

Univerzita Pardubice
Fakulta ekonomicko-správní

Pojetí kritické infrastruktury v mezinárodním srovnání

Zdenka Vernerová

Bakalářská práce

2011

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Zdenka VERNEROVÁ**
Osobní číslo: **E07631**
Studijní program: **B6208 Ekonomika a management**
Studijní obor: **Management podniku - Management malých a středních podniků**
Název tématu: **Pojetí kritické infrastruktury v mezinárodním srovnání**
Zadávající katedra: **Ústav ekonomiky a managementu**

Zásady pro vypracování:

1. Historie pojetí kritické infrastruktury
2. Charakteristika prvků kritické infrastruktury
3. Pojetí kritické infrastruktury ve vybraných zemích
4. Porovnání stavu kritické infrastruktury České republiky a jiných zemí
5. Formulování závěrů, zhodnocení a návrhy

Rozsah grafických prací: -
Rozsah pracovní zprávy: cca 30 stran
Forma zpracování bakalářské práce: tištěná/elektronická

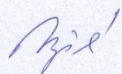
Seznam odborné literatury:

- ŠENOVSKÝ, M., ADAMEC, V., ŠENOVSKÝ, P. Ochrana kritické infrastruktury. Edice SPBI Spektrum, 2007
KARDA, L., KUDLÁK, A. Analýza, metody a nástroje řešení krizových situací. Jihočeská univerzita, České Budějovice, 2007
MOZGA, J., VÍTEK, M., KOVAŘÍK, F. Kritická infrastruktura společnosti. Univerzita Hradec Králové, 2008
ROUDNÝ, R., LINHART, P. Krizový management I. Univerzita Pardubice, 2005
PROCHÁZKOVÁ, D., ŘÍHA, J. Krizové řízení. MV - generální ředitelství HZS ČR, Praha, 2004

Vedoucí bakalářské práce: **Ing. Ondřej Svoboda**
Ústav ekonomiky a managementu

Datum zadání bakalářské práce: **30. června 2010**

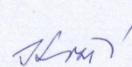
Termín odevzdání bakalářské práce: **30. dubna 2011**



doc. Ing. Renáta Myšková, Ph.D.

děkanka

L.S.



doc. Ing. Marcela Kožená, Ph.D.

vedoucí ústavu

V Pardubicích dne 8. července 2010

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 28.4.2011

Zdenka Vernerová

Poděkování

Tímto bych chtěla poděkovat svému vedoucímu bakalářské práce panu Ing. Ondřeji Svobodovi za pomoc a podnětné návrhy při zpracování této bakalářské práce.

ANOTACE

Práce se zaměřuje na komparaci pojetí kritické infrastruktury v mezinárodním srovnání. Cílem práce je přehledné srovnání pojetí kritické infrastruktury ve vybraných zemích. Práce srovnává pojetí kritické infrastruktury ve vybraných zemích vzhledem k historickým souvislostem a zaměřuje se na deskripci pojetí kritické infrastruktury dle legislativy, prvků a sektorů kritické infrastruktury a jejího financování.

KLÍČOVÁ SLOVA

kritická infrastruktura; ochrana kritické infrastruktury; prvek kritické infrastruktury; krizový stav; mezinárodní srovnání

TITLE

The Concept of Critical Infrastructure in International Comparison

ANNOTATION

The Bachelor's work focuses on a confrontation of the concept of critical infrastructure in International comparison. The aim of this work is general comparison of the concept of critical infrastructure in selected countries. The work comparatives the concept of critical infrastructure in selected countries regarding historical contexts and focuses on a description the concept of critical infrastructure according to legislation, components and segments of critical infrastructure and her funding.

KEYWORDS

critical infrastructure; critical infrastructure protection; component of critical infrastructure; crisis state; international comparison

OBSAH

Úvod.....	12
1 Historie pojetí kritické infrastruktury	14
1.1 Vývoj kritické infrastruktury v České republice	15
1.2 Vývoj kritické infrastruktury v Evropě.....	17
1.3 Vývoj kritické infrastruktury v USA.....	19
2 Charakteristika prvků kritické infrastruktury	21
2.1 Základní pojmy v kritické infrastruktuře	22
2.2 Prvky kritické infrastruktury	25
2.2.1 Energetika.....	25
2.2.2 Voda a vodní hospodářství	27
2.2.3 Potravinářství a zemědělství.....	28
2.2.4 Zdravotní péče	28
2.2.5 Doprava	29
2.2.6 Komunikační a informační systémy	30
2.2.7 Bankovní a finanční sektor	31
2.2.8 Nouzové služby	31
2.2.9 Veřejná správa	32
2.2.10 Průmysl a ochrana průmyslové základny	32
2.2.11 Vesmír a výzkum.....	33
2.2.12 Shromaždiště, budovy, národní památky	33
3 Pojetí kritické infrastruktury ve vybraných zemích.....	33
3.1 Kritická infrastruktura v České republice	34
3.1.1 Odpovědnost za chod kritické infrastruktury a orgány spravující kritickou infrastrukturu	34
3.1.2 Základní funkce státu za krizových situací	37
3.1.3 Možnosti vzniku krizového stavu v České republice	38
3.1.4 Oblasti kritické infrastruktury České republiky	39
3.2 Kritická infrastruktura Evropské unie	40
3.2.1 Odvětví kritické infrastruktury Evropské unie	42
3.3 Kritická infrastruktura v Německu.....	43
3.3.1 Sektory kritické infrastruktury v Německu	44
3.4 Kritická infrastruktura ve Velké Británii	45

3.4.1	Sektory kritické infrastruktury ve Velké Británii	46
3.5	Kritická infrastruktura Slovenska	46
3.5.1	Sektory Kritické infrastruktury Slovenské republiky	47
3.6	Kritická infrastruktura Spojených států amerických	48
3.6.1	Sektory kritické infrastruktury USA	49
4	Porovnání stavu kritické infrastruktury České republiky a jiných zemí	50
4.1	Komparace pojetí kritické infrastruktury	50
4.2	Komparace legislativy a odpovědnosti za chod kritické infrastruktury	52
4.3	Komparace prvků a sektorů kritické infrastruktury	54
4.3.1	Struktura prvků a sektorů (podobnosti a odlišnosti) ve vybraných zemích ...	54
4.3.2	Srovnání prvků kritické infrastruktury v České republice, Evropské unii a Spojených státech amerických	57
4.4	Financování kritické infrastruktury	61
5	Formulování závěrů, zhodnocení a návrhy	63
	Závěr	65

SEZNAM TABULEK

Tabulka 1: Oblasti kritické infrastruktury České republiky.....	39
Tabulka 2: Odvětví kritické infrastruktury EU	42
Tabulka 3: Sektory kritické infrastruktury v Německu.....	44
Tabulka 4: Sektory kritické infrastruktury ve Velké Británii	46
Tabulka 5: Sektory kritické infrastruktury Slovenské republiky	47
Tabulka 6: Sektory kritické infrastruktury USA	49
Tabulka 7: Sektory a prvky kritické infrastruktury dle vybraných zemí	55
Tabulka 8: Srovnání prvků kritické infrastruktury v České republice, Evropské unii a Spojených státech amerických	57

SEZNAM ZKRATEK

BRS	Bezpečnostní rada státu ČR
CIKR	Critical Infrastructure and Key Resources – Národní kritická infrastruktura a klíčové zdroje USA
CIRP	Critical Infrastructure Resilience Programme – Program odolnosti kritické infrastruktury Velké Británie
CIWIN	Critical Infrastructure Warning Information Network – Výstražná informační síť kritické infrastruktury EU
CO	civilní ochrana ČR
CONTEST	Counter terrorism strategy – Protiteroristická strategie Velké Británie
CPNI	Centre for the Protection of National Infrastructure – Koordinační centrum pro bezpečnost národní infrastruktury ve Velké Británii
ČR	Česká republika
D	Německo
DHS	Department of Homeland Security – Ministerstvo národní bezpečnosti USA
ECI	evropská kritická infrastruktura
EPCIP	European Programme for Critical Infrastructure Protection – Evropský program na ochranu kritické infrastruktury
EU	Evropská unie
GŘ HZS	Generální ředitelství Hasičského záchranného sboru
HSPD-7	Homeland Security Presidential Directive – Prezidentská směrnice č. 7 USA
IS PCZ ARGIS	Informační systém plánování civilních zdrojů v ČR
JSVV	Jednotný systém varování a vyrozumění v ČR
KI	kritická infrastruktura
KIS KD	Krizový informační systém v ČR
KRITIS	Umsetzungsplan KRITIS – Plán na ochranu kritické infrastruktury Německa
Krizkom	Informační systém předávání požadavků na věcné zdroje v ČR

NATO	The North Atlantic Treaty Organization – Severoatlantická alliance
NCI	národní kritická infrastruktura
NIPP	National Infrastructure Protection Plan – Národní plan ochrany kritické infrastruktury USA
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen – Národní plán ochrany informační infrastruktury Německa
NSHS	National Strategy for Homeland Security – Národní strategie vnitřní bezpečnosti USA
NSPP	The National Strategy for The Physical Protection of Critical Infrastructure and Key Assets – Národní strategie pro ochranu kritické infrastruktury a klíčových aktiv USA
PCCIP	President’s Commission on Critical Infrastructure Protection – Prezidentská komise pro ochranu kritické infrastruktury USA
RACVIAC	Regional Arms Control Verification and Implementation Assistance Centre – SE Europe (South-East Europe) – Centrum pro koordinaci společných záležitostí v oblasti ochrany státu, které sdružuje země jihovýchodní Evropy
SCADA	Supervisory control and data acquisition – Nadřazené ovládání a sběr dat
SCEPS	Senior Civil Emergency Planning Committee – Hlavní výbor pro civilní nouzové plánování NATO
SR, SK	Slovenská republika
TEN-T	Transevropská dopravní síť
USA	The United States of America – Spojené státy americké
ÚSÚ	Ústřední správní úřad ČR
VB	Velká Británie
VCNP	Výbor pro civilní nouzové plánování ČR

ÚVOD

Tématem bakalářské práce je kritická infrastruktura resp. historické pojetí tohoto pojmu včetně srovnání přístupů ke kritické infrastruktuře ve vybraných zemích.

