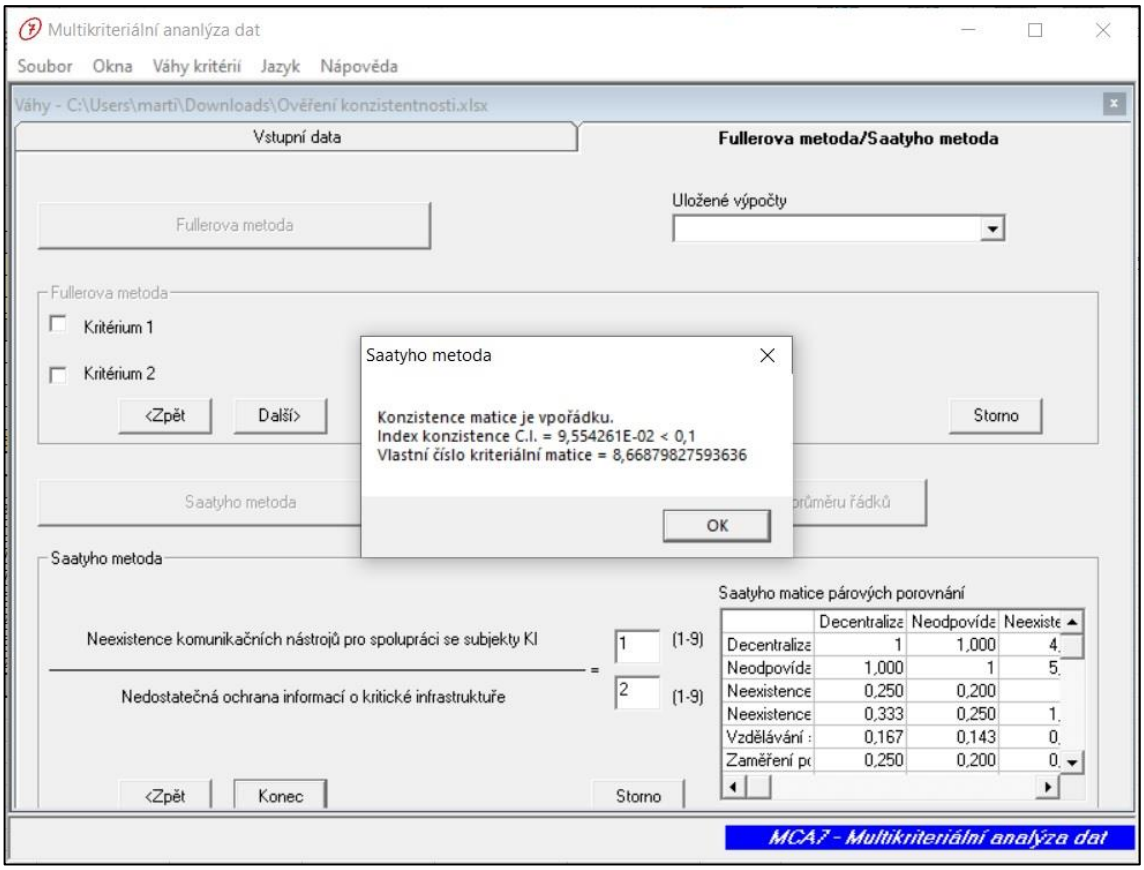
Tabulka 6 - výpočet vah slabých stránek [zdroj vlastní]

	W1	W2	W3	W4	W5	W6	W7	W8	Skóre
W1	0,297029703	0,322333078	0,328767123	0,298013245	0,176470588	0,186046512	0,233009709	0,262697023	0,263045873
W2	0,297029703	0,322333078	0,410958904	0,397350993	0,205882353	0,23255814	0,27184466	0,315236427	0,306649282
W3	0,074257426	0,064466616	0,082191781	0,099337748	0,117647059	0,139534884	0,155339806	0,157618214	0,111299192
W4	0,099009901	0,080583269	0,082191781	0,099337748	0,147058824	0,139534884	0,194174757	0,157618214	0,124938672
W5	0,04950495	0,046047583	0,020547945	0,01986755	0,029411765	0,023255814	0,009708738	0,010507881	0,026106528
W6	0,074257426	0,064466616	0,02739726	0,033112583	0,058823529	0,046511628	0,019417476	0,017513135	0,042687457
W7	0,04950495	0,046047583	0,020547945	0,01986755	0,117647059	0,093023256	0,038834951	0,026269702	0,051467875
W8	0,059405941	0,05372218	0,02739726	0,033112583	0,147058824	0,139534884	0,077669903	0,052539405	0,073805122
Součet									1

Výsledné váhy jednotlivých slabých stránek jsou následující:

- decentralizace systému v případě nestátních prvků KI – 0,26;
- neodpovídající kritéria – 0,31;
- absence sankcí – 0,11;
- neexistence standardů ochrany – 0,12;
- vzdělávání styčných bezpečnostních zaměstnanců – 0,03;
- zaměření pouze na ochranu – 0,04;
- absence komunikačních nástrojů pro spolupráci se subjekty KI – 0,05;
- nedostatečná ochrana informací o kritické infrastruktuře – 0,07.

Následně je ověřena konzistentnost párového porovnání, kdy výsledný indikátor konzistentnosti dosahuje hodnoty 0,096, jak lze pozorovat na obrázku 5.



Obrázek 5 - ověření konzistentnosti párového porovnání slabých stránek programem MCA7 [zdroj vlastní]

5.2.3 Párové porovnání příležitostí

Výsledky párového porovnání příležitostí jsou uvedeny v tabulce 7. Následně je použitý stejný postup jako v případě silných stránek, viz tabulka 8.

Tabulka 7 - párové porovnání příležitostí [zdroj vlastní]

Příležitosti		J						
		O1	O2	O3	O4	O5	O6	O7
I	O1	1	2	1/4	1/3	2	1	4
	O2	1/2	1	1/4	1/4	1	1/2	3
	O3	4	4	1	1	3	4	6
	O4	3	4	1	1	3	4	5
	O5	1/2	1	1/3	1/3	1	2	3
	O6	1	2	1/4	1/4	1/2	1	2
	O7	1/4	1/3	1/6	1/5	1/3	1/2	1
Suma		10,25	14,33333333	3,25	3,366666667	10,83333333	13	24

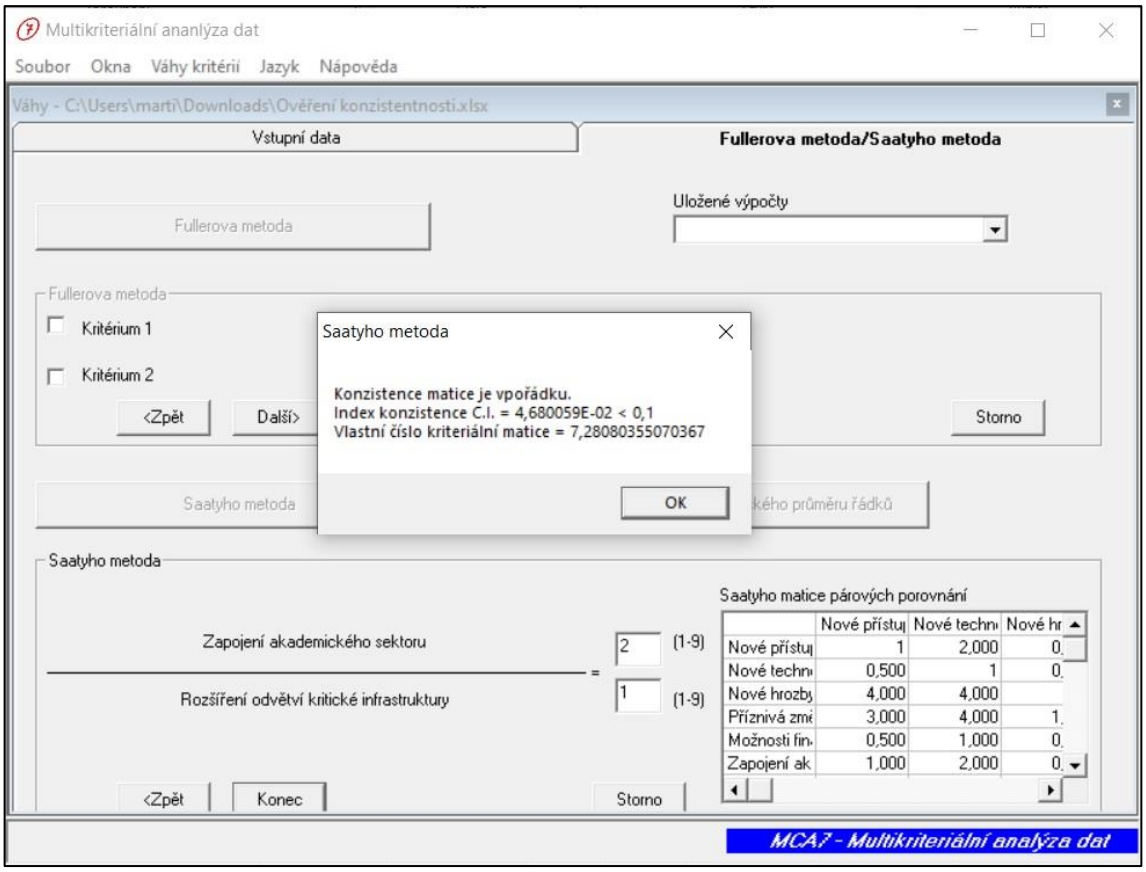
Tabulka 8 - výpočet vah příležitostí [zdroj vlastní]

	O1	O2	O3	O4	O5	O6	O7	Skóre
O1	0,097560976	0,139534884	0,076923077	0,099009901	0,184615385	0,076923077	0,166666667	0,120176281
O2	0,048780488	0,069767442	0,076923077	0,074257426	0,092307692	0,038461538	0,125	0,075071095
O3	0,390243902	0,279069767	0,307692308	0,297029703	0,276923077	0,307692308	0,25	0,301235866
O4	0,292682927	0,279069767	0,307692308	0,297029703	0,276923077	0,307692308	0,208333333	0,281346203
O5	0,048780488	0,069767442	0,102564103	0,099009901	0,092307692	0,153846154	0,125	0,098753683
O6	0,097560976	0,139534884	0,076923077	0,074257426	0,046153846	0,076923077	0,083333333	0,084955231
O7	0,024390244	0,023255814	0,051282051	0,059405941	0,030769231	0,038461538	0,041666667	0,038461641
Součet								1

Výsledné váhy jednotlivých příležitostí jsou následující:

- nové přístupy – 0,12;
- nové technologie – 0,08;
- nové hrozby – 0,30;
- příznivá změna evropské legislativy – 0,28;
- možnosti financování ISF či jiných fondů – 0,10;
- zapojení akademického prostoru – 0,08;
- rozšíření odvětví kritické infrastruktury – 0,04.

Následně je ověřena konzistentnost párového porovnání, kdy výsledný indikátor konzistentnosti dosahuje hodnoty 0,047, jak lze pozorovat na obrázku 6.



Obrázek 6 - ověření konzistentnosti párového porovnání příležitostí programem MCA7 [zdroj vlastní]

5.2.4 Párové porovnání hrozeb

Výsledky párového porovnání hrozeb jsou uvedeny v tabulce 9. Následně je použitý stejný postup jako v případě silných stránek, viz tabulka 10.

Tabulka 9 - párové porovnání hrozeb [zdroj vlastní]

Hrozby		J					
		T1	T2	T3	T4	T5	T6
I	T1	1	2	1	1/3	1/5	1/4
	T2	1/2	1	1	1/4	1/3	1/4
	T3	1	1	1	0,5	0,25	1/3
	T4	3	4	2	1	1/3	1/2
	T5	5	3	4	3	1	3
	T6	4	4	3	2	1/3	1
Suma		14,5	15	12	7,083333333	2,45	5,333333333

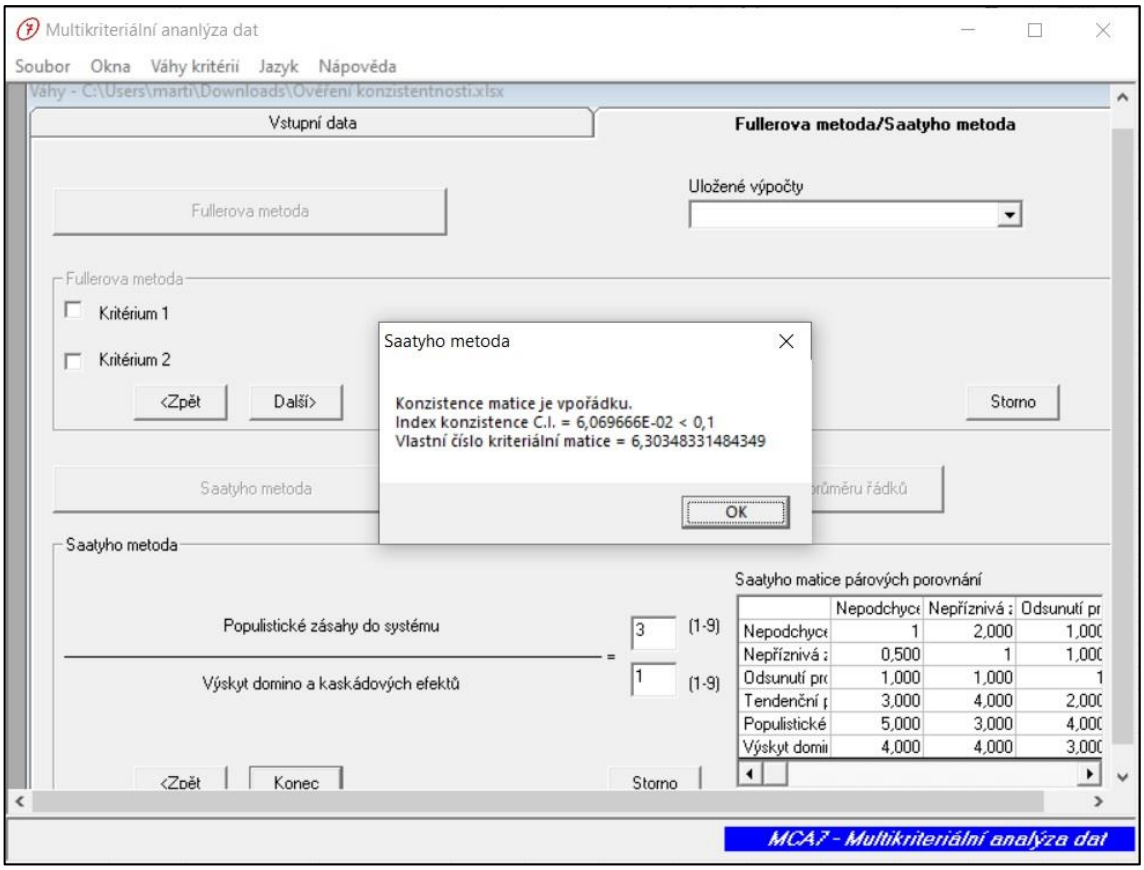
Tabulka 10 - výpočet vah hrozeb [zdroj vlastní]

	T1	T2	T3	T4	T5	T6	Skóre
T1	0,068965517	0,133333333	0,083333333	0,047058824	0,081632653	0,046875	0,076866443
T2	0,034482759	0,066666667	0,083333333	0,035294118	0,136054422	0,046875	0,067117716
T3	0,068965517	0,066666667	0,083333333	0,070588235	0,102040816	0,0625	0,075682428
T4	0,206896552	0,266666667	0,166666667	0,141176471	0,136054422	0,09375	0,16853513
T5	0,344827586	0,2	0,333333333	0,423529412	0,408163265	0,5625	0,378725599
T6	0,275862069	0,266666667	0,25	0,282352941	0,136054422	0,1875	0,233072683
Součet							1

Výsledné váhy jednotlivých příležitostí jsou následující:

- nepodchycení všech relevantních odvětví – 0,08;
- nepříznivá změna evropské legislativy – 0,07;
- odsunutí problematiky na okraj zájmu – 0,08;
- tendenční přístup k řešení ochrany kritické infrastruktury – 0,17;
- populistické zásahy do systému kritické infrastruktury – 0,38;
- výskyt domino a kaskádových efektů – 0,23.

Následně je ověřena konzistentnost párového porovnání, kdy výsledný indikátor konzistentnosti dosahuje hodnoty 0,061, jak lze pozorovat na obrázku 7.



Obrázek 7 - ověření konzistentnosti párového porovnání hrozeb programem MCA7 [zdroj vlastní]

5.3 Aplikace Paretova pravidla

Následnou aplikací Paretova pravidla jsou pomocí kumulativní funkce a podle dosaženého váhového koeficientu identifikovány ty nejvýznamnější jevy, které spolu dosahují 80 % významnosti (tedy součet jejich identifikovaných vah je roven nebo je menší jak 0,8) v každé z řešených kategorií. Níže jsou vypsány takto identifikované jevy, a to sestupně podle postupně kumulovaných vah.

- Silné stránky:
  - legislativní ukotvení – 0,30 (0,30);
  - stanovená gesce a role – 0,48 (0,18);

    - nastavený systém identifikace a určování prvků KI – 0,65 (0,17);
    - provázání se systémem krizového řízení – 0,78 (0,13).
- Slabé stránky:
    - neodpovídající kritéria – 0,31 (0,31);
    - decentralizace systému v případě soukromých prvků KI – 0,57 (0,26)
    - neexistence standardů ochrany – 0,69 (0,12);
    - absence sankcí – 0,80 (0,11).
- Příležitosti:
    - nové hrozby – 0,30 (0,30);
    - příznivá změna evropské legislativy – 0,58 (0,28);
    - nové přístupy – 0,70 (0,12);
    - možnosti financování z ISF či jiných fondů – 0,80 (0,10).
- Hrozby:
    - populistické zásahy do systému – 0,38 (0,38);
    - výskyt domino a kaskádových efektů – 0,61 (0,23);
    - tendenční přístup k řešení ochrany kritické infrastruktury – 0,78 (0,17).

Výše uvedené jevy jsou pro přehlednost uvedeny v upravené SWOT analýze (viz tabulka 11), kde se již nevyskytují ty jevy, jež v hodnocení významnosti nedosáhly dostatečné hodnoty. Právě tato SWOT analýza je výchozím podkladem pro stanovení opatření pro zlepšení současného stavu v systému kritické infrastruktury v ČR.

Tabulka 11 - SWOT analýza provedení metody AHP a aplikaci Paretova pravidla [zdroj vlastní]

SILNÉ STRÁNKY	SLABÉ STRÁNKY
- Legislativní ukotvení systému KI - Jednoznačně stanovené gesce a role všech aktérů - Systém identifikace a určování prvků KI - Provázání systému KI se systémem krizového řízení	- Špatně nastavená kritéria pro určování prvků KI - Decentralizace systému v případě nestátních prvků KI - Neexistence standardů ochrany - Absence sankcí
PŘÍLEŽITOSTI	**HROZBY**
- Nové hrozby - Příznivá změna evropské legislativy - Nové přístupy - Možnosti financování z ISF či jiných fondů	- Populistické či neodborné zásahy do systému - Výskyt domino a kaskádových efektů - Tendenční přístup k řešení ochrany KI

5.4 Komparace se systémem kritické infrastruktury na Slovensku

V této kapitole je pomocí komparativní metody srovnán systém kritické infrastruktury v ČR se systémem kritické infrastruktury na Slovenku. Jak je uvedeno výše v kapitole 4, komparace je zaměřena na oblasti právního ukotvení, definic, kompetence aktérů, určujících kritérií, identifikace a určování prvků KI, ochrany kritické infrastruktury a kontroly plnění opatření.

Systém kritické infrastruktury na Slovensku (dále jen „SR“) byl stejně jako v případě ČR výrazně legislativně upraven v souvislosti s implementací Směrnice EKI. Konkrétně se jednalo o přijetí specifického a samostatného *zákona*

č. 45/2011 Sb., o kritické infrastruktuře (dále jen „zákon o KI"), čímž se již na první pohled slovenský přístup od toho českého liší.

Předmětem zákona o KI je především vymezení organizace a působnosti orgánů státní správy v oblasti kritické infrastruktury a s tím související postup při určování prvků KI spolu se stanovením povinností provozovatelům kritických infrastruktur (dále jen „provozovatel KI") a zodpovědnosti těchto provozovatelů za porušení stanovených povinností.

Tomuto právnímu předpisu také jako v případě ČR ještě předcházelo řešení problematiky mimo nastavení vytyčené Směrnicí EKI. Konkrétně se o kritické infrastruktuře začalo v kontextu SR hovořit již v roce 2006, kdy byla vládou SR přijata *Koncepce kritické infrastruktury ve Slovenské republice a způsob její ochrany a obrany* (29).

Současná právní úprava této problematiky stejně tak, jako v případě ČR, rozlišuje v definicích mezi prvkem KI a kritickou infrastrukturou, kdy prvek KI je chápán jako *„především inženýrská stavba, služba ve veřejném zájmu a informační systém v sektoru kritické infrastruktury, jejichž narušení anebo zničení by mělo dle sektorových a průřezových kritérií závažné a nepříznivé důsledky na uskutečňování hospodářské a sociální funkce státu, a tím na kvalitu života obyvatel z hlediska ochrany jejich života, zdraví, bezpečnosti, majetku a životního prostředí."* (30).

Kritická infrastruktura je naproti tomu chápána jako *„systém, který se člení na sektory a prvky"*, přičemž slovenské pojetí rovněž zavádí také pojem sektor kritické infrastruktury, jež je chápán jako *„část kritické infrastruktury, do které se zařazují prvky; sektor může obsahovat jeden anebo více podsektorů kritické infrastruktury"*.

Proti českému přístupu je odlišný přístup k určujícím kritériím. Ta jsou sice, stejně tak jako ta česká, rozdělena podle Směrnice EKI na průřezová a odvětvová. Nicméně zatímco český systém nerozlišuje tyto dva typy kritérií pro národní a evropskou úroveň, ve slovenském pojetí je odlišnost těchto kritérií pro národní a evropskou úroveň zohledněna specifickými definicemi (30). Obecně lze konstatovat, že v kontextu definic je slovenský zákon o KI mnohem podrobnější, neboť dále definuje i mechanické a technické zabezpečovací prostředky ve vztahu ke kritické infrastruktuře, a zároveň definuje pojem citlivých informací o kritické infrastruktuře, což souvisí se skutečností, že slovenský systém kritické infrastruktury utajuje některé z informací o prvcích KI, a to takových, které by svým zveřejněním mohly vést k narušení nebo zničení prvku KI.

Stejně jako v českém systému kritické infrastruktury, i zde je v souladu se Směrnicí EKI řešena pouze otázka ochrany kritické infrastruktury a problematika odolnosti (resilience) tak ještě není na legislativní úrovni řešena (31). Problematika byla dosud řešena tak jako v českém případě pouze na akademické úrovni, a to konkrétně v rámci společného česko-slovenského projektu *Metodika hodnocení resilience prvků kritické infrastruktury*, na kterém se podílela Žilinská univerzita s Technickou univerzitou v Otravě (31).

Z hlediska ochrany prvků KI slovenský systém kritické infrastruktury primárně stanovuje povinnosti pro provozovatele KI, kdy zodpovědnost za ochranu prvku KI plně odpovídá daný provozovatel KI, jež musí přijmout všechny potřebné opatření k zajištění absolutní funkčnosti, integrity a kontinuity provozu tohoto prvku KI. Za tímto účelem provozovatel KI zpracovává bezpečnostní plán, který musí zpracovat do šesti měsíců od oznámení o určení prvku KI a v případě nutnosti dále aktualizovat. Dále má povinnost realizovat jednou za tři roky cvičení s cílem procvičit postupy a opatření uvedené v bezpečnostním plánu. Zároveň má povinnost určit oprávněnou osobu, která

vykonává povinnosti styčného bezpečnostního zaměstnance. Dalším opatřením, které je pro slovenský systém specifické, je povinnost provozovatele KI při modernizaci technologií prvku KI volit takovou technologii, která zároveň zajistí jeho ochranu (30).

Aktéři v systému kritické infrastruktury SR v kontextu orgánů veřejné správy jsou přímo uvedeni v příslušném ustanovení zákona o KI. Zastřešujícím orgánem je vláda SR, mezi jejíž hlavní kompetence, kromě schvalování koncepce kritické infrastruktury, je určování prvků KI a jejich zařazení do příslušného sektoru kritické infrastruktury.

Ministerstvo vnitra SR potom plní v celém systému, stejně jako jeho český protějšek, koordinační roli. Proti českému systému je však tato role mnohem významnější, neboť zákon o KI dává slovenskému Ministerstvu vnitra rozsáhlé pravomoci v oblasti stanovování průřezových a také odvětvových kritérií, kde právě Ministerstvo vnitra SR předkládá vládě ke schválení průřezová i odvětvová kritéria. Má tak v této věci silnější postavení vůči ostatním věcně příslušným ministerstvům či jiným ÚSÚ. Ve srovnání s českým systémem je tak ten slovenský více centralizován (30).

V neposlední řadě plní úkoly v systému kritické infrastruktury SR další ministerstva či jiné ÚSÚ. Zatímco v českém systému se povinnosti týkají všech věcně příslušných ministerstev a ÚSÚ, v případě slovenského systému jsou všechny zainteresované státní instituce přímo uvedeny v zákoně (30).

Vyšší míra centralizace je patrná také v oblasti identifikace a určování prvků KI. Zde věcně příslušná ministerstva a jiné ÚSÚ připravují návrh prvků KI, které by měly být v jejich sektorech určeny. Tento návrh následně předávají na Ministerstvo vnitra SR, které potom po posouzení tento návrh předkládá vládě ke schválení. Ve srovnání s českým mechanismem se tak jedná pouze

o jeden způsob určování prvků KI, přičemž všechny prvky KI procházejí v rámci procesu určování přes jedno konkrétní místo (30).

Při určování prvků KI jsou posuzována průřezová a sektorová kritéria, přičemž, jak již byl uvedeno výše, existují dvě úrovně těchto kritérií v závislosti na tom, zda se jedná či nejedná o prvek EKI. Průřezová kritéria jsou posuzována podle předpokládaného počtu ohrožených osob (usmrcených a zraněných), hospodářského vlivu (zohledňovány jsou hospodářské ztráty, zhoršení kvality zboží či poskytovaných služeb) a vlivu na obyvatelstvo ve smyslu zhoršení kvality života (zohledňován je výpadek dodávek zboží a služeb a jejich dostupnost). V případě sektorových kritérií je jejich výčet uveden v příloze zákona o KI. Identifikovanými sektory jsou:

- doprava,
- elektronické komunikace,
- energetika,
- pošta,
- průmysl,
- informační a komunikační technologie,
- voda a atmosféra,
- zdravotnictví,
- finance,
- půdní hospodářství.[2]

Konkrétní hodnoty a limity uvedených průřezových a sektorových kritérií byly schváleny vládou jako samostatný dokument, přičemž vzhledem k tomu, že

[2] zemědělství a potravinářství

je k těmto limitům přistupováno jako k citlivým informacím podle zákona o KI, nejsou tyto hodnoty k dispozici (30).

V případě kontrolní činnosti v systému kritické infrastruktury je postupováno obdobným způsobem jako v ČR. Tedy za kontrolu provozovatelů KI je zodpovědné věcně příslušné ministerstvo nebo jiný ÚSÚ. Oproti českému systému je zde navíc stanovena povinnost pro tato věcně příslušná ministerstva nebo jiné ÚSÚ předkládat jedenkrát ročně Ministerstvu vnitra SR souhrnnou zprávu o kontrole provozovatelů KI (30).

5.5 Komparace se systémem kritické infrastruktury ve Finsku

Zlomovým bodem ve Finském přístupu ke kritické infrastruktuře byla mohutná bouře Tapani, která Finsko, zejména jeho západní pobřeží, zasáhla v prosinci 2011. Bouře vedla ke vzniku kaskádového efektu poruch, což způsobilo výpadek dodávek elektrické energie pro téměř 600 tisíc odběratelů. Ve Finsku se tak jednalo o jednu šestinu všech domácností. Zároveň byla zasažena teplárenská infrastruktura, nemocnice a rozvody vody spolu s čističkami odpadních vod. Bouře zároveň způsobila rozsáhlé výpadky v oblasti telekomunikačních služeb. Tato mimořádná událost byla pro Finsko zlomovým bodem, který vedl k zásadnímu přehodnocení politiky v oblasti kritické infrastruktury (32).

Finský legislativní rámec pro řešení problematiky kritické infrastruktury tvoří v základu *zákon č. 1390/1992 Sb., o opatřeních nezbytných k zabezpečení nouzového zásobování*, na které přímo navazuje *nařízení vlády 1048/2018, o úkolech nouzového zásobování* (33). V tomto nařízení vlády je poté obsažena definice kritické

infrastruktury, kterou se rozumí *„základní struktury, služby a související funkce, které jsou zásadní pro zachování životně důležitých společenských funkcí. Kritická infrastruktura zahrnuje jak fyzická zařízení a struktury, tak i elektronické funkce a služby. Kritickou infrastrukturu udržují hlavně podnikatelské subjekty, jejichž funkce jsou často vzájemně závislé“* (34).

Tento základní právní rámec poté doplňují dokumenty nelegislativní povahy, kde se jedná zejména o *Bezpečnostní strategii pro společnost* z roku 2017, která se zaměřuje na odolnost dodávek služeb nezbytných pro fungování společnosti a vlády. Ve vztahu ke kritické infrastruktuře je pak v této strategii konstatováno, že fungování národní infrastruktury je zaručeno zejména zajištěním bezpečnosti dodávek. Opatření nezbytná k zachování bezpečnosti dodávek pak musí být podle této strategie taková, aby jejich narušení nevedlo k ohrožení života a zdraví obyvatelstva, životně důležitých funkcí společnosti, zásobování potravinami, sociální a zdravotní péče a materiální základny pro národní obranu (35).

Dále je systém kritické infrastruktury Finska ovlivňován dalšími předpisy, které jsou specifické pro některá z řešených odvětví kritické infrastruktury. Zde se jedná například o *zákon č. 588/2013 Sb., o trhu s elektrickou energií* v případě legislativních předpisů, či o finskou *Strategii kybernetické bezpečnosti* v případě nelegislativních dokumentů (33).

Z hlediska aktérů systému kritické infrastruktury je tato problematika v kompetenci Agentury pro nouzové zásobování (dále jen „NESA“), která ve finském bezpečnostním systému zastává funkci organizace řešící otázku krizového řízení, přípravy na krizové situace a ochrany a zajišťování trvalého fungování životně důležitých společenských funkcí (36).

Původní rolí NESA bylo především udržování rezervních zásob určených na ochranu obživy obyvatelstva i fungování ekonomiky. V současném systému

však NESA zastává aktivní roli při zajišťování kontinuity provozu kritické infrastruktury a posilování odolnosti v dotčených odvětvích. NESA dále hodnotí aktuální stav problematiky v jednotlivých odvětvích KI, a poskytuje konkrétní doporučení (37).