Kritická infrastruktura je neustále aktuální téma. Společnost je velmi často ohrožována různými vlivy. Tyto vlivy mohou být antropogenní, tedy způsobené člověkem, vlivy přírodní nebo smíšené. Pokud má být zachováno fungování státu a lidské společnosti v době krize, musí existovat systém propracované kritické infrastruktury, která dokáže v případě krizí odolávat a dodávat stabilitu celé společnosti.

Na bezpočtu příkladů nejen v této práci, ale i v novinách, televizi, internetu atd., můžeme sledovat, jak je svět neustále ohrožován nějakou hrozbou. Jak se z této hrozby postupně stává opravdová katastrofa, která stojí desítky, stovky, někdy i tisíce lidí životy.

Dnes a denně můžeme sledovat osudy lidí z různých koutů planety, které jsou postiženy nějakou hroživou událostí. Stanou se obětí zemětřesení, vlny tsunami, výbuchu elektrárny, teroristického útoku atd. Na všechna tato rizika bychom měli umět reagovat, vždy bychom měli umět pomoci lidem, kteří se v takovéto situaci vyskytnou. Ještě lépe bychom se měli snažit těmto situacím předcházet.

Velmi aktuální je v dnešní době hrozba teroristických útoků. Je to pouze jeden z možných případů antropogenních hrozeb, který může vyvolat krizovou situaci. Přesto dnes představuje jednu z nejobávanějších hrozeb. Teroristé se většinou snaží zasáhnout páteří systémů států a jejich infrastrukturu a narušit tak běžný život lidí. Teroristické útoky jsou většinou neočekávané a provázejí je obrovské ztráty na životech. Z tohoto důvodu začala také být podrobněji projednávána kritická infrastruktura některých zemí. Spojené státy americké začaly řešit velmi podrobně kritickou infrastrukturu po útocích na Světové obchodní centrum v New Yorku dne 11. září 2001. Stejně tak kritická infrastruktura některých států v Evropě začala být více řešena až v době po teroristických útocích v Londýně a Madridu.

Jak již bylo řečeno, kromě teroristických útoků jako hrozby současnosti, která se řadí mezi antropogenní katastrofy, mohou být dále katastrofy původu přírodního nebo smíšeného [54]. Antropogenní katastrofy má na svědomí člověk a většinou se jedná o řetězec různých selhání lidského faktoru. Mezi takové může patřit narušení dodávek elektřiny, plynu, tepla. Dále pak také selhání zařízení a lidského faktoru v elektrárnách,

v řízení dopravní infrastruktury atd. Nehody z různých příčin se mohou stát i při přepravě nebezpečného materiálu, ropy, ve výzkumných laboratořích, výzkumu biologických vzorků, chemikálií atd. Různé případy selhání musí být zohledněny v krizových plánech a postupech v nich obsažených. V některých případech se dá havárii předejít, zabránit, nebo alespoň minimalizovat škody.

Katastrofy přírodního typu nejsou nic ojedinělého. Zemi mohou zachvátit povodně, záplavy, vlny tsunami, extrémní sucha, lesní požáry, zemětřesení, výbuchy sopek, vichřice, tornáda atd. Řadu těchto pohrom umíme už pomocí moderní vědy a techniky předpokládat, nikdy se jim však nedá zabránit. Proto musejí být vypracovány krizové plány a postupy, které sníží škody jak na majetku, tak na životech. Obzvlášť propracovaná musí být kritická infrastruktura a její fungování vzhledem k následné záchraně životů, pomoci lidem a likvidaci škod.

Cílem této práce je pomocí metod deskripce, analýzy, syntézy a komparace provést zhodnocení pojetí kritické infrastruktury v mezinárodním pohledu. V práci jsou nejprve popsána pojetí kritické infrastruktury vybraných zemí a následně srovnána mezi sebou. Cílem je ukázat a porovnat kvalitu a rozpracovanost pojetí kritické infrastruktury ve vybraných zemích, nalézt její společné a rozdílné znaky, a tím přinést možnost nového pohledu na kritickou infrastrukturu z více stránek. Přínosem této práce bude získání cenných poznatků z odlišného pojetí kritické infrastruktury vybraných zemí.

V první kapitole je popsán vývoj kritické infrastruktury v České republice, vybraných zemích Evropské Unie a Spojených státech amerických. Popis historie kritické infrastruktury je důležitý vzhledem k tomu, že podává ucelený pohled na to, jak které státy kritickou infrastrukturu řeší, jak dlouho se o řešení kritické infrastruktury snaží, a jaké souvislosti k tomuto řešení vedli.

V druhé kapitole je vysvětleno základní pojmosloví kritické infrastruktury, aby bylo možné se v oblasti kritické infrastruktury lépe orientovat a chápat ji ve všech možných souvislostech. Dále jsou zde charakterizovány jednotlivé prvky kritické infrastruktury, z kterých se skládají sektory kritické infrastruktury a tvoří tak ucelený prvek kritické infrastruktury státu.

Třetí kapitola popisuje a člení kritickou infrastrukturu ve vybraných zemích. Je zde popsána kritická infrastruktura na úrovni Evropské unie v kontextu národních pojetí kritické infrastruktury České republiky, Německa, Velké Británie, Slovenska a Spojených států amerických.

Čtvrtá kapitola se zabývá komparací pojetí v rámci vybraných států. Srovnání se odehrává na úrovni pojetí kritické infrastruktury, legislativy a odpovědností za chod kritické infrastruktury, prvků a sektorů kritické infrastruktury a jejího financování.

Kapitola pátá podává souhrnné zhodnocení všech poznatků, které z práce vyplývají, snaží se o podání návrhů na zlepšení pojetí kritické infrastruktury a o ucelený pohled na kritickou infrastrukturu.

1 HISTORIE POJETÍ KRITICKÉ INFRASTRUKTURY

Požadavek správného fungování infrastruktury společnosti není ničím novým, jak se lze dozvědět z historie. Římské impérium nebo středověké čínské císařství jsou příklady společností, jež znaly důležitost společenské infrastruktury, a proto ji ochraňovaly vojenskou silou nebo náboženstvím. A pakliže společenská infrastruktura přestala plnit své funkce, došlo ke kolapsu. Příkladem budiž kolaps římského impéria, které se rozpadlo především z vnitřních příčin (nefunkční infrastruktura státu) a nájezdy barbarů rozpad jen dovršily [47].

Přístupy k ochraně kritické infrastruktury se dlouhodobě vyvíjejí, a to nejen v zahraničí, ale i u nás. Vývoj v posledních 50 letech zaznamenal různorodost priorit v její ochraně. Zatímco v polovině minulého století byla prioritou hrozba jaderného napadení, o 30 let později začalo převládat ohrožení živelnými pohromami [55].

Problematika kritické infrastruktury jako takové se začala v hojné míře diskutovat především v období 1. a 2. světové války. Problematické konflikty jako války, politická bouření, živelné katastrofy a další neštěstí dávaly a dávají vždy velký podnět k řešení toho, jak zajistit, aby infrastruktura společnosti fungovala správně a tak jak má i v krizových situacích, tím je tedy dán podnět vzniku novodobé kritické infrastruktury jako důležitému pojmu fungování lidské společnosti.

V současné době je řada prvků kritické infrastruktury zaměřena především na časté výskyty a vážné problémy s terorismem a se zvládnutím jeho následků. Stále živá je hrozba teroristických útoků na všech místech světa, je tedy velice důležité ochránit infrastrukturu před těmito útoky, které v případě ničivých následků mohou zapříčinit výpadek infrastruktury velkých rozsahů a nefunkčnost některých jejích prvků na několik hodin nebo i dní.

Nelze opomenout ani možnost poničení infrastruktury z důvodu živelných katastrof, které tu byly v minulosti a budou tu i nadále. Nelze ovlivnit přírodní živly, které mohou způsobit mohutné vichřice, vlny tsunami, zemětřesení, výbuchy sopek atd.

1.1 VÝVOJ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE

V České republice byl jako první orgán, který se zabýval řešením krizových situací na území státu ustanoven 10. června 1998 **Výbor pro civilní nouzové plánování**, který byl zřízen usnesením vlády č. 391, o Bezpečnostní radě státu a o plánování opatření k zajištění bezpečnosti České republiky [60].