Na rozdíl od českého a slovenského modelu je finský přístup specifický tím, že je zaměřen primárně na úzkou spolupráci mezi soukromým a veřejným sektorem v oblasti sdílení informací a budování konsensu o koncepci politiky a stanovování cílů k rozvoji systému kritické infrastruktury. Tento přístup zahrnuje kombinaci politických nástrojů pro stimulaci investic do odolnosti kritických infrastruktur, a to jak regulačních, tak především dobrovolných (33).

Pro podporu tohoto přístupu byla zřízena Národní organizace pro nouzové zásobování (dále jen „NESO“), která funguje jako základní platforma pro výše uváděné partnerství mezi soukromým a veřejným sektorem. NESO sdružuje provozovatele KI a zástupce veřejné správy v odvětvově specifických skupinách (tzv. poolech), kde je cílem rozvíjet společné chápání rizik v jednotlivých odvětvích a identifikování zranitelných míst pro kritickou infrastrukturu v těchto odvětvích. Dále je v těchto odvětvových skupinách řešena otázka přípravy a realizace praktických opatření k posilování připravenosti na vznik možných mimořádných událostí a k zajištění kontinuity provozu kritické infrastruktury (33).

Odvětví KI jsou ve finském systému definována v nařízení vlády o úkolech nouzového zásobování, přičemž v současné době jsou řešena následující odvětví kritické infrastruktury: (33)

- energetika,
- komunikační a informační systémy,
- finanční služby,

- doprava a logistika,
- zásobování vodou,
- odpadové hospodářství.

Dalším významným rozdílem finského přístupu ve srovnání s českým a slovenským přístupem je odlišné pojetí kritické infrastruktury v případě jejího identifikování a určování. Zatímco v případě systému kritické infrastruktury v ČR a SR je kladen důraz na určování kritické infrastruktury jako konkrétních objektů, resp. prvků systému, které dosahují kritičnosti z pohledu odvětvových a průřezových kritérií, ve Finsku je kritická infrastruktura primárně pojímána jako poskytování služby, tedy hlavní důraz není kladen na jednotlivé prvky, ale na jejich provozovatele a jejich schopnost zajistit dodávky nezbytných služeb a zboží (33).

S tím souvisí i finská snaha o ochranu kritické infrastruktury pomocí posilování odolnosti této infrastruktury ve vazbě na posílení schopností identifikovaných subjektů KI v odvětvích KI ve smyslu zajištění dodávek nezbytných služeb v případě narušení infrastruktury těchto subjektů a co nejkratšího času potřebného pro obnovu do normálního stavu (33).

V případě ochrany kritické infrastruktury a s tím souvisejících povinností subjektů KI neexistuje ve finském systému jednotný přístup. V zásadě mají subjekty KI odpovědnost za posouzení kritičnosti své sítě a za tímto účelem provádějí vlastní analýzy rizik, kdy neexistuje jednotný postup k provedení této analýzy, ale NESA jako ústřední orgán pro tuto oblast poskytuje metodické vedení. Subjekty KI jsou dále motivovány k přijímání a upřednostňování opatření, která vedou k posilování odolnosti těchto subjektů a k vypracování plánů kontinuity provozu, které slouží jako PKP subjektu KI (31). Tyto činnosti však nejsou ve finském případě nařizovány direktivně, ale jedná se o činnosti

vzešlé z konsenzu mezi subjekty KI a veřejnou správou v rámci jednotlivých odvětvových skupin. Ve srovnání se systémem v ČR a SR se tak nejedná o direktivní přístup, ale je zde určitá míra dobrovolnosti (32).

Direktivní povinnosti jsou samozřejmě také v rámci jednotlivých odvětví stanoveny. Ty však nejsou řešeny v rámci systému kritické infrastruktury, ale jsou obsahem specifických právních předpisů pro dané odvětví (33).

5.6 Posouzení hypotéz

V této části jsou posouzeny hypotézy, které jsou stanoveny v kapitole 2. Při jejich posuzování je vycházeno zejména z výsledků provedené SWOT analýzy a z komparace systému kritické infrastruktury ČR s obdobnými systémy na Slovensku a ve Finsku.

Hypotéza 1: Přístup k identifikaci a určování prvků KI je v jednotlivých odvětvích rozdílný. V rámci provedené SWOT analýzy byla jako jedna ze slabých stránek systému kritické infrastruktury v ČR identifikována špatně nastavená kritéria pro určování prvků KI v jednotlivých odvětvích, přičemž jedním z hlavních argumentů k tomuto tvrzení je nerovnoměrné určování prvků KI napříč všemi odvětvími, což vede k výrazným odlišnostem v počtu určených prvků KI.

Otázkou tedy je, jaké jsou důvody těchto odlišností mezi jednotlivými odvětvími. Podstatným důvodem může být samotná povaha prvků KI v jednotlivých odvětvích. Tedy, že u některých odvětví je dynamika identifikace a určování prvků, a s tím spojené rušení stávajících prvků KI, spojeno s konkrétním typem infrastruktury, která se v daném odvětví vyskytuje.

Ideálním příkladem je v tomto kontextu odvětví komunikačních a informačních systémů, ve kterém k takovýmto změnám dochází ze všech odvětví nejčastěji, K tomu velkou měrou přispívá oblast kybernetické bezpečnosti, která do odvětví komunikačních a informačních systémů spadá. Naproti tomu v „tradičních" odvětvích kritické infrastruktury probíhá fluktuace prvků KI v mnohem menším měřítku nebo vůbec. Příkladem může být odvětví vodního hospodářství, kde od implementace problematiky kritické infrastruktury nedošlo k navýšení či snížení celkového počtu prvků KI. Ačkoli se v případě určování prvků KI může jednat o jeden z důvodů, nebude určitě jediný, a to zejména v kontextu odvětví, kde je taktéž určována „klasická" kritická infrastruktura (ve smyslu objektů), ale změny zde kontinuálně probíhají. V tomto případě se jedná především o odvětví nouzových služeb.

Tímto se dostáváme k tomu, co již vychází přímo ze SWOT analýzy, tedy že určující kritéria jsou nastavena nerovnoměrným způsobem. Nejedná se v tomto kontextu pouze o to, že by kritéria byla nastavena na příliš vysoké prahové hodnoty, které splňuje pouze pár objektů či zařízení v daném odvětví (případně je nesplňuje žádný z takových objektů), ale i o situaci, kdy jsou jako prvky KI identifikovány objekty, či zařízení, které z pohledu definice kritické infrastruktury nedosahují národního významu. V prvním případě se jedná zejména o odvětví zdravotnictví a odvětví zemědělství a potravinářství. V případě toho druhého se pak jedná o odvětví nouzových služeb, kde jsou určovány jednotlivé stanice Hasičského záchranného sboru ČR, které jsou významné především na krajské, resp. místní úrovni.

Posledním důvodem této nerovnosti je odlišný přístup věcně příslušných ministerstev a jiných ÚSÚ, který však lze pozorovat již v případě stanovených odvětvových kritérií, neboť tato kritéria jsou navrhována právě věcně příslušnými ministerstvy či jinými ÚSÚ a následně zapracována do prováděcího

právního předpisu ke krizovému zákonu, tedy nařízení vlády. V současné době neexistuje nástroj, který by méně aktivní gestory přiměl k zodpovědnému přístupu v rámci svého odvětví.

V souladu s výše uvedeným tak lze konstatovat, že tato hypotéza byla na základě zjištění prezentovaných v kapitole 5 diplomové práce **potvrzena**.

Hypotéza 2: K ochraně prvků KI je v rámci hodnocených systémů kritické infrastruktury přistupováno srovnatelným způsobem. Tato hypotéza vychází z předpokladu, že hodnocené státy musely, jakožto členské státy EU, provést implementaci Směrnice EKI, tudíž jejich přístup k ochraně kritické infrastruktury vychází z náležitostí a povinností stanovených v tomto závazném předpise. V zásadě se jedná o implementaci ochrany kritické infrastruktury, povinnost zpracovávat dokumentaci řešící ochranu určené kritické infrastruktury a určení styčného bezpečnostního zaměstnance.

Při srovnání systému kritické infrastruktury ČR a SR lze konstatovat, že oba systémy vykazují v případě ochrany kritické infrastruktury vysokou míru podobnosti. Oba tyto systémy silně vychází z nastavení Směrnice EKI a povinnosti stanovené pro EKI rozšiřují na národní úroveň. Přesto lze v oblasti ochrany kritické infrastruktury identifikovat několik odlišností.

Slovenský systém je ve srovnání s tím českým a finským více direktivní a také mnohem více centralizovaný. V případě srovnání s českým systémem kritické infrastruktury jsou ve slovenském případě stanoveny i další povinnosti pro subjekty KI, kdy se jedná především o povinnost zohledňovat při modernizaci takové technologie, které povedou ke zvýšení ochrany prvku KI a zároveň jsou ve slovenském systému nad rámec směrnice definovány citlivé informace o kritické infrastruktuře, které podléhají utajení.

Tomuto předpokladu však úplně neodpovídá finský model. V základu je finské pojetí ochrany kritické infrastruktury postaveno na principu dobrovolnosti s velkým důrazem na budování úzkého partnerství mezi veřejným a soukromým sektorem. Zatímco v případě systému kritické infrastruktury v ČR a v SR je otázka ochrany pojímána jako ochrana konkrétních prvků KI tak, aby tyto prvky byly schopny zabezpečit svůj provoz, finský přístup je zaměřen na ochranu kritické infrastruktury jako na ochranu celého systému, resp. v tomto kontextu celého odvětví. Cílem pak je především zabezpečení nezbytných dodávek a služeb s důrazem na zajištění kontinuity dodávaných služeb. V tomto ohledu je tak finský systém zaměřen primárně na subjekty KI a na spolupráci s nimi.

Tomuto odlišnému pojetí odpovídá i skutečnost, že zatímco ČR a SR od roku 2011 identifikovalo na svém území několik prvků EKI, ve Finsku k tomu za celou dobu nedošlo, ačkoliv v rámci prostoru severní Evropy existuje výrazná propojenost s ostatními státy (zejména se Švédskem) v oblasti energetiky, kde se jedná především elektrizační soustavu (38).

Na základě výše uvedených skutečností tak lze konstatovat, že tato hypotéza byla **vyvrácena**.

Hypotéza 3: Problematika kritické infrastruktury byla na základě Směrnice EKI implementována v podmínkách ČR na dostatečné úrovni. Cílem poslední hypotézy je prověření samotné implementace Směrnice EKI do českého právního řádu. Dle legislativního procesu EU je směrnice dokumentem, který je pro členské státy právně závazný, nicméně na rozdíl od nařízení mohou být ustanovení směrnice implementována do národní legislativy způsobem, jaký uzná členský stát za vhodný. Míra implementace směrnice se tak mezi jednotlivými členskými státy může významně lišit.

To je patrné z provedené komparace, kde finské řešení nevedlo k určení žádného prvku EKI, ale také ze studie provedené Evropskou komisí, která identifikovala výrazný nepoměr v určování EKI mezi jednotlivými členskými státy.

Jak z diplomové práce vyplynulo, český model přímo vychází z pojetí, které bylo definováno ve Směrnici Rady 2008/114/ES, a to jak v případě stanovených definic, které v některých ohledech více rozvíjí (viz rozlišování mezi kritickou infrastrukturou a prvkem KI) tak i v případě stanovení povinností pro subjekty KI a určení aktérů ze strany veřejné správy (zde zejména otázka stanovení kontaktního bodu za ČR).

V ČR potom implementace vedla k identifikaci a určení 8 prvků EKI v odvětví energetiky a v souvislosti s určením těchto prvků pak také probíhá pravidelné odesílání zpráv EK tak, jak je to uvedeno ve směrnici (potažmo v krizovém zákoně).

Dle výše uvedeného lze tedy konstatovat, že tato hypotéza byla **potvrzena**.

5.7 Návrhy opatření

V této podkapitole je vycházeno z provedené SWOT analýzy, kdy cílem navrhovaných opatření je úprava oblastí, které byly v rámci slabých stránek identifikovány jako ty nejvýznamnější, přičemž návrhy těchto opatření se zároveň opírají jak o identifikované silné stránky systému kritické infrastruktury, tak také o příležitosti, které mohou pozitivním způsobem ovlivňovat fungování a další směřování tohoto systému.

Kromě využití identifikovaných silných stránek a příležitostí vychází navrhovaná opatření taktéž z provedené komparace, kdy je cílem využít příklady dobré praxe identifikované u srovnávaných systému kritické infrastruktury.

V tomto kontextu je potřeba zmínit, že v případě inspirace od srovnávaných systému lze definovat dvě možné cesty, které lze označit jako umírněnou a radikální. Umírněná cesta pak představuje dílčí změny již nastaveného systému, přičemž vycházet lze v tomto případě ze slovenského modelu. Naopak radikální cesta znamená výrazné předělání současného systému, kdy příkladem může být srovnávaný finský model, případně nové pojetí, které v současné době prosazuje Evropská komise se svým návrhem Směrnice CER.

5.7.1 Úprava kritérií pro určení prvku KI

Jak již bylo několikrát v této práci zmíněno, nejmarkantnější problém s nastavenými kritérii pro určení prvku KI se týká odvětvových kritérií v odvětví zdravotnictví a v odvětví zemědělství a potravinářství. Navrhované opatření tak tak bude zaměřeno na zlepšení současného stavu právě s přihlédnutím k těmto dvěma odvětvím.

A) Odvětví zdravotnictví

Až do jara 2020 byla odvětvová kritéria pro odvětví zdravotnictví stanovena pouze ve vazbě na zdravotnická zařízení. V souvislosti s pandemií koronaviru pak proběhla rychlá novelizace nařízení vlády o kritériích pro určení prvku KI, kterou bylo odvětví rozšířeno také o oblast výrobců léčivých přípravků, nicméně odvětví je i přesto stále charakteristické tím, že v něm nedošlo k určení žádného

prvku KI. Vzhledem k tomu, že zdravotnická infrastruktura, zejména pak zdravotnická zařízení poskytující akutní péči, patří mezi nejvýznamnější typ infrastruktury v ČR, je její absence v systému kritické infrastruktury překvapivá.

Vezmeme-li v potaz odvětvové kritérium pro určování zdravotnických zařízení, tak jeho přesné znění je následující:

- *„Poskytování zdravotních služeb – Zdravotnické zařízení, jehož celkový počet akutních lůžek je nejméně 2500.“*

Přitom největší zdravotnické zařízení v ČR, tedy Fakultní nemocnice v Motole, disponuje pouze celkem 2 199 lůžky (39). Pro další srovnání, Fakultní Thomayerova nemocnice disponuje 1 063 lůžky (40). Současné kritérium tak zamezuje určení zdravotnických zařízení v ČR. Takto nastavená mezní hodnota navíc významně přesahuje i průřezová kritéria.

Týká se to průřezového kritéria, které zohledňuje „*dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.*“, neboť dle dat Českého statistického úřadu (dále jen „ČSÚ“) bylo ke dni 31. prosince 2019 v ČR k dispozici 57 422 lůžek v nemocnicích s akutní péčí (41). Vzhledem k tomu, že ke stejnému datu, tedy k 31. prosinci 2019, bylo dle ČSÚ v ČR celkem 10 693 939 obyvatel (41), lze jednoduchým výpočtem dojít k údaji počtu akutních lůžek na 1 000 obyvatel, kdy tento údaj pro rok 2019 vycházel na 5,4 lůžek na 1 000 obyvatel.

Pokud aplikujeme tento údaj na průřezové kritérium dopadu na veřejnost postihujícího více než 125 000 osob lze dojít k závěru, že toto průřezové kritérium naplní všechna zdravotnická zařízení poskytují akutní péči, která disponují více než 675 lůžky.