Výbor pro civilní nouzové plánování (VCNP) je stálým pracovním orgánem **Bezpečnostní rady státu (BRS)** pro oblast civilního nouzového plánování a pro koordinaci a plánování opatření k zajištění ochrany vnitřní bezpečnosti státu [60].

Řízení VCNP patří do gesce generálního ředitelství Hasičského záchranného sboru (GŘ HZS) Ministerstva vnitra a jeho zaměstnanci zastupují Českou republiku v **Hlavním výboru pro civilní nouzové plánování v rámci NATO (SCEPS – Senior Civil Emergency Planning Committee)** [51].

Na základě usnesení Bezpečnostní rady státu byl v roce 2003 Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru ČR ve spolupráci s dalšími rezorty a ústředními správními úřady stanoven rozsah základních funkcí státu za krizových situací, které jsou nezbytné pro zajištění ochrany životů a zdraví občanů, majetku, životního prostředí a státu samotného [34].

Dalším důležitým dokumentem projednávaným na schůzi VCNP dne 24. září 2002, byla „**Zpráva o národní kritické infrastruktuře**“. Tato zpráva se zabývala samotným vymezením pojmu kritické infrastruktury [51].

VCNP dále na svých schůzích dne 24. června 2003 a 23. března 2004 řešil gesce a rozdělení kritické infrastruktury [51].

Výchozím dokumentem pro rozvíjení ochrany obyvatelstva v našich podmínkách v návaznosti na novou legislativu z roku 2000 je „**Koncepce ochrany obyvatelstva do roku 2006 s výhledem do roku 2015**“, schválená usnesením vlády ČR č. 417 ze dne 22. dubna 2002 a aktualizována usnesením vlády č. 21 ze dne 5. ledna 2005. Ochrana obyvatelstva je v koncepci charakterizována jako soubor činností a postupů, věcně příslušných orgánů, dalších subjektů i jednotlivých občanů, směřujících

k minimalizaci dopadů mimořádných událostí na životy a zdraví obyvatelstva, majetek a životní prostředí [54].

Dalšími **důležitými dokumenty** pro rozvoj kritické infrastruktury v České republice jsou [24]:

- Usnesení BRS č. 204/2001 – obsahuje informace ke zpracování definice a stanovení rozsahu základních funkcí státu za krizových situací,
- Usnesení VCNP č. 152/2002 – definuje rozsah základních funkcí státu za krizových situací,
- Usnesení VCNP č. 153/2002 – Zpráva o národní kritické infrastruktuře a ustanovení VCNP k řešení problematiky zachování základních funkcí státu a kritické infrastruktury,
- Usnesení VCNP č. 179/2003 – seznamy subjektů kritické infrastruktury na národní, regionální a místní úrovni; aktualizace usnesením VCNP č. 190/2004,
- Usnesení VCNP č. 222/2006 – Zpráva o stavu řešení problematiky kritické infrastruktury (obsahuje první srovnání kroků České republiky se zahraničím),
- Usnesení VCNP č. 244/2007 – Zpráva o řešení problematiky kritické infrastruktury,
- Usnesení BRS č. 30/2007 – Zpráva o řešení problematiky kritické infrastruktury v České republice.

Vzhledem ke vstupu České republiky do Evropské unie v roce 2004, souvisí další dokumenty, závazné pro Českou republiku s ustanoveními a nařízeními Evropské unie, která jsou závazná pro všechny členské státy Evropské unie. Nejdůležitějším dokumentem v oblasti kritické infrastruktury v rámci Evropské unie je **Zelená kniha o Evropském programu na ochranu kritické infrastruktury** z roku 2005. Na tento popud bylo vydáno usnesení VCNP č. 236/2005, které informuje o stanovisku České republiky k Zelené knize o Evropském programu pro ochranu kritické infrastruktury [24].

Česká republika také má vlastní zákon, který se dotýká problematiky kritické infrastruktury, je jím **zákon č. 240/2000 Sb., o krizovém řízení** a o změně některých zákonů (krizový zákon) [49].

V České republice je ve střednědobém výhledu vyloučena možnost masivního vojenského útoku. Je zde tedy zdůrazněn posun do oblastí tzv. nevojenského ohrožení. V České republice je možné počítat s rozsáhlými živelnými pohromami, jako jsou povodně, sněhové kalamity, dlouhodobá sucha (s nimi spojený nedostatek pitné

a užitkové vody a vliv na její kvalitu), lesní požáry nebo vichřice. I přes prevence je u nás možnost rizika vzniku průmyslových havárií, nebezpečí úniku chemických látek a odpadů [54].

V kritické infrastruktuře České republiky je také počítáno s možností teroristického útoku. Řešení této problematiky u nás obstarává „**Národní akční plán boje proti terorismu aktualizované znění pro léta 2007 – 2009**“ [40].

1.2 VÝVOJ KRITICKÉ INFRASTRUKTURY V EVROPĚ

Mezi první státy v Evropě, které začaly řešit problematiku kritické infrastruktury podrobněji, patří Velká Británie a Německo. Velká Británie ustanovila v roce 1999 **Koordináční centrum pro bezpečnost národní infrastruktury (CPNI - Centre for the Protection of National Infrastructure)** [8]. V tomtéž roce byl v Německu projednáván materiál **Informačně technické ohrožení klíčových infrastruktur** v Německu, který byl základním materiálem pro další jednání o kritické infrastruktuře v Německu [30].

V podmínkách orgánů Evropské unie (EU) se problematika ochrany kritické infrastruktury (KI) začala řešit o něco později. A to až po narušení dodávek elektrické energie (black-outs) v některých státech Evropy přírodními katastrofami a v neposlední řadě v souvislosti s následky teroristických útoků v Madridě a Londýně [55].

V červnu roku 2004 požádala Evropská rada Evropskou komisi o přípravu celkové strategie na ochranu kritické infrastruktury. Na základě toho byla Evropskou komisí přijata 20. října 2004 sdělení „**Ochrana kritické infrastruktury v boji proti terorismu**“. V tomto dokumentu byly dány jasné návrhy, jak zlepšit prevenci, připravenost a schopnost reakce na teroristické útoky zasahující kritickou infrastrukturu. Na základě závěrů Evropské rady „**Předcházení, připravenost a reakce na teroristické útoky**“ a „**Program solidarity EU o následcích teroristických hrozeb a útoků**“ na jejím zasedání v prosinci 2004 byl podpořen záměr Evropské komise o předložení **Evropského programu na ochranu kritické infrastruktury (EPCIP – European Programme for Critical Infrastructure Protection)** a byl udělen souhlas ke zřízení **Výstražné informační sítě kritické infrastruktury (CIWIN – Critical Infrastructure Warning Information Network)** [29].

Hlavním dokumentem upravujícím **Evropský program na ochranu kritické infrastruktury (EPCIP)** je **Zelená kniha o Evropském programu na ochranu kritické infrastruktury** z roku 2005 [29].

Cílem EPCIP je zajistit, aby v rámci celé EU existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření.

Základními principy EPCIP jsou [29]:

- **Subsidiarita** – ochrana kritické infrastruktury je v odpovědnosti subjektů především na národní úrovni,
- **Doplňkovost** – EPCIP by doplňoval již existující opatření,
- **Důvěrnost** - sdílení informací o ochraně kritické infrastruktury zůstává zachováno v důvěrném prostředí,
- **Spolupráce zainteresovaných subjektů** - svou roli při ochraně kritické infrastruktury hrají členské státy, Evropská komise, sdružení, normalizační orgány, vlastníci i provozovatelé. Tito všichni by měli v rámci kritické infrastruktury spolupracovat,
- **Proporcionalita** – není opodstatněné chránit veškerou infrastrukturu před všemi hrozbami, ochranné strategie a opatření musí být úměrné úrovni daného nebezpečí.

Kritická infrastruktura v rámci Evropské unie je tak rozdělena dle principu subsidiarity na kritickou infrastrukturu na úrovni EU, tzv. **evropskou kritickou infrastrukturu (ECI)** a **národní kritické infrastruktury jednotlivých členských států (NCI)**.

Evropská kritická infrastruktura (ECI) je taková kritická infrastruktura, která v případě narušení bude mít dopad příhraniční, což znamená ve dvou a více členských státech včetně některé kritické infrastruktury bilaterální povahy nebo ve třech a více členských státech kromě veškeré kritické infrastruktury bilaterální povahy [29].

V rámci EPCIP byly vydány ještě další dokumenty, vyjadřující se k této problematice, jako je **Sdělení Komise o Evropském programu na ochranu kritické infrastruktury** [26] a **Návrh Směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu** [28].

Pomocí EPCIP je tedy na úrovni EU dán společný rámec na ochranu kritické infrastruktury, kdy bylo dosaženo dohody o společném seznamu definic a odvětví, kterých se ochrana kritické infrastruktury týká a spolupráci zainteresovaných subjektů.

Národní kritická infrastruktura (NCI) je taková kritická infrastruktura, kterou má každý členský stát a kterou chrání pomocí společného rámce EPCIP a zároveň podle vlastního národního programu na ochranu kritické infrastruktury. Tato národní kritická infrastruktura je v gesci členských zemí EU.

Jako podpůrné opatření pro rámec EPCIP byla zřízena **Výstražná informační síť kritické infrastruktury (CIWIN - Critical Infrastructure Warning Information Network)**. CIWIN má a bude sloužit pro komunikaci a koordinaci v naléhavých situacích. Síť dále usnadňuje výměnu nejlepších postupů v oblasti bezpečnosti a podporuje předávání potřebné výstrahy a informací o bezprostředních hrozbách [29].

1.3 VÝVOJ KRITICKÉ INFRASTRUKTURY V USA

Kritická infrastruktura ve Spojených státech amerických a Austrálii patří k jedné z nejpropracovanějších kritických infrastruktur světa. Stejně tak USA a Austrálie jsou prvními státy, které začaly pracovat na tvorbě kritické infrastruktury a vnímat její důležitost pro fungující společnost.

Již v roce 1996 je vydáno **Vládní nařízení č. 13010 (Executive Order 13010)**, které je vydáno s vědomím prezidenta Clintona a toto nařízení jako první ustanovuje **Prezidentskou komisi pro ochranu kritické infrastruktury (PCCIP – President's Commission on Critical Infrastructure Protection)**. V této době je v USA definováno 8 sektorů kritické infrastruktury.

Základním pilířem a dokumentem, který jako první ustanovil kritickou infrastrukturu a věnoval se této problematice do hloubky je **Směrnice č. 63 (Presidential decision directive 63)**, často nazývaná také jako „**Bílá kniha**“ **kritické infrastruktury (White Paper)**. Tato směrnice byla vydána v květnu roku 1998. V této době USA kromě klasických krizových sektorů začala vnímat jako sektor ohrožený napadeními a útoky také kyberprostor. Rozšiřuje se hrozba počítačového pirátství, hackeři, krádeže dat a zneužití internetu. Proto byly sektory kritické infrastruktury rozšířeny o další sektor, a to sektor informací v kyberprostoru, které je nutné chránit. Touto směrnicí byly také dány gesci jednotlivých úřadů a přiděleny jejich funkce v rámci ochrany kritické infrastruktury. Kritická infrastruktura začala mít tendenci členit se na podsektory. Tato Směrnice byla a je vnímána jako jakási 1. verze „**Národního plánu na ochranu kritické infrastruktury**“.

Velkým zásahem nejenom do americké, ale i do světové bezpečnosti a také obrovským podnětem pro lepší propracování kritické infrastruktury s velkým zaměřením a důrazem na terorismus byl teroristický útok na Světové obchodní centrum v New Yorku dne 11. září 2001. Tento teroristický útok se nedotkl pouze amerických občanů, ale byl zamýšlen jako obrovská demonstrace síly teroristických organizací po celém světě a hluboce se vryl do povědomí celého světa. Na tento popud bylo vydáno za vlády prezidenta Bushe v říjnu roku 2001 další **Vládní nařízení č. 13228 (Executive Order 13228)**, které navazovalo svým obsahem na tyto teroristické útoky a v němž už je kritická infrastruktura v USA členěna na 9 sektorů, které obsahují i ochranu jaderných elektráren, specifických událostí a zemědělství.

V návaznosti na teroristické útoky z 11. září 2001 byl kongresem USA schválen a vydán tzv. **Patriot Act (The USA Patriot and Homeland Security Acts)**, který se silně zaměřil na odstrašení a potrestání všech teroristických činů spáchaných v USA a ve světě a také na zlepšení výkonu práva, vyšetřovacích postupů a zaměřil se na další cíle v oblasti práva a nařízení v souvislosti s terorismem.

V roce 2002 byl vydán „**Zákon o národní bezpečnosti**“ (**Homeland Security Act**), který ustanovil **ministerstvo „národní bezpečnosti“ (DHS - Department of Homeland Security)**. V tomtéž roce byl vydán dokument „**Národní strategie vnitřní bezpečnosti**“ (**NSHS - National Strategy for Homeland Security**). V této strategii je přeformulována definice kritické infrastruktury, která byla původně definována v „**Patriot Actu**“. Tato národní strategie také rozšiřuje dosavadní sektory kritické infrastruktury o další a celkem jich tedy v roce 2002 je již 13. Přidává do sektorů např. ochranu chemických továren a výroby, poštovní a lodní dopravy.

V prosinci roku 2003 je vydána **Prezidentská směrnice č. 7, tzv. HSPD-7 (Homeland Security Presidential Directive)**, která identifikuje kritickou infrastrukturu, utváří priority v oblastech kritické infrastruktury a stanovuje způsob ochrany kritické infrastruktury. V návaznosti na tuto směrnici je vydána „**Národní strategie pro ochranu kritické infrastruktury a klíčových aktiv**“ (**NSPP - The National Strategy for The Physical Protection of Critical Infrastructure and Key Assets**), v jejímž rámci je již pevně zakotveno všech 13 dosavadních sektorů kritické infrastruktury. V tomtéž roce je vydána ještě tzv. „**Národní strategie pro ochranu fyzické infrastruktury**“ (**National Strategy for Physical Infrastructure Protection**), která navazuje na Bushovu NSPP a navíc definuje 3 klíčová aktiva důležitá jako infrastruktura státu, mezi které se řadí národní památky a monumenty národní hrdosti,

budovy a objekty nesoucí národní bohatství a ekonomickou sílu státu, vládní budovy a veřejná shromaždiště. Tyto klíčová aktiva jsou důležité body, které musejí být chráněny před možnými krizovými událostmi nebo potencionálními teroristickými útoky [45].

Později vydaný „**Národní plán ochrany kritické infrastruktury**“ (NIPP - National Infrastructure Protection Plan), který byl vydán roku 2006, člení sektory kritické infrastruktury už na 17 sektorů, a to podle plánů dohodnutých již ve směrnici HSPD-7. Sektory kritické infrastruktury jsou typu národního, státního, lokálního nebo soukromého. Soukromý sektor má v USA velice významné postavení, protože 85 % objektů kritické infrastruktury je vlastněno soukromým sektorem a je tedy nutná spolupráce soukromého sektoru a úřadů. V této době je také vydána speciální **Strategie na ochranu kyberprostoru** (The National Strategy to Secure Cyberspace, NIPP's Cyber Security Plan), který s počítačovým pokrokem získává na své důležitosti.

Národní strategie je aktualizována dokumentem z roku 2007 „**Národní strategie pro národní ochranu**“ (National Strategy for Homeland Security), která se zabývá prevencí před teroristickými útoky a také označuje pojem „**národní kritická infrastruktura a klíčové zdroje**“ (CIKR – Critical Infrastructure and Key Resources).

Národní plán ochrany kritické infrastruktury je aktualizován dokumentem z roku 2009 (**National Infrastructure Protection Plan – NIPP 2009**). Nyní aktuálně je tedy počet sektorů kritické infrastruktury vzhledem k tomuto plánu 18.

Posledním dokumentem týkající se národní bezpečnosti je „**Národní ochranná strategie**“ (National Security Strategy) vydaný v květnu roku 2010 [13].

2 CHARAKTERISTIKA PRVKŮ KRITICKÉ INFRASTRUKTURY

Kritická infrastruktura se skládá z jednotlivých prvků. Tyto prvky budou v této kapitole blíže specifikovány. K tomu, abychom pochopili nejen prvky kritické infrastruktury, ale co to vlastně kritická infrastruktura je, zabývá se první část této kapitoly stručnou terminologií a vysvětlením základních pojmů z oblasti kritické infrastruktury.

2.1 ZÁKLADNÍ POJMY V KRITICKÉ INFRASTRUKTUŘE

Infrastruktura

„Infrastruktura je odvětví zajišťující ekonomické a sociální systémové funkce (např. doprava, energetika, stavby škol a zdravotnických zařízení) [33].“

Kritická infrastruktura

„V každé společnosti existuje část infrastruktury označovaná jako životně důležitá, resp. kritická, která má pro fungování společnosti rozhodující význam [55].“

Definice kritické infrastruktury v jednotlivých zemích světa se může mírně odlišovat, ale základní koncept bývá vždy stejný. Dle Ministerstva vnitra České republiky se *„kritickou infrastrukturou rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva [39].“*

Kritická infrastruktura je vymezována jako [46]: *„nezbytný systém státu, jehož neschopnost plnit své funkce nebo jeho částečné či úplné zničení by mohlo mít nepříznivé dopady na národní bezpečnost, ekonomickou prosperitu, životní prostředí, zdraví a bezpečnost obyvatel. Kritická infrastruktura představuje souhrn vybraných výrobních, nevýrobních, telekomunikačních a dopravních zařízení a objektů, pomocí kterých jsou za krizových stavů naplňovány základní funkce státu.“*

Kritickou infrastrukturu můžeme rozdělit na **národní** a **evropskou**. Národní kritická infrastruktura je samostatná pro každý členský stát. Evropská kritická infrastruktura je taková kritická infrastruktura, jejíž narušení by mělo dopad na více členských států najednou [29].

Z pohledu funkcionality se kritická infrastruktura dělí na **základní** infrastrukturu (energetika, doprava, dodávky vody), **socio-ekonomickou** infrastrukturu (potravinářství, zdravotní péče, záchranné služby, bankovníctví, poštovní služby, veřejná správa) a **socio-kulturní** infrastrukturu, která zajišťuje a udržuje soudržnost společnosti [46].