V kontextu výše uvedeného potom lze jít cestou úpravy limitní hodnoty tohoto odvětvového kritéria podle navrhované hodnoty, tedy 675 akutních lůžek, nebo lze, vzhledem k neustále se měnícímu počtu akutních lůžek, stanovit obecné odvětvové kritérium, které pouze vymezí okruh dotčených subjektů a jejich významnost bude následně posuzována podle průřezových kritérií. Druhá možnost se v tomto kontextu jeví praktičtější, neboť umožňuje pružněji reagovat na změny v odvětví a v celkovém počtu akutních lůžek. Podobný princip je přitom použit například u stanic Hasičského záchranného sboru ČR, nebo v případě operačních a informačních středisek základních složek IZS (12).

B) Odvětví potravinářství a zemědělství

V případě odvětví potravinářství a zemědělství je situace velice podobná situaci v odvětví zdravotnictví. Odvětví spadá do kompetence Ministerstva zemědělství, které je zároveň věcně příslušné také za odvětví vodní hospodářství. Zatímco v odvětví vodní hospodářství byla odvětvová kritéria stanovena takovým způsobem, že v konečném důsledku došlo k určení 11 prvků KI, v případě odvětví potravinářství a zemědělství nedošlo k určení žádného prvku KI. Opět by tak zásadním nedostatkem v tomto případě měla být nevhodně nastavená odvětvová kritéria.

Na rozdíl od odvětví zdravotnictví, kde bylo relativně jednoduché dohledat počty akutních lůžek v největších zdravotnických zařízeních, v případě infrastruktury v zemědělství a potravinářství je situace mnohem složitější. Jednak existuje v tomto odvětví obrovské množství subjektů, druhým aspektem je poté skutečnost, že na rozdíl od zdravotnictví, dochází v případě potravin k jejich vývozu a dovozu ze zahraničí, což komplikuje situaci při určování prvků KI v tomto odvětví. Významným faktorem je tak v tomto případě roztříštěnost celého odvětví na velké množství menších subjektů. Pro posouzení vhodnosti

stanovených kritérií byla zvolena odvětvová kritéria pro živočišnou a potravinářskou výrobu, neboť data týkající se těchto kritérií jsou relativně snadno dostupná skrze informace, které sbírá ČSÚ.

Kritérium pro živočišnou produkci je stanoveno pomocí hlediska odpovídajícího počtu kusů chovaných zvířat v jednom chovu na území jednoho kraje. Konkrétně je to 10 000 kusů v případě skotu, 45 000 kusů v případě prasat a 300 000 kusů drůbeže.

Dle dat ČSÚ bylo k 1. dubnu 2020 v českých velkochovech celkem 1 404 000 kusů skotu, 1 499 000 prasat a 24 247 000 drůbeže (41). Přepočítáme-li počty zvířat na počet obyvatel (10 693 939 osob viz výše), vychází statisticky 7,6 osob na 1 ks skotu, 7,1 osob na 1 ks prasete a 0,44 osob na 1 ks drůbeže. Následným přepočtem podle průřezového kritéria dopadu na 125 000 osob vychází hodnoty 16 447 skotu, 17 606 prasat a 284 000 drůbeže. K určení konečného počtu zvířat ve velkochovech je však ještě potřeba vzít v potaz soběstačnost ČR v případě těchto zvířat, tedy jaký je podíl zahraniční produkce na celkové spotřebě v ČR. Dle dat Ministerstva zemědělství byla v případě řešených komodit soběstačnost v roce 2019 následující (42):

- hovězí maso – 120,9%,
- vepřové maso – 50,8%,
- drůbeží maso – 65,2%.

Přepočítáním s využitím soběstačnosti jsou výsledné hodnoty 13 593 kusů skotu, 34 522 kusů prasat a 436 923 kusů drůbeže. Dle výsledných hodnot lze konstatovat, že odvětvová kritéria nebyla ze strany Ministerstva zemědělství stanovena nepřiměřeným způsobem, nicméně při přepočtu těchto kritérií byly identifikovány některé jejich problematické aspekty. Zaprvé kritéria

nezohledňují, jestli se jedná o jatečné zvíře nebo ne (s výjimkou velkochovů prasat), přičemž soběstačnost v produkci mléka a vajec je zcela odlišná.

Dalším problémem je skutečnost, že počet kusů ve velkochovech a potravinová soběstačnost ČR se dynamicky vyvíjí a data jsou každý rok výrazně odlišná (často s klesající tendencí), přičemž kritérium bylo stanoveno v roce 2010 a dnešní situaci tak neodpovídá. Například v roce 2010 evidoval ČSÚ celkem 1 909 000 ks prasat (41), tedy přibližně o půl milionu více než v roce 2020, a soběstačnost v případě vepřového masa dosahovala hodnoty 63,8 % (43). Zároveň bylo v roce 2010 v ČR evidováno celkem 24 838 000 ks drůbeže, ale soběstačnost ve stejném roce dosahovala hodnoty 84,9 %, tedy téměř o 20 % vyšší, než v roce 2020.

V případě potravinářské výroby je situace u posuzování odvětvových kritérií jednodušší, neboť ČSÚ každoročně eviduje kapacitu výroby v ČR u určitých druhů surovin a tyto hodnoty tak lze snadno porovnat s nastavenými kritérii. V tabulce 12 je uvedeno srovnání mezi odvětvovými kritérii v potravinářské výrobě a roční produkcí v ČR dle dat ČSÚ (41).

Tabulka 12 - porovnání odvětvových kritérií s výrobou v roce 2019 [zdroj vlastní]

Odvětvové kritérium	**Hodnota kritéria**	**Výroba v roce 2019**	**Jednotka**	**Podíl kritéria na výrobě (v %)**
mlýnské výrobky	80 000	725 141	t	11
cukr	230 000	590 000	t	39
pekařské výrobky	600 000	576 061	t	104
mléko	65	3 073	mil. l.	2
maso	200 000	167 902 (hovězí) 286 762 (vepřové) 262 843 (drůbeží)	t	119 70 76

Z této tabulky vyplývají dva závěry. Prvním z nich je skutečnost, že odvětvová kritéria jsou nastavena u jednotlivých základních typů potravin na výrazně

odlišných úrovních, kdy podíl na výrobě se pohybuje od 2 % v případě mléka až po 119 % v případě hovězího masa. Druhou skutečností je to, že některá z těchto kritérií jsou nastavena takovým způsobem, že nejsou naplnitelná ani celkovou výrobou v ČR (viz produkce pekařských výrobků či hovězího masa).

C) Navrhované opatření

Po posouzení současného stavu odvětvových kritérií v odvětví zdravotnictví a v odvětví potravinářství a zemědělství je navrhované opatření ke zlepšení současného systému následující.

Odvětvová kritéria by měla sloužit k prvotní identifikaci potenciálních prvků KI podle typu poskytované služby. Jejich stanovení by tak mělo být zaměřeno pouze na popis, resp. výčet typů objektů, zařízení a služeb, které jsou pro bezpečnost státu nezbytné. Kritičnost daného objektu pak bude posuzována pomocí průřezových kritérií. Zároveň to znamená, že odvětvová kritéria by neměla být stanovena ve formě mezních hodnot, a to i z důvodu jejich proměnlivosti v čase.

Zároveň, pokud bude kritičnost posuzována pouze pomocí průřezových kritérií, bude zajištěno sjednocení úrovně významnosti prvků KI v jednotlivých odvětvích, čímž dojde k zamezení vzniku situace, kdy v některých odvětvích nejsou určeny žádné prvky KI a v jiných jsou určeny i prvky, které jsou z hlediska základní definice kritické infrastruktury méně významné.

Tento princip, kdy odvětvové kritérium pouze stanovuje kritické odvětví, ale ne míru významnosti, byl použit u některých odvětví KI již v současném systému kritické infrastruktury a k zajištění systémovosti by měl být aplikován i na ostatní odvětvová kritéria.

Další možností by mohl být odklon od identifikace a určování jednotlivých prvků KI směrem k identifikaci a určování samotných subjektů KI podle kritičnosti jimi poskytované služby. Výhodou této úpravy je skutečnost, že mohou být identifikovány a určeny subjekty, jejichž infrastruktura je roztříštěna na velké množství menších objektů či zařízení, která jednotlivě nesplňují kritéria pro určení prvku KI, ale jejich síť již dosahuje značného významu. Nevýhodu tohoto pojetí však v kontextu ČR vidím zejména ve ztrátě kontroly nad jednotlivými prvky KI a ztížení identifikace prvků KI na území ve vazbě na krizové řízení. Více o tomto řešení je uvedeno v kapitole 6.

5.7.2 Decentralizace systému v případě soukromých prvků KI

Z výsledků komparace vyplývají, v případě možných opatření ke zlepšení aktuálního stavu, dva možné přístupy k řešení této slabé stránky. Prvním z nich je možnost prohloubení decentralizace podobným způsobem jako ve finském modelu, kde systém kritické infrastruktury zastřešuje NESA, ale jednotlivá odvětví fungují samostatně a odděleně. Druhou možností je naopak posílení centralizace celého systému s posílením kompetencí jednoho ministerstva nebo jiného ÚSÚ, což je případ slovenského modelu. Zde má Ministerstvo vnitra SR významnou pravomoc ovlivňovat nejen podobu průřezových kritérií, ale také odvětvových kritérií. Zároveň posuzuje veškeré návrhy na určování nových prvků KI, a to jak těch státních, tak také soukromých, které jsou v kompetenci věcně příslušných ministerstev a jiných ÚSÚ.

V souvislosti s provedenou SWOT analýzou a také v kontextu předchozí podkapitoly, jež se týká nevhodně nastavených kritérií, není v podmínkách ČR vhodné vydávat se cestou větší decentralizace celého systému, neboť dotčení aktéři k celé problematice přistupují odlišným způsobem a přikládají jí odlišný

význam. Ještě větší decentralizace by tak mohla vést k úplné ztrátě kontroly nad celým systémem a ke vzniku nesystémových řešení v rámci jednotlivých odvětví.

Cílem však zároveň není převedení co největšího počtu kompetencí pod jeden resort. K problematice kritické infrastruktury je stále potřeba přistupovat jako k odvětvové záležitosti, kde jsou kompetence a znalost odvětví ze strany věcně příslušných ministerstev a jiných ÚSÚ velmi významné. Úprava kompetencí by tak měla směřovat zejména ke zvýšení kontroly a dohledu nad systémem kritické infrastruktury jako celku.

Z tohoto pohledu se jako problematická část jeví právě oblast určování prvků KI, jejichž provozovatelem není organizační složka státu, kde je celý proces identifikace a určování prvků KI plně v kompetenci věcně příslušných ministerstev a jiných ÚSÚ. Ministerstvo vnitra, jako hlavní gestor za celou problematiku, je pak v tomto případě pouze příjemcem informace o určení těchto prvků KI, přičemž jeho možnosti ovlivnit samotný proces určování jsou prakticky nulové.

To je dáno samotným nastavením procesu určování soukromých prvků KI, kdy věcně příslušné ministerstvo a jiný ÚSÚ nejprve provede určení takovýchto prvků KI cestou opatření obecné povahy a následně o tomto určení Ministerstvo vnitra informuje. Dochází tedy k situaci, kdy je Ministerstvo vnitra o nových prvcích KI informováno až po jejich určení. Pokud by bylo toto určení vyhodnoceno jako problematické (např. z důvodu nevhodně aplikovaných určujících kritérií) lze tuto záležitost pomocí zákonných nástrojů řešit pouze pomocí ustanovení § 10 odst. 3 krizového zákona, dle kterého řeší rozpory v oblasti krizového řízení (do kterého spadá taky problematika kritické infrastruktury) ministr vnitra. Přesto se jedná o nástroj, který lze použít až v okamžiku, kdy už k samotnému určení došlo.

Druhý problematický aspekt je skutečnost, že mezi určením prvků KI a informováním o tomto určení vzniká časový prostor, kdy již byly určeny nové prvky KI, ale gestor za problematiku o tomto určení ještě nebyl informován. V krizovém zákoně je uvedeno, že o určení je Ministerstvo vnitra informováno bez zbytečného odkladu, což je však lhůta, která přímo neurčuje, v jakém konkrétním časovém okamžiku je třeba povinnost splnit. Jde tak o neurčitě krátkou lhůtu, přičemž doba trvání lhůty závisí na okolnostech konkrétního případu (44).

Další oblastí možné centralizace je problematika kontrol plnění povinností subjektů KI, které provádějí věcně příslušná ministerstva a jiné ÚSÚ v rámci jimi řešených odvětví KI. O výsledcích těchto kontrol přitom věcně příslušné ministerstvo nebo jiný ÚSÚ nemá povinnost informovat Ministerstvo vnitra. V současné době tak sice kontrolní činnost probíhá, ale hlavní gestor za problematiku nezískává žádné informace o stavu plnění povinností ze strany subjektů KI v jednotlivých odvětvích, ani o aktivitě věcně příslušných ministerstev a jiných ÚSÚ.

V souvislosti s výše uvedeným a s využitím slovenského modelu tak navrhuji upravení kompetencí tak, aby v případě, kdy dochází k určení prvku KI opatřením obecné povahy, bylo nejprve Ministerstvo vnitra požádáno o posouzení tohoto určení a věcně příslušné ministerstvo nebo jiný ÚSÚ by přistoupil k určení takového prvku až po obdržení souhlasného stanoviska od Ministerstva vnitra.

Druhou navrhovanou úpravou je povinnost věcně příslušných ministerstev a jiných ÚSÚ zasílat jedenkrát ročně souhrnnou zprávu o provedených kontrolách subjektů KI Ministerstvu vnitra.

5.7.3 Neexistence standardů ochrany

Jak je uvedeno v kapitole 3, v současné době neexistují obecné standardy ochrany prvků KI, kdy k fyzické ochraně kritické infrastruktury existuje pouze jedna předběžná technická norma a v případě KII jsou požadavky na ochranu řešeny pomocí vyhlášky o kybernetické bezpečnosti. K závěru, že stanovení jednotných požadavků na ochranu je velice komplikované, neboť konkrétní opatření na ochranu prvků KI se mezi odvětvími výrazně liší, se přiklání také Neag z Akademie pozemních sil Nicolae Balescu v Rumunsku (45). Místo cesty konkrétních standardů ochrany tak navrhuji se vydat spíše cestou rozšíření ochrany KI o prvky resilience, které v současné legislativní úpravě řešeny nejsou. Prvním řešením by tak mělo být zavedení resilience do krizového zákona a navázání tohoto pojmu na povinnosti subjektu KI uvedené v § 29a. Resilience by měla být řešena jak skrze posílení celého systému a zvýšení schopnosti návratu do normálního stavu, tak i skrze budování úzkého partnerství mezi veřejným a soukromým sektorem. Možnou cestou je vytvoření poolů (podle finského modelu), kde by však hlavní zastoupení neměl ústřední orgán pro tuto problematiku, jak je tomu ve Finsku v případě agentury NESA, ale gestoři za jednotlivá odvětví. Specifické otázky a standardy ochrany kritické infrastruktury by pak byly řešeny právě na této úrovni. Ministerstvo vnitra, jako gestor za problematiku na národní úrovni, by bylo o činnosti těchto poolů průběžně informováno.

Další krok k posílení ochrany KI vede cestou investic zvyšujících resilienci prvků KI. Slovenský model v tomto kontextu zavádí povinnost uplatňovat při modernizaci prvku KI technologie, které zabezpečují jeho ochranu (30). Tento přístup je však již příliš direktivní, neboť subjektu KI stanovuje povinnost zabezpečit ochranu prvku KI a při modernizaci vynakládat další finanční prostředky ke zvýšení ochrany.