Někdy se místo pojmu kritická infrastruktura používá pojem **„život podporující síť“**. Tento pojem propaguje zejména Austrálie a Nový Zéland, naopak Finsko používá pojem **„vitální funkce“** a ve Švédsku se vžil pojem **„kritické společenské funkce“** [46].

Ochrana kritické infrastruktury

„Souhrn opatření, která při zohlednění možných rizik směřují k zabránění jejího narušení [39].“

Objekt kritické infrastruktury

„Stavba nebo zařízení zajišťující fungování kritické infrastruktury.“ Vlastníky objektů kritické infrastruktury jsou subjekty kritické infrastruktury [39].

Subjekt kritické infrastruktury

„Vlastník nebo provozovatel objektů kritické infrastruktury [39].“ Subjekty kritické infrastruktury jsou z větší části ve všech kritických infrastrukturách soukromé. Je zde tedy nutnost spolupráce a komunikace s veřejným a státním sektorem.

Krize

„Krise je situace, v níž je významným způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí k danému systému na straně druhé. Krize je vždy spjata s nějakou hrozbou. Krize obecně je tedy stav, kdy dojde k nežádoucí situaci a to překročení nebo naopak podkročení určité meze, kterou považujeme za kritickou [54].“

Krizová situace

„Krizové situace obecně nastávají, když nežádoucí situace svým rozsahem překročí určité stanovené hranice [54].“

Dle zákona č. 240/2000 Sb., o krizovém řízení a zákona č. 110/1998 Sb., o bezpečnosti České republiky *„je krizovou situací mimořádná událost, při níž je vyhlášen stav nebezpečí nebo nouzový stav, stav ohrožení státu nebo válečný stav.“*

- **Stav nebezpečí:** *„Stav nebezpečí se jako bezodkladné opatření může vyhlásit, jsou-li ohroženy životy, zdraví, majetek, životní prostředí, pokud nedosahuje intenzita ohrožení značného rozsahu a není možné odvrátit ohrožení běžnou činností správních úřadů, orgánů krajů a obcí, složek integrovaného záchranného systému nebo subjektů kritické infrastruktury [59].“*
- **Nouzový stav:** *„Vláda může vyhlásit nouzový stav v případě živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo jiného*

nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost [59].“

- **Stav ohrožení státu:** *„Parlament může na návrh vlády vyhlásit stav ohrožení státu, je-li bezprostředně ohrožena svrchovanost státu nebo územní celistvost státu anebo jeho demokratické základy [59].“*
- **Válečný stav:** *„Stav vzniklý mezi nepřátelými stranami (státy nebo jinými subjekty mezinárodního práva) vypuknutím ozbrojeného konfliktu, a to bez ohledu na to zda byla vypovězena válka. Ústava ČR jej definuje jako situaci, kdy je ČR napadena, nebo je-li třeba plnit mezinárodní smluvní závazky o společné obraně proti napadení. Válečný stav vyhláší Parlament České republiky [58].“*

Krizové řízení

„Je to souhrn řídicích činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činnosti prováděných v souvislosti s řešením krizové situace [54].“

Mimořádné události

„Jsou to události, které vyžadují provedení záchranných a likvidačních prací integrovaným záchranným systémem“, jak vymezuje zákon č. 239/2000 Sb., o integrovaném záchranném systému [48].

*„Mimořádné události mohou být členěny na **přírodní, antropogenní** (způsobené lidmi), **smíšené** [54].“*

Hrozba

„Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu [25].“

*„Hrozba je něco, co je na počátku nežádoucího jevu a působí na ohrožená aktiva, tedy ohrožené objekty nebo osoby, subjekty. Hrozby členíme na **úmyslné** a **neúmyslné** [54].“*

Riziko

„Riziko je nebezpečí škod v souvislosti s hrozbou a konečnou ztrátou. Rizikem je pravděpodobnost škody [54].“

„Riziko vyjadřuje míru budoucího ohrožení objektu, respektive aktiva hrozbami, které vedou ke škodám [25].“

2.2 PRVKY KRITICKÉ INFRASTRUKTURY

Prvky kritické infrastruktury se pro různé státy světa mohou lišit. V této kapitole je uveden výčet prvků kritické infrastruktury, které jsou v různých obměnách používány ve vybraných státech světa. Jejich komparace a tedy srovnání států dle prvků kritické infrastruktury je předmětem kapitoly 4.

2.2.1 ENERGETIKA

Prvek infrastruktury energetika v sobě zahrnuje více odvětví. Těmi jsou elektrická energie, plyn, tepelná energie a ropa.

Elektrická energie

Elektrická energie je velice důležitým článkem infrastruktury. Pomocí elektřiny je propojeno fungování více systémů mezi sebou. Elektřina osvětluje většinu měst, zajišťuje chod nemocnic, obchodních center, škol, dodává energii pro přenos informací pomocí komunikačních systémů atd. Elektrická energie je vyráběna v malých či větších elektrárnách. Elektrárny mohou být poháněny různými druhy paliv, ať už je to uhlí, tedy tepelné elektrárny, elektrárny vodní, větrné nebo jaderné. V dnešní době se rozmáhá také výroba elektřiny ze zdrojů solárních nebo biomasy. Elektrárny jsou tedy velmi cenným objektem kritické infrastruktury. Jejich poškození, ať už živelnou pohromou nebo úmyslným zapříčiněním např. teroristickým útokem může být zdrcující, vzhledem k tomu, kolik obyvatel a výrobních zařízení zůstane bez elektrické energie. Zdroje elektrické energie musí být tedy velice dobře chráněny proti narušení, a pokud už toto narušení bude způsobeno, musejí být vyhotoveny havarijní plány pro záložní fungování nebo pro přesun elektrické energie z jiných sítí a záložních zdrojů, které jsou pro tyto případy vytipovány a ustanoveny objektem kritické infrastruktury [32].

Co mohou tzv. black outs, neboli masivní výpadky elektřiny způsobit už bylo několikrát v historii zaznamenáno. Příkladem může být výpadek proudu v Brazílii v roce 2009, kdy na dvě hodiny bylo více než deset milionů lidí bez elektrické energie.

Tento výpadek způsobil problémy i ve vodní elektrárně, přestože se jednalo o pouhé 2 hodiny. Cestující uvízli v metru, byla přerušena sportovní utkání [10].

Plyn

Plyn je využíván nejen v domácnostech. Pomocí plynu vaříme, ohříváme vodu. Některé budovy jsou pomocí plynu i vytápěny. Plyn je tedy velice důležitým prvkem, který je dodnes využíván jak ve velkých městech, tak i v malých obcích. Plyn je ve většině domácností kombinován s elektrickou energií [21].

Vzhledem k tomu, že je plyn těžen jen v některých částech světa, je dodáván plynovým potrubím, která musejí být připravena na případné havárie nebo poškození. A jelikož např. Evropa má velice nízké zásoby zemního plynu, bývá spousta států závislá na dodávkách plynu z okolních regionů, které jsou na plyn bohaté, např. Blízkého Východu nebo Ruska [19].

Velice poučným pro situace výpadků plynu mohou být např. politické spory mezi Ukrajinou a Ruskem v roce 2008. Ruský vývozce plynu Gazprom kvůli nesplacenému dluhu Ukrajiny snížil dodávky plynu o 50 %. Ukrajina si v té době začala brát chybějící dodávky plynu z plynovodu směřujícího k západoevropským odběratelům. Česká republika odebírá zhruba 70 % plynu z Ruska, byla tedy touto situací také dosti ohrožena, jelikož nemá vlastní zásoby plynu. I takto tedy může vypadat krizová situace [20].

Tepelná energie

Tepelná energie a její rozvod souvisí s vytápěním domácností, továren, obchodních center, úřadů a správních budov atd. Tepelnou energií je zajišťován ohřev vody, její rozvod do výměníků tepla a budov. Tepelná energie je vyráběna v tepelných elektrárnách, ať už v elektrárnách na uhlí, plyn, biomasu atd. Bez tepelné energie se dnes většina lidí neobejde, pokud nemá vlastní zdroj energie přímo ve svém domě.

Většina z obyvatel města Pardubic a blízkého okolí má ještě na paměti výpadek tepla roku 2002, kdy rozsáhlá havárie v tepelné elektrárně Opatovice nad Labem způsobila výpadek centrálního vytápění lokálního charakteru. Přestože elektrárna Opatovice nad Labem je pouze malá regionální elektrárna, ocitlo se téměř 55 tisíc lidí v přilehlých městech a obcích bez tepla. Výpadkem byly zasaženy nemocnice, školy, domácnosti, firmy i úřady a v této době nebyl dostatečně dořešen žádný záložní zdroj, který by dodávky tepla zajistil [56].

Ropa

Ropa je v dnešní době velmi ceněnou surovinou, bývá také nazývána černým zlatem. Ropa a její ropné produkty jako benzin a nafta jsou klíčovými produkty používanými v dopravě. Bez dodávek těchto produktů by se doslova zastavila veškerá doprava na planetě. Ropa je také surovinou pro výrobu plastů, některých léků a hnojiv. Není tedy divu, že je ropa tak moc ceněna a její cena neustále roste. Ropa a její produkty se používají téměř všude, jak ve výrobě, tak v dopravě [22].