V současné české úpravě má subjekt KI povinnost chránit prvek KI proti jeho narušení, není zde však nastaven systém financování opatření, která by zabezpečovala tuto ochranu. Navíc, jak uvádí Seidl, Šimák a Ristvej z Žilinské univerzity, výstavba a rozvoj infrastruktury je pro soukromé subjekty z pohledu krátkého časového horizontu velice nákladná záležitost a návratnost takovéto investice je navíc nejistá, nebo se projeví až v dlouhodobém horizontu. Pro soukromé subjekty jsou tak takové investice málo atraktivní. Proto je v této oblasti nezbytná činnost státu a využití veřejných zdrojů (46). Z tohoto důvodu by možnou cestou bylo rozšíření financování v této oblasti. Příležitostí by v tomto mohlo být zajištění finančních zdrojů z evropských fondů, jako například již zmiňovaného ISF.

5.7.4 Absence sankcí

Jak bylo uvedeno ve SWOT analýze, současný systém kritické infrastruktury v ČR nemá stanoveny sankce za neplnění povinností subjektu KI dle krizového zákona. V platném znění jsou sankce obsaženy v ustanovení § 34 krizového zákona, přičemž právnických a podnikajících fyzických osob se konkrétně týká ustanovení § 34a. Výše sankce za nesplnění povinností uvedených v odstavcích 1 až 3 tohoto ustanovení může dosáhnout celkové výše 3 000 000 Kč. Nejsou zde však řešeny přestupky v případě porušení povinností subjektu KI (10), tedy např. povinnosti zpracovat plán krizové připravenosti subjektu KI či určit styčného bezpečnostního zaměstnance.

Tento nedostatek se nejvíce projevuje v případě kompetence věcně příslušných ministerstev a jiných ÚSÚ provádět kontrolu subjektů KI (10), kdy z důvodu neexistujících sankcí je vymahatelnost jakýchkoliv zjištěných nedostatků problematická až nereálná. Zavedení sankcí za neplnění povinností

tak může zásadním způsobem zefektivnit systém kritické infrastruktury v ČR. Cílem sankcí však tomto případě nesmí být likvidace dotčeného subjektu KI, nebo výrazné finanční zatížení dotčených subjektů KI, což by se mělo odrážet i na samotném nastavení výše sankcí.

V případě konkrétního nastavení za neplnění povinností pak lze vycházet z výše, která je již stanovena § 34a. Variantou by mohla být i vyšší částka, jako je tomu v případě slovenského modelu, která v přepočtu dosahuje maximální výše přibližně 5 000 000 Kč[3] (30), v závislosti na aktuálním směnném kurzu. Vzhledem k rozsáhlým povinnostem, které subjekty KI musí plnit, však je vhodnější volit spíše nižší částku, a proto se částka do 3 000 000 Kč jeví jako vhodnější.

Pravomoc udělit sankci za neplnění povinností subjektu KI podle krizového zákona by měla být udělena věcně příslušnému ministerstvu a jinému ÚSÚ, které je oprávněno provádět kontroly podle krizového zákona a má tak zároveň nástroj pro ověření zde subjekt KI povinnosti plní a v jaké míře. V souladu s výše uvedeným navrhuji úpravu krizového zákona následujícím tak aby v samostatném paragrafu, který by následoval po § 34a, byly přidány přestupky subjektů KI. Konkrétně by se subjekt KI dopustil přestupku v případě, že by neplnil povinnost stanovené v § 29a. Výše pokuty by odpovídala sankci uvedené v § 34a, tedy do 3 000 000 Kč. Přestupky subjektů KI by následně projednávalo věcně příslušné ministerstvo nebo jiný ÚSÚ.

[3] Pokuta za porušení či neplnění povinností podle zákona o KI může být uložena v rozsahu 1 000 až 200 000 € (30).

6. DISKUSE

V rámci této kapitoly jsou výsledky této diplomové práce ověřeny a porovnány s výsledky jiných odborných prací či výzkumů z oblasti ochrany kritické infrastruktury. Hodnoceny jsou jak výsledky provedené SWOT analýzy tak také navrhovaná opatření, jež jsou obsahem kapitoly 5.

Metoda SWOT analýzy použitá pro zhodnocení aktuálního stavu systému kritické infrastruktury využili i někteří odborníci zabývající se problematikou zvyšování ochrany kritické infrastruktury jako například Skalická, která využila metodu SWOT analýzy ve svém článku *Ochrana a obrana kritické infrastruktury: úskalí a možnosti rozvoje v České republice*, který vyšel v odborném časopise *The Science for Population Protection*. Z pohledu porovnání výsledků této diplomové práce se tak jedná o ideální zdroj, neboť předmět i metoda použitá k hodnocení jsou stejné, přesto v některých oblastech dochází autorka k odlišným závěrům, než jsou obsahem této práce.

Skalická rovněž identifikovala jako silné stránky systému kritické infrastruktury v ČR její legislativní ukotvení, provázanost se systémem krizového řízení (a také s dalšími oblastmi jako je ochrana obyvatelstva) či aktivitu dotčených aktérů na úrovni EU. Kromě těchto silných stránek však také zmiňuje mj. existenci analýzy hrozeb, která je využitelná jako možný výchozí podklad pro identifikaci hrozeb ochrany kritické infrastruktury či zavedený bezpečnostní výzkum v této oblasti (47). S těmito identifikovanými jevy lze souhlasit, neboť i v aktuálním návrhu Směrnice CER je otázka provedení analýzy hrozeb (ačkoliv v tomto kontextu se jedná přímo o hrozby pro kritickou infrastrukturu, resp. kritický subjekt) jako jedna z klíčových činností, která má

být ze strany členských států provedena a ve tříletých cyklech pravidelně aktualizována (19).

V případě slabých stránek již lze vypozorovat výraznější rozdíly oproti výsledkům této diplomové práce. Skalická identifikovala nevhodně nastavená kritéria pro určování prvků KI, což byl i jeden z výsledků této práce či nedostatečná metodická podpora gestorů za jednotlivá odvětví KI, což bylo v této práci řešeno v rámci slabé stránky decentralizace systému kritické infrastruktury. Kromě těchto slabých stránek však Skalická také identifikovala další slabé stránky, které v diplomové práci identifikovány nebyly. Jedná se například o nesoulad mezi pojetím kritické a obranné infrastruktury, dále neexistence strategického dokumentu, finanční nákladnost modernizace infrastruktury, absence zapojení územní úrovně či nedostatečná spolupráce mezi veřejnou a soukromou sférou (47).

V případě neexistence strategického dokumentu, je toto tvrzení z části pravdivé. V současné době neexistuje samostatný koncepční či strategický dokument, který by řešil pouze problematiku kritické infrastruktury a její rozvoj v ČR. V případě systému kritické infrastruktury v ČR je však potřeba tento systém vnímat jako nedílnou součást systému krizového řízení, kvůli čemuž byla tato problematika vůbec implementována do krizového zákona. Rozvoj systému krizového řízení je pak spolu s kritickou infrastrukturou koncepčně a strategicky řešen koncepcí ochrany obyvatelstva (6).

V případě nesouladu mezi kritickou a obranou infrastrukturou autorka uvádí, že zlepšení systému by pomohlo provázání obranné a kritické infrastruktury například vytvořením *„bezpečnostní infrastruktury státu“, která by se členila na podkategorie (obrannou infrastrukturu a kritickou), přičemž určující pro uplatnění přístupů ochrany či obrany infrastruktury by byl vyhlášený krizový stav*“. Problémem

tohoto opatření však, jak autorka dodává, je odlišné pojetí kritické a obranné infrastruktury ve vztahu k území, kdy kritická infrastruktura byla v roce 2011 implementována pouze na úrovni nadnárodní (v tomto kontextu se jedná o prvky EKI) a národní (prvky KI), naproti tomu obranná infrastruktura, konkrétně objekty možného napadení (dále jen „OMN"), řeší i územní úroveň (až na úroveň obce). Právě nesoulad pak dle autorky brání v provázání těchto dvou oblastí.

S tímto však s autorkou nesouhlasím, neboť ač oba typy infrastruktury vykazují určité stejné znaky, nejedná se o identické problematiky. Předně, OMN zahrnuje objekty, které jsou svojí funkcí či umístěním nezbytné pro zabezpečení mobilizace ozbrojených sil na území kraje, plnění opatření k zajišťování obrany na území kraje, zajištění základních životních potřeb obyvatel kraje a fungování státní správy a samosprávy na tomto území. Z tohoto pohledu se tak OMN může překrývat s kritickou infrastrukturou v otázce zajišťování základních životních potřeb obyvatelstva. Nicméně dle kategorizace OMN je zajišťování těchto potřeb navázáno na situaci při zajišťování obrany ČR (48). Kritická infrastruktura je naproti tomu dle definice prvkem KI nebo systémem prvků KI, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu (10). Jedná se tedy infrastrukturu, jejíž funkce a poskytování služby je kritické bez ohledu, zda je tato služba poskytována během nevojenských či vojenských krizových stavů. Naopak její narušení může vést ke vzniku krizové situace.

Dále, jelikož je problematika kritické infrastruktury provázána se systémem krizového řízení, byl zvolen model, kdy kritická infrastruktura je řešena pouze na národní úrovni, neboť v systému krizového řízení již existuje identifikace klíčových objektů a subjektů na úrovni kraje a obce s rozšířenou působností, a to dle ustanovení § 29 krizového zákona (10).

S autorkou se naopak ztotožňuji v případě nutnosti zvýšit spolupráci a komunikaci mezi orgány veřejné správy a soukromými subjekty, přičemž význam této spolupráce zmiňuje také Dvořák s Luskovou, a to zejména z toho důvodu, že drtivá většina prvků kritické infrastruktury je ve vlastnictví, nebo je provozována, soukromými subjekty. V kontextu systému kritické infrastruktury SR se tak jedná o více než 90 % všech prvků KI. V ČR je tato dominance soukromých prvků KI méně výrazná (jedná se přibližně o 75 % všech prvků KI), to však nijak neubírá na významu prohubování spolupráce (49).

Dle Dvořáka a Luskové je pak spolupráce mezi veřejným a soukromým sektorem zásadní zejména z důvodu důkladnějšího posuzování vzájemných závislostí mezi jednotlivými prvky KI a dopadů těchto závislostí na úrovni celých systémů (49).

K významnosti prohlubování spolupráce se přiklání také Cirdei, který spolupráci vnímá v kontextu odlišných rolí a kompetencí soukromých a veřejných aktérů v systému kritické infrastruktury. Rolí vlastníků a provozovatelů KI pak je přijímání adekvátních opatření zaměřených na zvyšování ochrany prvků KI, naopak aktéři z veřejného sektoru mohou v rámci systému přispívat zejména přijímáním adekvátních a vhodných legislativních i nelegislativních nástrojů, které slouží k podpoře provozovatelů KI pro zvyšování jejich ochrany. Cirdei zároveň otázku spolupráce pojímá jako jeden z prvků zvyšování resilience kritické infrastruktury, neboť vhodně nastavená spolupráce mezi všemi zainteresovanými aktéry ve svém důsledku umožňuje výrazné zkrácení doby obnovy a návratu do normální stavu po narušení funkce prvku KI (50).

V kontextu zvyšování ochrany KI pak Cirdei zároveň dodává, že v současné době už přístup, který je zaměřen pouze na otázku ochrany KI, nestačí a je

potřeba ochranu KI posílit i o složku resilience. Cirdei to vysvětluje zvyšující se provázaností, kdy prvky KI již neexistují izolovaně, ale vytváří rozsáhlé propojené systémy, které jsou na sobě vzájemně závislé a v případě narušení jednoho prvku KI pak dochází k postupnému narušení i dalších, na něj navázaných prvků KI. To v konečném důsledku vede k celkovému narušení systému. Samotná ochrana KI pak takovémuto narušení není schopna zabránit a jediným řešením je zvyšování resilience, která sice nezabrání narušení funkce, ale umožní rychlý návrat do původního stavu (50).

Dalším argumentem pro zahrnutí resilience do systému kritické infrastruktury je právě skutečnost, že sebelepší a dokonalejší ochrana prvku KI nebude nikdy schopna úplně zabránit narušení funkce prvku KI, neboť se vždy mohou objevit situace nebo nové způsoby útoku, na které současné standardy ochrany nebudou dostatečné. Právě pro tyto situace je určena resilience, která zajistí, že prvek KI, jehož funkce byla narušena, bude schopen v přijatelném čase obnovit svou činnost v dostatečné míře. Cirdei však dodává, že resilience nesmí být vnímána jako protiklad ochrany, ale právě naopak. Stále se musí k resilienci přistupovat jako k doplňkové vrstvě ochrany a jedná se tak o dvě propojené oblasti, které se vzájemně doplňují (50).

Pro porovnání adekvátnosti opatření navrhovaných v této diplomové práci je využitelná také hodnoticí studie ke Směrnici EKI a na ni navazující návrh Směrnice CER, které byly ve stručnosti představeny v kapitole 3.

V hodnocení Směrnice EKI přineslo jasné konstatování, že některé z bodů této směrnice jsou i v současné době stále relevantní, ale v mnoha bodech je již Směrnice EKI zastaralá a je potřeba provést její důkladnější revizi. Hlavním důvodem této potřeby je především razantní změna podmínek od roku 2008. Konkrétně se jedná potřebu implementace nových postupů a nástrojů v této

oblasti jako například koncept resilience a identifikaci vzájemných závislostí. Významnou roli také hraje změna bezpečnostního prostředí, či zvyšování významu kybernetické bezpečnosti (18).

V souladu s tímto závěrem potom byla navržena možná opatření ke zlepšení aktuálního stavu na úrovni EU. Ve studii jich bylo identifikováno celkem osm a jejich cílem byla úprava stávajícího znění Směrnice EKI, kdy každé opatření bylo definováno třemi možnými scénáři odstupňovanými podle obtížnosti jeho implementace. Opatření byla zaměřena především na otázku zpřesnění a rozšíření definic, a to konkrétně ve vazbě na definování pojmu resilience v kontextu kritických infrastruktur, dále na rozšíření odvětví EKI do dalších oblastí jako jsou komunikační a informační systémy a vesmír. Hodnocení směrnice rovněž přišlo s návrhem úpravy kompetencí jednotlivých aktérů, a to i na národní úrovni, kde cílem mělo být zahrnutí subjektů KI do procesu identifikace a určování nových prvků KI, dále také opatření určená k posílení spolupráce mezi veřejným a soukromým sektorem (vytvořením separátní pracovní skupiny pro zástupce subjektů EKI) a zefektivnění poskytování finančních prostředků na ochranu kritické infrastruktury na úrovni EU (18).

Na Hodnotící studii Směrnice EKI poté na konci roku 2020 navázalo představení návrhu nové Směrnice CER, jejímž cílem je souhrnná úprava systému kritické infrastruktury na úrovni EU s výrazným přesahem do národních systémů kritických infrastruktur členských států. Návrh Směrnice CER již konkrétně popisuje změny systému kritické infrastruktury, a to ve všech podstatných oblastech, tedy v oblasti definic, identifikace, určování a ochrany KI, resp. kritických subjektů, které mají pojem kritická infrastruktura nahradit (18).

Jelikož nejzásadnější změny jsou navrhovány v oblasti identifikace a určování kritické infrastruktury, je návrh Směrnice CER vhodným dokumentem

ke srovnání výsledků této diplomové práce, a to právě v oblasti navrhované úpravy odvětvových kritérií.

Výrazným posunem Směrnice CER je rozšíření problematiky na národní úroveň, kdy směrnice CER definuje deset odvětví KI (resp. poskytovatelů základních služeb). Zásadní změnou v tomto případě je odlišný přístup k určování kritické infrastruktury, kdy důraz není kladen na konkrétní prvky KI, ale přímo na samotné subjekty, které poskytují určitou základní službu. Tento přístup je tak odlišný od toho, který je nastaven v systému kritické infrastruktury v ČR, jež je naopak zaměřen na určování konkrétních prvků KI (19).