V poslední době dodávají cenám ropy a strachu o budoucnost těžby ropy nepokoje na Blízkém Východě (např. konflikt v Libyi v letošním roce, který rapidně zvedl ceny paliv v České republice), který má největší zásoby ropy na světě. Vzhledem k tomuto prvenství jsou na místě neustále obavy o budoucnost dodávek ropy do ostatních států světa [9].

2.2.2 VODA A VODNÍ HOSPODÁŘSTVÍ

Prvek kritické infrastruktury voda a vodní hospodářství, v sobě zahrnuje více podsektorů, kterými je voda jako prvek sama o sobě, vodohospodářství a odpadní vody.

Voda

Voda je důležitým prvkem pro lidský život. Vodu každý den pijí miliardy lidí na celé planetě, užitková voda je spotřebována k chovu zvířat, k zavlažování polí. Bez vody by v krajině nastala sucha, bez vody nebudou růst rostliny a zvířata i lidé zahynou. Jak povrchové tak podzemní vody jsou důležitou zásobárnou pro život celého lidstva. Voda je dnes již v mnoha státech používána i k výrobě energií. Je tedy nutné chránit vodní zdroje, přehrady, vodní toky a zásobárny vod. Je nutné kontrolovat kvalitu vody a její znečištění a nepodceňovat možnost bioterrorismu [43].

Systémy odpadních vod

V dnešní době, která je velice vyspělá, ale také produkuje spoustu škodlivin, které mají dopad na ekologii, je nutné, aby byl propracován systém odpadních vod. Nejen k výrobě a i k dalším činnostem jsou používány chemikálie, prostředí je znečišťováno, musíme si tedy dávat pozor, co je vypouštěno s odpadní vodou zpět do

země. Země je důležitá pro další prvek kritické infrastruktury, tedy zemědělství. Po celém světě jsou stavěny čistírny odpadních vod, jímky a systémy potrubí, které mají zamezit znečištění svého okolí [43].

2.2.3 POTRAVINY A ZEMĚDĚLSTVÍ

Prvek kritické infrastruktury potravin a zemědělství v sobě zahrnuje zemědělskou výrobu, potravinářství, péče o potraviny, zásobování, kvalitu potravin atd.

Zemědělská výroba je důležitá pro produkci základních potravin. Je provázána s dalšími prvky kritické infrastruktury jako např. vodní hospodářství, ropa v přísadách pro hnojiva atd. Z půdy a zemědělských zvířat se zpracovávají další suroviny. Těžké dopady na zemědělství a potravinářství mohou mít dlouhotrvající sucha, stejně tak i velké záplavy, krupobití, vichřice atd.

Chráněnou složkou musí být také **zásobování potravinami** a jejich výroba, jejich skladování, péče o potraviny a měření jejich kvality [42].

2.2.4 ZDRAVOTNÍ PÉČE

Prvek kritické infrastruktury zdravotní péče se dělí na podsektory přednemocniční a neodkladné péče, nemocniční péče, ochranu veřejného zdraví, léčiva a séra.

Přednemocniční a neodkladná péče, nemocniční péče

Péče a ošetření lidí, kterým hrozí újma na zdraví nebo ztráta života je velice důležitá. Přednemocniční a neodkladná péče je jednou ze složek integrovaných záchranných systémů států. Výjezdové služby jsou využívány i v době ohrožení živelnými pohromami, teroristickými útoky atd. Je zde nutná sladění všech složek rychlých záchranných služeb, rychlost a profesionalita všech článků. Nemocniční péče je péče následující po bezprostřední záchraně života a je prováděna již v budovách nemocnic, které musejí být také chráněny, dobře zásobovány energiemi, potravinami, vodou a dalšími nezbytnými pomůckami. Je tedy nutná další provázanost s ostatními

prvky kritické infrastruktury a tvorba záložních zdrojů, jelikož na nich poté závisí životy a zdraví pacientů i personálu [41]

Ochrana veřejného zdraví

Zdravotní péče se netýká pouze přímých zásahů při ohrožení zdraví nebo života občanů. Je nutné také sledovat zdraví občanů státu z dlouhodobějšího hlediska. V tomto případě se jedná o varování před nákazami, epidemiemi a infekčními onemocněními velkého rozsahu, které by mohly mít velký dopad na obrovské množství lidí [41].

Léčiva

Dalším prvkem zdravotní péče je i výroba léčiv, jejich následné skladování, jejich distribuce do zdravotnických zařízení. Toto se týká nejenom léčiv ale i dalších zdravotnických pomůcek nutných pro ošetření pacientů v době nastání krizové situace. V této složce může být zahrnuta i humanitární pomoc pro ostatní státy světa. Dále se sem může počítat i ochrana laboratorních zařízení a ústavů pro vývoj léčiv, sér, očkovacích látek a dalších biologických látek [41].

2.2.5 DOPRAVA

Doprava a transport jako prvek kritické infrastruktury se většinou dělí na dopravu silniční, leteckou, železniční, vnitrozemskou vodní, námořní, hromadnou, potrubní a poštovní.

Silniční doprava obsahuje veškeré důležité silniční dopravní uzly, které slouží k přepravě materiálu a osob osobními a nákladními automobily. Tvoří ji silnice, dálnice, místní komunikace atd. Další uzly tvoří doprava **železniční**, díky které jsou přepravovány po tratích nejen osoby, ale také suroviny a materiály, produkty z jiných zemí atd. **Leteckou** dopravou jsou v dnešní době přepravovány především osoby na delší vzdálenosti, armádní zásilky atd. **Vodní** doprava ať již ve vnitrozemí nebo námořní slouží k přepravě osob i dalších zásob surovin a materiálů na velké vzdálenosti. Narušení jakéhokoliv prvku dopravy je velice závažný problém, jelikož nefunkční dopravní infrastruktura zamezuje pohyb osob, kdy se lidé nemohou dostat do svých domovů, do zaměstnání, škol atd. Je tím tedy narušen běžný chod života osob. Nehledě

na to, že narušení dopravních tratí způsobí nedodání materiálů a surovin k výrobě, zastaví se chody továren a výrobních podniků atd.

Mezi druhy dopravy řešené v rámci kritické infrastruktury pouze v některých státech je doprava **hromadná**, tedy páteční systém většiny velkoměst, kdy se jedná o dopravu v metru, autobusy, tramvaje atd. Za kritickou dopravní infrastrukturu lze považovat i dnes rozšířenou dopravu zásilek **poštovní** a zasilatelskou. **Potrubní** doprava je někdy řešena zvlášť, někdy v rámci prvku energetiky [36].

2.2.6 KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY

Komunikace a proudění informací je v dnešní době velmi potřebné. Bez možnosti přenosu informací a komunikace by nastalo naprosté informační a komunikační „ticho“. V tomto prvku jsou zahrnuty **služby pevných i mobilních telefonních sítí**, které jsou velice důležité pro sdělování pokynů a informací mezi občany i orgány krizového řízení. Ve většině států je tedy zřízena i výstražná komunikační síť, která je schopna fungovat jako síť záložní ke komunikaci krizových orgánů v případě narušení komunikačních a informačních systémů. V prvku komunikace je také zahrnuto **radiové vysílání**, které v leckterých dobách, např. světových válek bylo jedním z mála možností jak získat informace o průběhu dění doma i ve světě. Prvkem důležitým např. pro armádní účely je **satelitní komunikace a navigace**. V dnešní moderní době je také na paměti, aby bylo v době krize zachováno alespoň nouzové **televizní vysílání**, které by nemělo být narušeno. A na co nelze zapomenout je důležitý prvek komunikace a sběru informací a dat, **Internet a datová komunikace**. Přes internet je v dnešní době propojena většina světa, fungují přes něj obchody, dorozumívání na velké vzdálenosti, je to studnice informací pro veškeré účely. Z tohoto hlediska, kdy je internet velice citlivou informační databází o spoustě firem nebo osob na zemi, je ve většině zemí vypracován krizový plán v boji proti kyberterorismu, který se velmi rychle rozrůstá a šíří se světem, narušuje informační síť, sbírá citlivá data a zneužívá je pro své účely [7].

2.2.7 BANKOVNÍ A FINANČNÍ SEKTOR

Finanční služby v sobě zahrnují **bankovníctví, pojišťovnictví, investiční společnosti, makléře a dealery, kapitálový trh, burzy i veřejné finance.**

Veškeré tyto prvky jsou důležité pro chod ekonomiky státu a pro jeho ekonomické zdraví. Narušení subjektů bankovních nebo burzovních společností a veřejných financí může způsobit pokles nebo naopak zvýšení cen, úroků, dále také finanční nestabilitu, znehodnocení měny atd. Ekonomika státu by měla fungovat dále i při velkých katastrofách, kdy je přesto možné, že se na nějaký krátký čas zastaví její chod. Toto by přesto nemělo ohrozit fungování celého finančního sektoru a způsobit větší problémy [6].

Příkladem takovéto krize může být např. Krach na Newyorské burze roku 1929, který odstartoval Velkou hospodářskou krizí nebo Celosvětová ekonomická krize roku 2008, která odstartovala americkou hypoteční krizí z roku 2007 a postupně přerostla ve světovou finanční krizi, a u níž byl jedním z hlavních spouštěčů prudký nárůst cen ropy a nárůst spotřebitelských cen [31].

Dokonce i silné ekonomiky států mohou být ochromeny některými kritickými situacemi, např. silné zemětřesení v jihovýchodním Japonsku z 11. března 2011 může podle ekonomů dočasně oslabit očekávané oživení třetí největší ekonomiky světa, která se již vzpamatovávala z útlumu na konci loňského roku. Po zemětřesení s velkými ztrátami na životech byly zastaveny jaderné elektrárny, ropné rafinerie, byla ochromena doprava a přerušeny dodávky elektřiny. Dokonce přední japonské společnosti zastavily svoji výrobu. V Japonsku se nacházejí závody na výrobu automobilů a polovodičů, proto způsobené škody nejspíš budou mít ekonomický dopad [11].

2.2.8 NOUZOVÉ SLUŽBY

Mezi nouzové služby v rámci kritické infrastruktury jsou řazeny většinou všechny složky ochrany a obrany státu. Důležitou složkou nouzových služeb jsou **hasičské záchranné sbory**, které pomáhají nejen při hašení požárů, ale i při vyprošťovacích a záchranných pracích. Je zde nutná provázanost s prvkem **zdravotní péče**, v případě že není přímo zahrnut do nouzových služeb. Další složkou obrany státu je **armáda a policie**, která v krizových situacích zjednává pořádek, udržuje bezpečnost a pomáhá při nouzových pracích. Mezi nouzové služby může být zahrnuto také např.

radiační monitorování, předpovědní, varovná a hlásná služba, která částečně spadá do prvku komunikace [23].

2.2.9 VEŘEJNÁ SPRÁVA

Složka veřejné správy v sobě zahrnuje **funkčnost vlády, úřadů, soudů, věznic, sociálních správ, zaměstnanosti, chod vládních zařízení a budov** atd.

V době krizové situace je nutné zabezpečit základní funkce státu, dodržování zákonů a základních lidských práv a svobod. Je nutné koordinovat záchranné a další práce, které koordinují příslušné státní úřady. Nelze také opomenout to, že v případě krizové situace musí být funkční justiční orgány a musí fungovat zabezpečení věznic, občané musí dostávat své finanční jistoty a chod státu musí fungovat dál i v případě krizové situace [39].

2.2.10 PRŮMYSL A OCHRANA PRŮMYSLOVÉ ZÁKLADNY

Některé státy světa mají mezi svými prvky kritické infrastruktury zahrnutou ochranu průmyslu a průmyslové základny. Mezi hlavní průmyslové odvětví, která byla vybrána pro ochranu, patří především **průmysl jaderný**, skladování jaderného materiálu a jeho přeprava, likvidace nebezpečného jaderného materiálu atd. Dalším odvětvím je **průmysl chemický**, výroba chemikálií, farmaceutik, jejich uskladnění a přeprava nebezpečných látek. Důležitým průmyslovým odvětvím je také průmysl **zbrojní, strojírenský, kovovýroba a hutnictví**, které mají na starost výrobu důležitých prvků a materiálů pro obranu státu. Do této sekce lze zahrnout i **zpracování odpadů**, ať už odpadů běžných, odpadů z výroby nebo odpadů nebezpečných a jejich likvidaci [37].

Jako nedostatečná se např. ukázala ochrana jaderného průmyslu při zemětřesení v Japonsku 11. března 2011, kdy po zemětřesení o síle 8,6 stupňů Richterovy škály selhalo chlazení dvou jaderných reaktorů v jaderné elektrárně Fukušima 1. V této elektrárně se následkem zemětřesení a ničivé vlny tsunami zhroutila střecha a byl poškozen reaktor, z kterého následně musela být upouštěna radioaktivní pára. Nedostatečná také byla evakuace lidí z bezprostřední blízkosti elektrárny. Těžko zde můžu posoudit, čím byla tato chyba způsobena, zda nedostatečným zabezpečením nebo

nepřipraveností na takto silné zemětřesení, které přesto mohlo být v oblasti s takto silnou tektonickou aktivitou předpokládáno [50].

2.2.11 VESMÍR A VÝZKUM

V rámci prvků některých pojetí kritické infrastruktury není opomenuto ani na složku vesmíru, jeho vlivy na planetu zemi, hrozící nebezpečí a ochranu vesmírných zařízení a projektů. Nejedná se však pouze o vesmírná výzkumná zařízení, ale o zařízení výzkumného charakteru ve všech oborech, které jsou důležité pro vynálezy a zlepšení kultury dnešní doby. Lze k tomuto prvku přiřadit i meteorologické služby a výzkumná centra pro hlášení meteorologických změn a předpovědi zemětřesení, sopečných aktivit atd. [18]

2.2.12 SHROMAŽDIŠTĚ, BUDOVY, NÁRODNÍ PAMÁTKY

Jako prvky kritické infrastruktury některých států jsou zařazeny i objekty, kde se shromažďuje velké množství lidí a je zde proto možnost teroristického útoku. Jedná se většinou o obchodní zařízení, centra, sportovní stadiony, veřejná shromaždiště, veřejné budovy a také národní památky a monumenty, které jsou chráněny především před napadením státní hrdosti a jejich zneuctěním [13].

3 POJETÍ KRITICKÉ INFRASTRUKTURY VE VYBRANÝCH ZEMÍCH

Kritická infrastruktura jednotlivých zemí světa je více či méně odlišná. V některých zemích je kritická infrastruktura téměř shodná, v některých naprosto odlišná. Strukturu kritické infrastruktury si určují státy samy, je proto více než jasné, že koncepce jako taková bude ve většině zemí podobná, ale další členění a podrobnosti kritické infrastruktury budou odlišné. Proč tomu tak je? Každý stát světa je specifický svojí velikostí, polohou, obyvatelstvem, zdroji a bohatstvím země. Každý stát se tedy ve svojí kritické infrastruktuře zaměřuje na ty události, jejichž vznik je předpokládán nejčastěji. Jako příklad lze uvést Českou republiku, která se například bude lišit od Spojených států amerických ve své infrastruktuře tím, že nebude mít objekty kritické

infrastruktury zaměřené na zajištění funkčnosti infrastruktury při tornádech, které se oproti tomu v USA vyskytují velmi často.

Tato kapitola se zabývá kritickou infrastrukturou vybraných zemí. Kapitola následující komparuje, tedy srovnává podobné a rozdílné znaky pojetí kritické infrastruktury ve světě.

3.1 KRITICKÁ INFRASTRUKTURA V ČESKÉ REPUBLICE

Kritickou infrastrukturou v České republice podle Ministerstva vnitra ČR se rozumí „výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva [39].“

Česká republika, jakožto člen Evropské unie spadá do Evropského **programu na ochranu kritické infrastruktury**, tzv. EPCIP. Tento program stanovuje tzv. **evropskou kritickou infrastrukturu**, což je „*infrastruktura, která se nachází v členských státech a jejíž narušení nebo zničení by mělo závažný dopad pro nejméně 2 členské státy EU* [39].“

Národní kritická infrastruktura členských států Evropské unie je přesto v gesci členských zemí, což znamená, že kritická infrastruktura České republiky, jejíž narušení by mělo dopad přímo a pouze na Českou republiku je v gesci České republiky [29].

3.1.1 ODPOVĚDNOST ZA CHOD KRITICKÉ INFRASTRUKTURY A ORGÁNY SPRAVUJÍCÍ KRITICKOU INFRASTRUKTURU

Odpovědnost za jednotlivé oblasti kritické infrastruktury mají jednotlivá ministerstva podle jejich pole působnosti a ústřední správní úřady podle jejich kompetencí [34].

Nejvyšším orgánem z hlediska bezpečnosti České republiky je **Bezpečnostní rada státu**, která je stálým pracovním orgánem Vlády České republiky, a to na základě ústavního zákona č 110/1998 Sb., o bezpečnosti České republiky. Dalšími stálými pracovními orgány jsou **Výbor pro koordinaci zahraniční bezpečnostní politiky**,

Výbor pro obranné plánování, Výbor pro civilní nouzové plánování a Výbor pro zpravodajskou činnost.

Stálým pracovním orgánem **Bezpečnostní rady státu** pro oblast civilního nouzového plánování a pro koordinaci a plánování opatření k zajištění ochrany vnitřní bezpečnosti státu je výše zmíněný **Výbor pro civilního nouzové plánování**. Tento výbor byl zřízen usnesením vlády ze dne 10.6.1998 č. 391, o Bezpečnostní radě státu a o plánování opatření k zajištění bezpečnosti České republiky. Výbor má 22 členů (zastoupen ústředními správními úřady – ÚSÚ) a jeho předsedou je ministr vnitra České republiky [60].

Ústřední krizový štáb v případě nastání krize tvoří předseda Vlády České republiky a další členové Vlády dle rozhodnutí.