I přes své nezpochybnitelné výhody, související s možností určovat i subjekty, které poskytují základní služby pomocí sítě malých prvků, jež nedosahují kritických hodnot, má tento nový způsob určování v kontextu ČR jednu velkou nevýhodu, která souvisí s úzkým propojením problematiky kritické infrastruktury se systémem krizového řízení. Určování samotných subjektů totiž výrazně znemožňuje přesnou identifikaci kritické infrastruktury v území ze strany dotčených orgánů, které s těmito daty dále pracují i v rámci krizové plánovací dokumentace.

V případě určujících kritérií pak Směrnice CER navrhuje obdobný model odvětvových a průřezových kritérií jaký je navržen i v této práci, kdy odvětvová kritéria slouží k identifikaci základních služeb, které mají být řešeny touto směrnicí a míra kritičnosti je stanovena pouze skrze průřezová kritéria (19).

7. ZÁVĚR

Cílem diplomové práce bylo analyzovat systém kritické infrastruktury v České republice, přičemž k tomuto hodnocení bylo využito metody SWOT analýzy doplněné o párové porovnání identifikovaných jevů pomocí multikriteriální analýzy AHP a následnou selekci pomocí Paretova pravidla. Druhým cílem diplomové práce potom bylo navržení opatření ke zlepšení a zefektivnění současného stavu, kdy navrhovaná opatření vycházela mimo jiné i z komparace se systémy kritické infrastruktury Slovenska a Finska.

V rámci hlavních cílů byly rovněž řešeny stanovené hypotézy, kdy po provedené analýze došlo k potvrzení první a třetí hypotézy, které se týkaly rozdílnosti přístupu k identifikaci a určování prvků KI v jednotlivých odvětvích a otázky dostatečnosti implementace Směrnice EKI v podmínkách ČR.

Naopak v případě druhé hypotézy došlo k jejímu vyvrácení, neboť komparace systémů kritické infrastruktury poukázala na výrazné rozdíly mezi porovnávanými systémy, a to nejen v oblasti určování a identifikace prvků KI, ale také v oblasti jejich ochrany před narušením provozu.

V návaznosti na výsledky analýzy a na vyhodnocení hypotéz byly následně identifikovány čtyři oblasti, ve kterých byla navržena opatření ke zlepšení aktuálního stavu. Jednalo se o oblast odvětvových kritérií, kde závěrem je doporučení úpravy odvětvových kritérií jako kritérií bez stanovených mezních hodnot, kdy je míra kritičnosti posuzována pouze pomocí průřezových kritérií. Dalším navrhovaným opatřením je úprava kompetencí jednotlivých gestorů, jež má za cíl posílit koordinační roli Ministerstva vnitra a zavedení sankcí pro subjekty KI v případě neplnění opatření dle krizového zákona. Posledním

z navrhovaných opatření je rozšíření ochrany kritické infrastruktury o oblast resilience a o užší spolupráci mezi veřejným a soukromým sektorem podle finského vzoru.

V případě opatření na úpravu systému kritické infrastruktury se poté jedná o konkrétní cílené návrhy, jež nemají za cíl kompletní přepracování aktuálního systému, ale pouze změnu v identifikovaných slabých oblastech. Systém kritické infrastruktury je v podmínkách ČR implementován na dostatečné úrovni, a proto by zásadnější zásahy mohli být spíše kontraproduktivní.

Přesto v nejbližších letech pravděpodobně čeká tento systém radikálnější proměna, a to ve vztahu k možnému přijetí nové Směrnice CER. Teprve až budoucnost však ukáže, nakolik povede nové pojetí kritické infrastruktury ke zlepšení tohoto systému oproti současnému stavu.

8. SEZNAM POUŽITÝCH ZKRATEK

CER	Critical Entities Resilience
ČSÚ	**Č**eský statistický úřad
ČR	Česká republika
EKI	evropská kritická infrastruktura
EU	Evropská unie
ISF	Fond pro vnitřní bezpečnost
KII	kritická informační infrastruktura
MV-GŘ HZS ČR	Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru České republiky
NESA	Agentura pro nouzové zásobování Finska
NESO	Národní organizace pro nouzové zásobování Finska
odvětví KI	**o**dvětví kritické infrastruktury
PKP subjektu KI	plán krizové připravenosti subjektu kritické infrastruktury
prvek KI	prvek kritické infrastruktury
provozovatel KI	provozovatel kritické infrastruktury

SR	Slovenská republika
subjekt KI	subjekt kritické infrastruktury
ÚSÚ	jiný ústřední správní úřad

9. SEZNAM POUŽITÉ LITERATURY

1. ŘEHÁK, David, HROMADA, Martin a ŠENOVSKÝ, Pavel. *Resilience kritické infratruktury: Teorie, principy, metody.* Ostrava : Sdružení požárního a bezpečnostního inženýrství, z.s., 2019. ISBN 978-80-7385-224-5.

2. LINHART, Petr a RICHTER, Rostislav. *Ochrana kritické infrastruktury*. 112 - odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva, 2003, 3.

3. MARTÍNEK, Bohumír. *Východiska a principy zajištění ochrany kritické infrastruktury v České republice*. 112 - odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva, 2008, 4.

4. KOLEŇÁK, Ivan, MIKLÓS, Daniel a ROSINOVÁ, Marika. *Novelizace krizového zákona*. Časopis 112, 2011, Sv. 10. ISSN 1213-7057.

5. MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Bezpečnostní strategie ČR* [online]. Praha, 2015 [cit. 15.10.2020] Dostupné z: https://www.vlada.cz/cz/ppov/brs/dokumenty/vyznamne-dokumenty-v-oblasti-bezpecnosti-ceske-republiky-18963/

6. MV-GŘ HZS ČR. *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030.* Praha, 2013. ISBN 978-80-86466-50-7.

7. MV-GŘ HZS ČR. *Zpráva o stavu ochrany obyvatelstva v České republice 2018* [online]. Praha, 2018 [cit. 20. 10. 2020]. Dostupné z: https://www.hzscr.cz/clanek/ochrana-obyvatelstva-v-ceske-republice.aspx

8. MV-GŘ HZS ČR. *Komplexní strategie k řešení problematiky kritické infrastruktury* [online]. Praha, 2010 [cit. 20.10.2020] Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/komplexni-strategie-cr-k-reseni-problematiky-kritic ke-infrastruktury-2010?typ=tematicky&v=f60814df7922813fb693699fd8ad749e

9. MV-GŘ HZS ČR. *Národní program ohrany kritické infrastruktury* [online]. Praha, 2010 [cit. 20.10.2020]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/narodni-program-ochrany-kriticke-infrastruktury?t yp=download

10. ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů. In: *Sbírka zákonů*. 9. srpna 2000. ISSN 1211-1244.

11. EVROPSKÁ UNIE. Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. In: *Úřední věstník Evropské unie. 23. prosince 2008.*

12. ČESKÁ REPUBLIKA. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů*. 30. prosince 2010. ISSN 1211-1244.

13. ČESKÁ REPUBLIKA. Zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích. In: *Sbírka zákonů*. 21. července 2000. ISSN 1211-1244.

14. ČESKÁ REPUBLIKA. Zákon č. 500/2004 Sb., Správní řád. In: *Sbírka zákonů*. 24. července 2004. ISSN 1211-1244.

15. ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Sbírka zákonů*. 23. července 2014. ISSN 1211-1244.

16. ČESKÁ REPUBLIKA. Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*, 29. prosince 2000, ISSN: 1211-1244.

17. MINISTERSTVO PRŮMYSLU A OBCHODU ČR. *Postup pro vytvoření seznamu strategických objektů a určení jejich priorit a pro definici scénářů narušení dodávek elektrické energie velkého rozsahu* [online]. Praha, 2019. *Dostupné z: https://www.mpo.cz/cz/energetika/elektroenergetika/elektroenergetika/postup-pro-vytvoreni-seznamu-strategickych-objektu-a-urceni-jejich-priorit-a-pro-definici-scenaru-naruseni-dodavek-elektricke-energie-velkeho-rozsahu--249971/.*

18. DG HOME. *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* [online]. Lucemburk: Publications Office of European Union, 2020 [cit. 30.11.2020]. ISBN 978-92-76-19510-8. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/118dcd3d-b041-11ea-bb7a-01aa75ed71a1

19. DG HOME. *Návrh Směrnice Evropského parlamentu a Rady o posílení odolnosti kritických subjektů* [online]. Brusel, 16. prosince 2020 [cit. 30.11.2020]. *Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-b27b-01aa75ed71a1.0016.02/DOC_1&format=PDF.*

20. KEŘKOVSKÝ, Miloslav, VYKYPĚL, Ondřej. *Strategické řízení: teorie pro praxi.* 1 vydání. Praha: C. H. Beck, 2002. ISBN 80-7179-578-X.

21. AKSystem.cz. *Co je to Paretovo pravidlo a jak funguje* [online]. 2020 [cit. 29.04.2021]. Dostupné z: https://www.aksystem.cz/co-je-to-paretovo-pravidlo-a-jak-funguje-p10313/#gallery.

22. FOTR, Jiří,DĚDINA, Jiří a HRŮZOVÁ, Helena. *Manažerské rozhodování*. 2. aktualiz. vyd. Praha: Ekopress, 2000. ISBN 80-86119-20-3.

23. KORVINY, Petr. *MCA7* [online]. 2021 [cit. 30.03.2021] Dostupné z: https://korviny.cz/korviny/homepage/mca7#.

24. MOLNÁR, Zdeněk, MILDEOVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRIXÍ, Radim, KALINA, Jaroslav. *Pokročilé metody vědecké práce*. Praha: Profess Consulting, s.r.o., 2012. ISBN 978-80-7259-064-3.

25. EVROPSKÁ KOMISE. *Internal Security Fund - Police* [online]. 2020 [cit. 15.04.2021] *Dostupné z: https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police_en.*

26. VLÁDA ČR. *Usnesení vlády ze dne 30. března 2020 č. 332 o přijetí krizového opatření* [online]. 2020 [cit. 10.04.2021] Dostupné z: https://apps.odok.cz/attachment/-/down/IHOABN7SBKG8.

27. ASOCIACE KRITICKÉ INFRASTRUKTURY ČR. *Stanovisko AKI ČR k usnesení vlády č. 332* [online]. 2020 [cit. 10.04.2021] Dostupné z: https://www.akicr.cz/2020/04/01/stanovisko-aki-cr-k-usneseni-vlady-c-332/.

28. VLÁDA ČR. *Usnesení vlády ze dne 1. dubna 2020 č. 377 o přijeté krizového opatření* [online]. 2020 [10.04.2021] Dostupné z: https://apps.odok.cz/attachment/-/down/IHOABNAA2FGO.

29. SELINGER, Petr. *Kritická infraštruktúra a možnosti jej ochrany* [online]. Žilina: Krízový manažment, 2/2011 [cit. 06.04.2021]. ISSN 1336-0019. Dostupné z: https://www.fbi.uniza.sk/stranka/casopis-krizovy-manazment-cislo-2-2011

30. SLOVENSKÁ REPUBLIKA. Zákon č. 45/2011 Z. z.., o kritickej infraštruktúre. In: *Zbierka zákonov*, 8. února 2011.

31. CHOVANČÍKOVÁ, Nikola. *Odolnosť prvkov kritickej infraštruktúry* [online]. Žilina: Krízový Manažment, 2/2018 [cit. 06.04.2021]. ISSN: 1336-0019. Dostupné z: https://www.fbi.uniza.sk/stranka/casopis-krizovy-manazment-cislo-2-2018

32. BAUBION, Charles. *What the World Can Learn from Finland's Brush with Critical Infrastructure Failure* [online]. BRINK, 2019 [cit. 4.10.2021]. Dostupné z: https://www.brinknews.com/what-the-world-can-learn-from-finlands-brush-with-critical-infrastructure-failure/.

33. OECD. *Good governance for Critical Infrastructure Resilience* [online]. Paříž: OECD Publishing, 2019 [cit. 16.04.2021]. ISBN 978-92-64-410503, Dostupné z: https://www.oecd-ilibrary.org/governance/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.

34. FINSKÁ REPUBLIKA. *Government Decision no. 1048/2018 on Objectives of Security of Supply* [online]. Helsinky, 2018 [cit. 12.04.2021]. *Dostupné z: https://tem.fi/documents/1410877/2095070/Government+Decision+on+the+Objectives+of+Security+of+Supply/cf19f480-dc61-b59c-3926-11857f811bfa/Government+Decision+on+the+Objectives+of+Security+of+Supply.pdf.*

35. SECURITY COMMITTEE OF FINLAND. *The Security Strategy for Society* [online]. Helsinky: 2017 [cit. 12.04.2021]. ISBN 978-951-25-2963-6, Dostupné z: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

36. GJESVIK, Lars. *Comparing Cyber Security: Critical Infrastructure Protection in Norway, the UK and Finland* [online]. Oslo: Norwegian Institute of International

Affairs, 2019 [cit. 6.10.2021]. ISSN: 1894-650X, Dostupné z: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2598280/NUPI_Report_5_2019_Gjesvik.pdf?sequence=1&isAllowed=y.

37. OECD. *Public Private Partnerships for Critical Infrastructures Resilience in Finland* [online]. 2019 [cit. 12.04.2021] Dostupné z: https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/publicprivatepartnershipsforcriticalinfrastructuresresilienceinfinland.htm#tab_description.

38. FINGRID. *Nordic Power System and Interconnections with other Systems* [online]. 2021 [cit. 18.04.2021] Dostupné z: https://www.fingrid.fi/en/grid/power-transmission/nordic-power-system-and-interconnections-with-other-systems/.

39. FAKULTNÍ NEMOCNICE V MOTOLE. *Fakultní nemocnice v Motole v číslech* [online]. 2021 [cit. 29.04.2021]. Dostupné z: https://www.fnmotol.cz/o-nas/historie-a-soucasnost/fakultni-nemocnice-v-motole-v-cislech/.

40. FAKULTNÍ THOMAYEROVA NEMOCNICE. *TN je nemocnice s historií a také centrum služeb, kvalitní zdravotní péče a odpočinku* [online]. 2021 [cit. 29.04.2021] Dostupné z: https://www.ftn.cz/clanky/tn-je-nemocnice-s-historii-a-take-centrum-sluzeb-kvalitni-zdravotni-pece-a-odpocinku-669/.

41. ČESKÝ STATISTICKÝ ÚŘAD. *Statistická ročenka České republiky - 2020* [online]. Praha, 2020 [cit. 29.04.2021]. ISBN: 978-80-250-3051-6 Dostupné z: https://www.czso.cz/csu/czso/statisticka-rocenka-ceske-republiky-2020.

42. ADAMCOVÁ, Pavla, NEVYHOŠTĚNÝ, Jan, CHRIPÁK, Denis. S*oběstačné Česko? Možná před 400 lety. Datový přehled ukazuje, co sníme i co vyvezeme* [online]. *Aktuálně.cz, 2021 [cit. 20.04.2021]. Dostupné z: https://zpravy.aktualne.cz/finance/nakupovani/potravinova-sobestacnost/r~a080f45caeed11eaa25cac1f6b220ee8/.*

43. ZEMĚDĚLSKÝ SVAZ ČR. *Soběstačnost ČR u potravin živočišného původu loni vzrostla*. 2014 [cit. 29.04.2021]. Dostupné z: https://www.zscr.cz/clanek/sobestacnost-cr-u-potravin-zivocisneho-puvodu-loni-vzrostla-723?cid=723&nadpis=sobestacnost-cr-u-potravin-zivocisneho-puvodu-loni-vzrostla.

44. EPRAVO. *Lhůty* [online]. 2014 [cit. 01.05.2021]. Dostupné z: https://www.epravo.cz/top/soudni-rozhodnuti/lhuty-93319.html.

45. NEAG, Mihai-Marcel. *Critical Infrastructure Protection - the Foundation of National Security* [online]. Buletin Stiintific, 2014, 19/2 [cit. 21.04.2021]. ISSN 1224-5178. Dostupné z: http://web.a.ebscohost.com/ehost/detail/detail?vid=4&sid=ed3b62c2 b3e2-4c23-98f2-c7dc1b913a03%40sessionmgr4007&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=100330493&db=a9h

46. SEIDL, Miloslav, ŠIMÁK, Ladislav, RISTVEJ, Jozef. *Enhancing the Management Level of Critical Infrastructure Protection* [online]. Logistics and Transport, 2014, 4/24 [cit. 25.04.2021]. ISSN 1734-2015. Dostupné z: http://system.logistics-and-transport.eu/index.php/main/issue/view/24

47. SKALICKÁ, Petra. *Ochrana a obrana kritické infrastruktury: úskalí a možnosti rozvoje* [online]. The Science for Population Protection, 2017, 2 [cit. 29.04.2021]. ISSN 1803-635X. Dostupné z: http://www.population protection.eu/prilohy/casopis/35/294.pdf

48. MINISTERSTVO OBRANY ČR. *Směrnice pro vyhodnocování, výběr a ochranu objektů obranné infrastruktury a stanovení rozsahu zpracováváné dokumentace*. Praha, 2018, 4. vyd.

49. LUSKOVÁ, Maria, DVOŘÁK, Zdeněk. *Applying Risk Management Process in Critical Infrastructure Protection* [online]. Interdisciplinary Description of

Complex Systems, 2019, 17/1-A [cit. 29.04.2021]. ISSN 1334-4676. Dostupné z: http://web.a.ebscohost.com/ehost/detail/detail?vid=9&sid=ed3b62c2-b3e2-4c23-98f2-c7dc1b913a03%40sessionmgr4007&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=136003886&db=a9h

50. CIRDEI, Ionut Alin. *Improving the Level of Critical Infrastructure Protection by Developing Resilience* [online]. Land Forces Academy Review, 2018, 4/92 [cit. 30.04.2021]. ISSN 2247-840X. Dostupné z: http://web.a.ebscohost.com/ehost/detail/detail?vid=11&sid=ed3b62c2-b3e2-4c23-98f2-c7dc1b913a03%40sessionmgr4007&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=133788421&db=a9h

10. SEZNAM POUŽITÝCH OBRÁZKŮ

11. SEZNAM POUŽITÝCH TABULEK

12. SEZNAM PŘÍLOH

1. **Přehled odvětvových kritérií pro určení prvku kritické infrastruktury**
2. **Přehled věcně příslušných ministerstev a jiných ústředních správních úřadů v oblasti kritické infrastruktury**
3. **Přehledy počtů prvků a subjektů kritické infrastruktury v jednotlivých odvětvích v letech 2011 až 2020**

Příloha č. 1 - Přehled odvětvových kritérií pro určení prvku kritické infrastruktury

I) ENERGETIKA

A) Elektřina
- A1) Výrobna elektřiny
  - (a) výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW,
  - (b) výrobna poskytující podpůrné služby1) s celkovým instalovaným elektrickým výkonem nejméně 100 MW,
  - (c) vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny,
  - (d) dispečink výrobce elektřiny.
- A2) Přenosová soustava
  - (a) vedení přenosové soustavy o napětí nejméně 110 kV,
  - (b) elektrická stanice přenosové soustavy o napětí nejméně 110 kV,
  - (c) technický dispečink provozovatele přenosové soustavy.
- A3) Distribuční soustava
  - (a) elektrická stanice distribuční soustavy a vedení o napětí 110 kV (stanice typu 110/10 kV, 110/22 kV a 110/35 kV a k nim patřící vedení se posuzují podle jejich strategického významu v distribuční soustavě),
  - (b) technický dispečink provozovatele distribuční soustavy.

B) Zemní plyn
- B1) Přepravní soustava
  - (a) vysokotlaký tranzitní plynovod se jmenovitým průměrem nejméně 700 mm,
  - (b) vysokotlaký vnitrostátní plynovod se jmenovitým průměrem rovným nebo menším než 700 mm,
  - (c) kompresorová stanice,
  - (d) předávací stanice,
  - (e) technický dispečink.
- B2) Distribuční soustava
  - (a) vysokotlaký a středotlaký plynovod,
  - (b) předávací a regulační stanice,
  - (c) technický dispečink.
- B3) Skladování plynu
  - (a) podzemní zásobník plynu se skladovací kapacitou nejméně 50 mil. m3 plynu,
  - (b) technický dispečink.

C) Ropa a ropné produkty
  C1) Přepravní soustava
    (a) tranzitní ropovod se jmenovitým průměrem nejméně 500 mm, včetně vstupních bodů,
    (b) vnitrostátní ropovod se jmenovitým průměrem nejméně 200 mm, včetně vstupních bodů,
    (c) technický dispečink,
    (d) přečerpávací stanice,
    (e) koncové zařízení pro předání ropy,
    (f) začátek a konec zdvojení ropovodu a odbočky - ježkovací komora.
  C2) Distribuční soustava
    (a) produktovod se jmenovitým průměrem nejméně 200 mm včetně vstupních bodů,
    (b) technický dispečink,
    (c) přečerpávací stanice.
  C3) Skladování ropy a pohonných hmot
    (a) zásobník a komplex zásobníků s kapacitou nejméně 40 000 m3,
    (b) technický dispečink.
  C4) Výroba pohonných hmot
    (a) Rafinérie s kapacitou atmosférické destilace nejméně 500 000 t/rok.

D) Centrální zásobování teplem
  D1) Výrobna tepla
    (a) výrobna s celkovým instalovaným výkonem nejméně 200 MW,
    (b) vyvedení tepelného výkonu ze zdroje výroby tepla,
    (c) dispečink výrobce tepla.
  D2) Distribuce tepla
    (a) soustava zásobování tepelnou energií s výkonem nejméně 500 MW,
    (b) technický dispečink provozovatele distribuční soustavy.

II) VODNÍ HOSPODÁŘSTVÍ

(a) zásobování vodou z jednoho nenahraditelného zdroje při počtu zásobovaných obyvatel nejméně 125 000,
(b) úpravna vody o výkonu nejméně 3 000 l/s,
(c) vodní dílo o objemu zachycené vody nejméně 100 mil. m3.

III) POTRAVINÁŘSTVÍ A ZEMĚDĚLSTVÍ

A) Rostlinná výroba – Výměra obhospodařované půdy jednotlivé farmy nebo zemědělského podniku, na území jednoho kraje pro jednotlivou plodinu nejméně 4 000 ha.

B) Živočišná výroba – Počet chovaných kusů zvířat v jednom chovu na území jednoho kraje podle základních druhů hospodářských zvířat
   (a) skot: nejméně 10 000 kusů,
   (b) prasata: nejméně 45 000 kusů,
   (c) drůbež: nejméně 300 000 kusů.

C) Potravinářská výroba – Nenahraditelnost produkce výrobního závodu nebo provozovny na území jednoho kraje podle základních druhů potravin
   (a) mlýnské výrobky: nejméně 80 000 tun za rok podle základních druhů mlýnských výrobků,
   (b) cukr: nejméně 230 000 tun za rok,
   (c) pekařské výrobky: nejméně 600 000 tun za rok podle základních druhů pekařských výrobků,
   (d) mléko a mlékárenské výrobky: nejméně 65 mil. litrů mléka za rok nebo nejméně 100 000 tun mlékárenských výrobků za rok,
   (e) maso a masné výrobky: nejméně 200 000 tun masa za rok podle základních druhů masa nebo nejméně 500 000 tun masných výrobků za rok podle základních druhů masných výrobků.

IV)ZDRAVOTNICTVÍ

A) Poskytování zdravotních služeb – Zdravotnické zařízení, jehož celkový počet akutních lůžek je nejméně 2500.

B) Výroba léčivých přípravků – Výkon činnosti držitele povolení k výrobě léčivých přípravků spočívající ve výrobě léčivých přípravků nebo meziproduktů léčivých přípravků, a to včetně dalších souvisejících výrobních postupů, není-li činností pouze přebalování, balení, změny balení nebo úpravy balení, který na území České republiky
   (a) má nejméně 250 zaměstnanců celkem nebo
   (b) vyrobí nejméně 350 milionů vyrobených kusů pevných lékových forem za rok.

V) DOPRAVA

A) Silniční doprava – Pozemní komunikace, která je zařazena do kategorie dálnice a silnice I. třídy, pokud pro ni neexistuje objízdná trasa.

B) Železniční doprava
   (a) dráha celostátní, včetně jejích strukturálních součástí, pokud pro ni neexistují odklonové trasy s odpovídající traťovou třídou zatížení a prostorovou průchodností pro ložnou míru,
   (b) systém správy a organizace řízení železničního provozu na železniční síti České republiky ve vztahu k evropské železniční síti, s ohledem na nově vzniklé podmínky zajištění součinnosti v rámci Evropského železničního řídicího systému (centrální, regionální a lokální dispečerská pracoviště).

C) Letecká doprava
   C1) Letiště – Veřejné mezinárodní letiště způsobilé přijetí letu podle přístrojů, u kterého není možné leteckou obchodní dopravu zajistit alternativním letištěm nebo alternativní zajištění je příliš nákladné, nehospodárné nebo velmi těžko proveditelné. Alternativním letištěm se rozumí veřejné mezinárodní letiště, které
   (a) je schopno zajistit nejméně 80 % letecké obchodní dopravy letiště, pro které je určeno jako alternativní,
   (b) je v čase 2 hodin dosažitelné jiným druhem dopravy,
   (c) má dostatečnou kapacitu pohybových ploch a kapacitu terminálu,
   (d) má stejnou nebo podobnou kategorii jako letiště, pro které je určeno jako alternativní, a
   (e) je způsobilé přijmout let vykonaný podle přístrojů.
   C2) Řízení letového provozu
   (a) přibližovací služba řízení a letištní služba řízení letiště určeného jako kritická infrastruktura, nebo
   (b) oblastní služba řízení poskytující letové provozní služby včetně řízení letového provozu ve vzdušném prostoru České republiky.

D) Vnitrozemská vodní doprava – Vnitrozemská vodní cesta, jejíž užití nelze nahradit užitím náhradní vnitrozemské vodní cesty ani dopravou jiného druhu.

VI) KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY

A) Technologické prvky pevné sítě elektronických komunikací:
   (a) centrum řízení a podpory sítě,

(b) řídící ústředna,
(c) mezinárodní ústředna,
(d) transitní ústředna,
(e) datové centrum,
(f) telekomunikační vedení.

B) Technologické prvky mobilní sítě elektronických komunikací:
(a) centrum řízení a podpory sítě,
(b) ústředna mobilní sítě,
(c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
(d) základnová stanice sítě pokrývající strategickou lokalitu,
(e) datové centrum.

C) Technologické prvky sítí pro rozhlasové a televizní vysílání:
(a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací s vysílacím výkonem nejméně 1 kW k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele,
(b) řídící pracoviště provozu,
(c) datové centrum,
(d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

D) Technologické prvky pro satelitní komunikaci:
(a) hlavní pozemní satelitní přijímací a vysílací stanice,
(b) Evropský globální navigační družicový systém,
(c) pozemní řídící a komunikační středisko,
(d) pozemní propojovací síť.

E) Technologické prvky pro poštovní služby:
(a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,
(b) sběrný přepravní uzel,
(c) řídící a mezinárodní pošta,
(d) poštovní dopravní infrastruktura.

F) Technologické prvky informačních systémů:
(a) řídicí centrum,
(b) datové centrum,
(c) síť elektronických komunikací,

(d) technologický prvek zajišťující provoz registru doménových jmen „CZ“ a zabezpečení provozu domény nejvyšší úrovně „CZ“.

G) Oblast kybernetické bezpečnosti:
   (a) informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
   (b) komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,
   (c) informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách,
   (d) komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s,
   (e) odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

VII) FINANČNÍ TRH A MĚNA

A) Výkon činnosti České národní banky při zajištění působnosti stanovené zákonem.

B) Poskytování služeb v bankovnictví a pojišťovnictví subjektem, který nabízí komplexní portfolio služeb pro veškeré klienty, disponuje rozsáhlou skupinou dceřiných a přidružených společností zajišťujících další finanční služby a který má rozsáhlou síť regionálních poboček, a to za předpokladu, že
   (a) v bankovním sektoru přesahuje tržní podíl tohoto subjektu 10 % z bilanční sumy bankovního sektoru, nebo
   (b) v pojišťovnictví přesahuje tržní podíl tohoto subjektu měřený objemem předepsaného pojistného 25 %.

VIII) NOUZOVÉ SLUŽBY

A) Integrovaný záchranný systém

(a) operační a informační středisko generálního ředitelství Hasičského záchranného sboru České republiky,
(b) operační a informační středisko hasičského záchranného sboru kraje,
(c) stanice Hasičského záchranného sboru České republiky,
(d) operační středisko útvaru Policie České republiky,
(e) operační středisko zdravotnické záchranné služby,
(f) centrální a oblastní dispečinky horské služby.

B) Radiační monitorování
(a) Radiační monitorovací síť.

C) Předpovědní, varovná a hlásná služba
(a) předpovědní a výstražná služba pro orgány krizového řízení z monitorovacích systémů meteorologických a hydrologických sítí a ze sítí automatického imisního monitorovacího systému,
(b) monitorování meteorologické, hydrologické a imisní situace, mající bezprostřední vliv na vznik a šíření živelních pohrom a nebezpečných látek v ovzduší a informování příslušných orgánů a veřejnosti,
(c) hlásná a předpovědní povodňová služba,
(d) zajištění činnosti celostátní radiační monitorovací sítě,
(e) národní telekomunikační centrum pro zajištění národních monitorovacích a informačních sítí,
(f) regionální telekomunikační centrum v systému Světové meteorologické organizace,
(g) vyhlašování vzniku a ukončení smogových situací a regulačních opatření,
(h) meteorologické zabezpečení jaderných elektráren,
(i) meteorologické zabezpečení civilního letectví,
(j) meteorologické zabezpečení provozu na pozemních komunikacích,
(k) referenční pracoviště pro modelování znečištění ovzduší a zpracovávající zprávy o kvalitě ovzduší podle právních předpisů Evropské unie,
(l) referenční pracoviště zpracovávající zprávy o kvalitě ovzduší a údaje o emisích a imisích podle právních předpisů Evropské unie.

IX) VEŘEJNÁ SPRÁVA

A) Veřejné finance – Výkon činnosti Ministerstva financí, Generálního finančního ředitelství, Generálního ředitelství cel, Úřadu pro zastupování státu ve věcech majetkových a Státní tiskárny cenin, s. p., při zajišťování připravenosti na řešení krizových situací v oblasti
   (a) finanční správy,
   (b) celní správy,
   (c) zastupování státu ve věcech majetkových,
   (d) státního tisku cenin.

B) Sociální ochrana a zaměstnanost

B1) Sociální zabezpečení
   (a) informační systém registru pojištěnců nemocenského a důchodového pojištění, obsahující údaje o více než 125 000 pojištěncích,
   (b) informační systém pojištění registru pojištěnců, jde-li o zaměstnané osoby a osoby samostatně výdělečně činné, obsahující údaje o více než 125 000 osobách,
   (c) informační systém pojištění registru zaměstnavatelů, jde-li o zaměstnavatele zaměstnaných osob, obsahující údaje o více než 125 000 zaměstnavatelích,
   (d) aplikační programové vybavení automatizovaného zpracování údajů potřebných pro rozhodování o dávkách nemocenského a důchodového pojištění,
   (e) aplikační programové vybavení automatizovaného zpracování údajů potřebných pro posuzování zdravotního stavu,
   (f) aplikační programové vybavení automatizovaného zpracování údajů potřebných pro rozhodování o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti včetně záloh, o penále a o přirážce k pojistnému na sociální zabezpečení a o zřízení zástavního práva v případě dluhu na pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a na penále,
   (g) úložiště údajů a evidencí zpracovávaných informačním systémem registru pojištěnců nemocenského a důchodového pojištění, informačním systémem pojištění registru pojištěnců a informačním systémem pojištění registru zaměstnavatelů.

B2) Státní sociální podpora
   (a) informační systém dávek státní sociální podpory (o jejich výši, o poživatelích těchto dávek a žadatelích o tyto dávky a osobách s nimi společně posuzovaných) obsahující údaje o více než 125 000 osobách,

(b) informační systém pomoci v hmotné nouzi, který obsahuje údaje o více než 125 000 osobách,
(c) celorepubliková datová síť spojující generální ředitelství Úřadu práce České republiky, krajské pobočky Úřadu práce České republiky a pobočku pro hlavní město Prahu Úřadu práce České republiky, krajské úřady, obecní úřady obcí s rozšířenou působností a pověřené obecní úřady a další úřady.

B3) Sociální pomoc

(a) informační systém pro zajištění realizace dávek sociálních služeb, který obsahuje údaje o více než 125 000 osobách,
(b) celorepubliková datová síť spojující generální ředitelství Úřadu práce České republiky, krajské pobočky Úřadu práce České republiky a pobočku pro hlavní město Prahu Úřadu práce České republiky, krajské úřady, obecní úřady obcí s rozšířenou působností a další úřady,
(c) evidence dětí a evidence žadatelů pro účely zprostředkování osvojení nebo pěstounské péče, která obsahuje údaje o více než 125 000 osobách.

B4) Zaměstnanost

(a) informační systém politiky zaměstnanosti – evidence volných pracovních míst, evidence zájemců o zaměstnání, evidence uchazečů o zaměstnání, evidence osob se zdravotním postižením, evidence cizinců a evidence povolení k výkonu umělecké, kulturní, sportovní nebo reklamní činnosti dětí, které obsahují údaje o více než 125 000 osobách,
(b) celorepubliková datová síť spojující generální ředitelství Úřadu práce České republiky, krajské pobočky Úřadu práce České republiky a pobočku pro hlavní město Prahu Úřadu práce České republiky, krajské úřady, obecní úřady obcí s rozšířenou působností a pověřených obecních úřadů a další úřady.

C) Ostatní státní správa – Výkon činnosti ministerstev a jiných ústředních správních úřadů při zajišťování připravenosti na řešení krizových situací.

D) Zpravodajské služby

(a) výkon činnosti Úřadu pro zahraniční styky a informace,
(b) výkon činnosti Bezpečnostní informační služby.

Příloha č. 2 - Přehled věcně příslušných ministerstev a jiných ústředních správních úřadů v oblasti kritické infrastruktury

I) ENERGETIKA (MPO/SSHR)
   A) Elektřina (MPO)
   B) Zemní plyn (MPO)
   C) Ropa a ropné produkty (SSHR)
   D) Centrální zásobování teplem (MPO)
II) VODNÍ HOSPODÁŘSTVÍ (MZe)
III) POTRAVINÁŘSTVÍ A ZEMĚDĚLSTVÍ (MZe)
IV) ZDRAVOTNICTVÍ (MZ)
V) DOPRAVA (MD)
VI) KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY (MPO/MV/NÚKIB)
   A) Technologické prvky pevné sítě a el. komunikací (MPO)
   B) Technologické prvky mobilní sítě el. komunikací (MPO)
   C) Technologické prvky sítí pro rozhlasové a televizní vysílání (MPO)
   D) Technologické prvky pro satelitní komunikaci (MPO)
   E) Technologické prvky pro poštovní služby (MPO)
   F) Technologické prvky informačních systémů (MV)
   G) Oblast kybernetické bezpečnosti (NÚKIB)
VII) FINANČNÍ TRH A MĚNA (ČNB)
VIII) NOUZOVÉ SLUŽBY (MV)
   A) Integrovaný záchranný systém (MV)
   B) Radiační monitorování (SÚJB)
   C) Předpovědní, varovná a hlásná služba (MŽP)
IX) VEŘEJNÁ SPRÁVA
   A) Veřejné finance (MF)
   B) Sociální ochrana a zaměstnanost (MPSV)
   C) Ostatní státní správa (ÚSÚ)
   D) Zpravodajské služby (MV)

Příloha č. 3 - Přehledy počtů prvků a subjektů kritické infrastruktury v jednotlivých odvětvích v letech 2011 až 2020

stav ke dni 14.12.2011

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem	Poznámka
			je organizační složka státu [1]	není organizační složka státu [2]		
1.	Energetika	A. Elektřina	0	8	8	přehled "V"
2.	Doprava		0	0	0	
	Počet prvků EKI cekem		0	8	8	

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem	Poznámka
			je OSS [1]	není OSS [2]		
1	Energetika	A. Elektřina	0	202	202	přehled "V"
		B. Zemní plyn	0	0	0	
		C. Ropa a ropné produkty	0	93	93	
		Energetika celkem	0	295	295	
2	Vodní hospodářství	VH celkem	0	11	11	
3	Potravinářství a zemědělství	P a Z celkem	0	0	0	
4	Zdravotnictví	Zdravotnictví celkem	0	0	0	
5	Doprava	A. Silniční doprava	0	2	2	
		B. Železniční doprava	0	8	8	
		C. Letecká doprava	0	3	3	
		Doprava celkem	0	13	13	
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	0	710	710	
		E. Technologické prvky pro poštovní služby	0	155	155	
		F. Technologické prvky informačních systémů	4		4	
		KIS celkem	4	865	869	
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74	
8	Nouzové služby	A. IZS	33	19	52	
		B. Radiační monitorování	1	0	1	
		C. Předpovědní, varovná a hlásná služba	1	0	1	
		Nouzové služby celkem	35	19	54	
9	Veřejná správa	A. Veřejné finance	5	0	5	
		B. Sociální ochrana a zaměstnanost	33	0	33	
		C. Ostatní státní správa	24	0	24	
		D. Zpravodajské služby	2	0	2	
		Veřejná správa celkem	64	0	64	
	Celkem		103	1277	1380	

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (schváleno usnesením vlády ze dne 14. prosince 2011 č. 934)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	152

stav ke dni 4.9.2013

49491. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem	Poznámka
			je organizační složka státu [1]	není organizační složka státu [2]		
1.	Energetika	A. Elektřina	0	8	8	přehled "V"
2.	Doprava		0	0	0	
	Počet prvků EKI cekem		0	8	8	

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem	Poznámka
			je OSS [1]	není OSS [2]		
1	Energetika	A. Elektřina	0	202	202	přehled "V"
		B. Zemní plyn	0	0	0	
		C. Ropa a ropné produkty	0	93	93	
		Energetika celkem	0	295	295	
2	Vodní hospodářství	VH celkem	0	11	11	
3	Potravinářství a zemědělství	P a Z celkem	0	0	0	
4	Zdravotnictví	Zdravotnictví celkem	0	0	0	
5	Doprava	A. Silniční doprava	0	2	2	
		B. Železniční doprava	0	8	8	
		C. Letecká doprava	0	3	3	
		Doprava celkem	0	13	13	
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	0	710	710	
		E. Technologické prvky pro poštovní služby	0	155	155	
		F. Technologické prvky informačních systémů	4		4	
		KIS celkem	4	865	869	
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74	
8	Nouzové služby	A. IZS	33	19	52	
		B. Radiační monitorování	1	0	1	
		C. Předpovědní, varovná a hlásná služba	1	0	1	
		Nouzové služby celkem	35	19	54	
9	Veřejná správa	A. Veřejné finance	5	0	5	
		B. Sociální ochrana a zaměstnanost	18	0	18	
		C. Ostatní státní správa	24	0	24	
		D. Zpravodajské služby	2	0	2	
		Veřejná správa celkem	49	0	49	
	Celkem		88	1277	1365	

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (1. aktualizace schválena UV ze dne 4. září 2013 č. 681)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	139

stav ke dni 8.6.2015

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	202	202
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	93	93
		Energetika celkem	0	295	295
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	8	8
		C. Letecká doprava	0	3	3
		Doprava celkem	0	13	13
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	710	711
		E. Technologické prvky pro poštovní služby	0	155	155
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	45	0	45
		KIS celkem	50	865	915
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74
8	Nouzové služby	A. IZS	274	19	52
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	276	19	295
9	Veřejná správa	A. Veřejné finance	36	0	36
		B. Sociální ochrana a zaměstnanost	18	0	18
		C. Ostatní státní správa	24	0	24
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	80	0	80
	Celkem		406	1277	1683

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (2. aktualizace schválena UV ze dne 25.5.2015 č. 390)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	140

stav ke dni 2. 12. 2015

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	202	202
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	93	93
		D. Centrální zásobování teplem	0	0	0
		Energetika celkem	0	295	295
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	8	8
		C. Letecká doprava	0	3	3
		Doprava celkem	0	13	13
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	710	711
		E. Technologické prvky pro poštovní služby	0	155	155
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	48	28	76
		KIS celkem	53	893	946
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74
8	Nouzové služby	A. IZS	274	19	52
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	276	19	295
9	Veřejná správa	A. Veřejné finance	36	0	36
		B. Sociální ochrana a zaměstnanost	18	0	18
		C. Ostatní státní správa	24	0	24
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	80	0	80
	Celkem		409	1305	1714

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (2. aktualizace schválena UV ze dne 2. 12. 2015 č. 981)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	143

stav ke dni 13.1.2017

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	202	202
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	93	93
		D. Centrální zásobování teplem	0	8	8
		Energetika celkem	0	303	303
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	8	8
		C. Letecká doprava	0	3	3
		Doprava celkem	0	13	13
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	703	704
		E. Technologické prvky pro poštovní služby	0	155	155
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	50	28	78
		KIS celkem	55	886	941
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74
8	Nouzové služby	A. IZS	277	19	296
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	279	19	298
9	Veřejná správa	A. Veřejné finance	35	0	35
		B. Sociální ochrana a zaměstnanost	19	0	19
		C. Ostatní státní správa	25	0	25
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	81	0	81
	Celkem		415	1306	1721

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (4. aktualizace schválena UV ze dne 14. 12. 2016 č. 1139)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	147

stav ke dni 27. 2. 2018

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	202	202
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	93	93
		D. Centrální zásobování teplem	0	8	8
		Energetika celkem	0	303	303
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	8	8
		C. Letecká doprava	0	3	3
		Doprava celkem	0	13	13
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	696	697
		E. Technologické prvky pro poštovní služby	0	156	156
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	52	28	80
		KIS celkem	57	880	937
7	Finanční trh a měna	Fin trh a měna celkem	0	74	74
8	Nouzové služby	A. IZS	277	19	296
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	279	19	298
9	Veřejná správa	A. Veřejné finance	35	0	35
		B. Sociální ochrana a zaměstnanost	19	0	19
		C. Ostatní státní správa	26	0	26
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	82	0	82
	Celkem		418	1300	1718

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (5. aktualizace schválena UV ze dne 27. února 2018 č. 139)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	148

Stav ke dni 7.1.2019

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	212	212
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	92	92
		D. Centrální zásobování teplem	0	0	0
		Energetika celkem	0	304	304
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	9	9
		C. Letecká doprava	0	3	3
		Doprava celkem	0	14	14
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	815	816
		E. Technologické prvky pro poštovní služby	0	153	153
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	52	61	113
		KIS celkem	57	1028	1085
7	Finanční trh a měna	Fin trh a měna celkem	0	79	79
8	Nouzové služby	A. IZS	278	20	298
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	280	20	300
9	Veřejná správa	A. Veřejné finance	35	0	35
		B. Sociální ochrana a zaměstnanost	19	0	19
		C. Ostatní státní správa	26	0	26
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	82	0	82
	Celkem		419	1456	1875

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (6. aktualizace schválena UV ze dne 7. ledna 2019 č. 10)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	152

stav ke dni 13.1.2020

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	212	212
		B. Zemní plyn	0	0	0
		C. Ropa a ropné produkty	0	92	92
		D. Centrální zásobování teplem	0	0	0
		Energetika celkem	0	304	304
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	9	9
		C. Letecká doprava	0	3	3
		Doprava celkem	0	14	14
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	815	816
		E. Technologické prvky pro poštovní služby	0	153	153
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	55	61	116
		KIS celkem	60	1028	1088
7	Finanční trh a měna	Fin trh a měna celkem	0	79	79
8	Nouzové služby	A. IZS	281	20	301
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	283	20	303
9	Veřejná správa	A. Veřejné finance	35	0	35
		B. Sociální ochrana a zaměstnanost	19	0	19
		C. Ostatní státní správa	26	0	26
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	82	0	82
	Celkem		425	1456	1881

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (7. aktualizace projednána na schůzi VCNP dne 10. září 2019, Usn. č. 460)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	153

stav ke dni 21. 12. 2020

1. Přehled počtu prvků evropské kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků EKI, jejichž provozovatelem		Počet prvků EKI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1.	Energetika	A. Elektřina	0	8	8
2.	Doprava		0	0	0
	Počet prvků EKI cekem		0	8	8

2. Přehled počtu prvků kritické infrastruktury

P.č.	Odvětví	Pododvětví	Počty prvků KI, jejichž provozovatelem		Počet prvků KI celkem
			je organizační složka státu [1]	není organizační složka státu [2]	
1	Energetika	A. Elektřina	0	206	206
		B. Zemní plyn	0	25	25
		C. Ropa a ropné produkty	0	92	92
		D. Centrální zásobování teplem	0	0	0
		Energetika celkem	0	323	323
2	Vodní hospodářství	VH celkem	0	11	11
3	Potravinářství a zemědělství	P a Z celkem	0	0	0
4	Zdravotnictví	Zdravotnictví celkem	0	0	0
5	Doprava	A. Silniční doprava	0	2	2
		B. Železniční doprava	0	9	9
		C. Letecká doprava	0	3	3
		Doprava celkem	0	14	14
6	Komunikační a informační systémy	A. - D. Elektronické komunikace	1	831	832
		E. Technologické prvky pro poštovní služby	0	152	152
		F. Technologické prvky informačních systémů	4	0	4
		G. Oblast kybernetické bezpečnosti	58	65	123
		KIS celkem	63	1048	1111
7	Finanční trh a měna	Fin trh a měna celkem	0	79	79
8	Nouzové služby	A. IZS	281	20	301
		B. Radiační monitorování	1	0	1
		C. Předpovědní, varovná a hlásná služba	1	0	1
		Nouzové služby celkem	286	20	306
9	Veřejná správa	A. Veřejné finance	35	0	35
		B. Sociální ochrana a zaměstnanost	19	0	19
		C. Ostatní státní správa	26	0	26
		D. Zpravodajské služby	2	0	2
		Veřejná správa celkem	82	0	82
	Celkem		431	1495	1926

1) Prvky EKI (KI) určené podle § 4 odst. 1 písm. e) krizového zákona (8. aktualizace schválena UV ze dne 21. prosince 2020, Usn. č. 1359)
2) Prvky EKI (KI) určené podle § 9 odst. 3 písm. c) a § 13 odst. 4 písm. c) krizového zákona

3. Přehled počtu subjektů kritické infrastruktury

Celkový počet subjektů kritické infrastruktury	165