Velice důležitým ústředním orgánem státní správy v oblastech hospodářských opatření pro krizové stavy a státních hmotných rezerv je **Správa státních hmotných rezerv**. Hmotné rezervy jsou více než z poloviny tvořeny ropou a ropnými produkty, jejichž množství je určeno mezinárodními závazky České republiky. Součástí státních hmotných rezerv jsou mobilizační rezervy a pohotovostní zásoby určené pro 24 typových krizových situací. Pohotovostní zásoby vznikají podle požadavků jednotlivých resortů. Správa vytváří koncepci hospodářských opatření pro krizové stavy a jejich zabezpečení podle příslušných zákonů. Sleduje celkovou výši zásob ropy a ropných produktů v ČR. Doplňuje, ochraňuje, obměňuje a udržuje státní hmotné rezervy, včetně zásob pro humanitární pomoc. Společně s Ministerstvem zahraničních věcí ČR a Ministerstvem vnitra ČR realizuje poskytování humanitární pomoci České republiky do zahraničí. Dalším cílem Správy státních hmotných rezerv je poskytování informací orgánům krizového řízení. Jako **informační systémy** jsou používány systémy **KIS KD (Krizový informační systém)**, kde se evidují státní hmotné rezervy, dále pak **IS PCZ ARGIS (Informační systém plánování civilních zdrojů)**, který zabezpečuje informační podporu plánovacích a rozhodovacích procesů orgánů krizového řízení a dále **informační systém Krizkom**, který předává požadavky na věcné zdroje [57].

Na nižších úrovních jsou ustanoveny **Bezpečnostní rady krajů**, jejichž předsedou je hejtmán kraje, v případě hlavního města Prahy její primátor. Na úrovni obcí je ještě ustanovena **Bezpečnostní rada obce**, jejíž předsedou je starosta obce. Každá obec má pak vlastní **krizový plán na úrovni obce**, případně v rámci celého kraje. Tento krizový plán vypracovává Hasičský záchranný sbor ČR.

Dle výše zmíněného je tedy mírný krizový stav zvládnutelný obcí řešen na úrovni obce, stav krize na úrovni kraje řešen orgány kraje a stav krize celostátního rozsahu řešen na úrovni státu. Jak již bylo zmíněno, je v gesci jednotlivých ministerstev řešení takové kritické infrastruktury, která se jej týká.

Vzhledem k tomu tedy např. **ministerstvo dopravy**, řeší nastání krizové situace v oblasti dopravní infrastruktury, která je v tomto případě určena především společným rámcem Programu na ochranu evropské kritické infrastruktury.

Ministerstvo průmyslu a obchodu má také vlastní typové plány řešení krizí, například **Typový plán narušení dodávek plynu velkého rozsahu**, který byl aktualizován v souvislosti s vyhláškou č. 334/2009 Sb., o stavech nouze v plynárenství. Stejně tak jsou stanoveny **typové plány řešení krizových situací narušení dodávek elektřiny velkého rozsahu a dodávek tepelné energie velkého rozsahu**.

Stejně tak např. **Ministerstvo zahraničních věcí** má vlastní Bezpečnostní strategii. **Ministerstvo zdravotnictví** má vlastní strategii zaměřenou na vývoj současné a budoucí situace kritické infrastruktury v oblasti zdravotnictví. **Ministerstvo zemědělství** zabezpečuje zásobování obyvatelstva pitnou vodou za krizových situací, atd.

Ministerstvo obrany řeší především obranu státu při napadení zvenčí či zevnitř, a jako takové zajišťuje následnou ochranu kritické infrastruktury. V roce 2004 byla schválena **Koncepce operační přípravy státního území České republiky**, která vymezuje činnosti uskutečňované v míru, za stavu ohrožení státu a válečného stavu v oblasti vojenské a nevojenské infrastruktury zaměřené k vytvoření nezbytných podmínek pro splnění úkolů ochrany státu České republiky. Tato Koncepce se poté stala základním podkladem pro **Plán operační přípravy státního území České republiky**, schválený roku 2005, který dále rozpracovává a konkretizuje činnosti v jednotlivých druzích infrastruktury.

Pro jednotlivé druhy nevojenské infrastruktury Ministerstvo obrany stanovilo zásady jejich zabezpečení a v součinnosti s ostatními ministerstvy, Správou státních hmotných rezerv, Českým telekomunikačním úřadem a Českou národní bankou byla zahájena postupná realizace.

V současné době se Česká republika řídí **Koncepcí ochrany obyvatelstva do roku 2006 s výhledem do roku 2015**, což je základní dokument ochrany kritické infrastruktury v České republice. Dokument byl schválen usnesením vlády ze dne 22.4.2002 č. 417 a aktualizován usnesením vlády ze dne 5.1.2005 č. 21. Tento

dokument stanovuje jako ústřední orgán výše zmiňované **Ministerstvo vnitra**, na úrovni krajů s pomocným zastoupením Hasičských záchranných sborů krajů. Dále ustanovuje **zařízení civilní ochrany (CO)**, kterých je dosud 14 u obcí a 102 u právnických a podnikajících fyzických osob. Ustanovuje také **Jednotný systém varování a vyrozumění (JSVV)**. Přímou stanovuje také např. zóny havarijního plánování Jaderné elektrárny Dukovany a Jaderné elektrárny Temelín [49].

Česká republika spolupracuje na úrovni kritické infrastruktury kromě Evropské unie také se Severoatlantickou aliancí (NATO). V rámci této organizace je Česká republika zahrnuta ve **Vyšším výboru pro civilní nouzové plánování NATO**, tzv. SCEPS. Dále spolupracuje například s organizací **RACVIAC (Regional Arms Control Verification and Implementation Assistance Centre – SE Europe)**, což je centrum pro koordinaci společných záležitostí v oblasti ochrany státu, které sdružuje země jihovýchodní Evropy [5].

3.1.2 ZÁKLADNÍ FUNKCE STÁTU ZA KRIZOVÝCH SITUACÍ

Na základě usnesení **Bezpečnostní rady státu** byl v roce 2003 Ministerstvem vnitra stanoven rozsah základních funkcí státu za krizových situací. Pod pojmem rozsah základních funkcí státu při krizových situacích jsou chápány „*všechny funkce státní a soukromé sféry, které zabezpečují komplexní, tzn. i fyzickou základnu, umožňující zachování nezbytného rozsahu základních funkcí státu* [34].“

Základní funkce státu dle Linhart a Roudného [34] je zabezpečit:

- Ochranu života a zdraví obyvatel,
- Obranu ČR, svrchovanost státní moci a územní celistvost,
- Základní životní podmínky a potřeby obyvatelstva,
- Koncentraci a koordinaci výkonu státní správy a územní samosprávy pro řešení krizových situací,
- Zákonnost, bezpečnost a vnitřní pořádek,
- Ekonomické, materiální, energetické a finanční zdroje pro řešení krizové situace,
- Funkčnost orgánů krizového řízení, záchranných sborů, ozbrojených sil, ozbrojených bezpečnostních sborů a havarijních služeb pro krizové situace,

- Dopravní obslužnost,
- Systémy, jejich zničení nebo snížení funkčnosti by mělo závažné dopady na obranyschopnost, ekonomickou a společenskou stabilitu a bezpečnost státu.

3.1.3 MOŽNOSTI VZNIKU KRIZOVÉHO STAVU V ČESKÉ REPUBLICE

Podle **Krizového zákona č 240/2000 Sb.**, je ve střednědobém výhledu vyloučena možnost masivního vojenského útoku proti našemu území. Proto je zdůrazněn posun kritické infrastruktury spíše do oblasti tzv. nevojenského ohrožení.

Tímto nevojenským ohrožením jsou míněny rozsáhlé živelné pohromy, kterými mohou být povodně, sněhové kalamity, dlouhotrvající sucha, lesní požáry nebo vichřice. Většinu z těchto krizových stavů Česká republika již řešila a některé více než jednou. V poslední době se na území naší republiky vyskytují časté povodně, někdy i nepředpokládané sněhové kalamity a i ničící vichřice.

Dále i přes prevenci je na našem území možnost vzniku průmyslových havárií, kdy hrozí únik nebezpečných chemických látek, odpadů nebo možnost nehody při přepravě osob a materiálu.

Neposlední a hlavně celosvětovou hrozbou je riziko teroristického útoku, který může nastat kdykoliv, kdekoliv a je naprosto neočekávaný. Možnost teroristického útoku je v České republice řešena dokumentem **Akční plán boje proti terorismu**, který se zabývá jak prevencí, tak odstraňováním následků teroristického útoku. Zaměřuje se především na teroristické útoky za použití chemických, biologických a radiologických látek a jaderného materiálu. Řeší problematiku pozemní přepravy nebezpečných látek, bezpečnosti civilního letectví a boj proti kybernetickým teroristickým hrozbám.

Co se týká úrovně připravenosti prvků systému ochrany obyvatelstva, tak mohou říct, že Česká republika se může srovnávat s dalšími vyspělými zeměmi světa, v některých oblastech může dokonce i jít příkladem. Některé další aspekty v kritické infrastruktuře, např. investování, organizace a komunikace orgánů ale vyžadují další úsilí [49].

3.1.4 OBLASTI KRITICKÉ INFRASTRUKTURY ČESKÉ REPUBLIKY

Zpráva Výboru pro civilní nouzové plánování, schválená Bezpečnostní radou státu usnesením č. 30 z července 2007, stanoví těchto **9 oblastí kritické infrastruktury České republiky**:

Tabulka 1: Oblasti kritické infrastruktury České republiky

Oblasti kritické infrastruktury České republiky	
1. Energetika	Elektrína
	Plyn
	Tepelná energie
	Ropa
2. Vodní hospodářství	Zásobování pitnou a užitkovou vodou
	Zabezpečení a správa povrchových vod a podzemních zdrojů vody
	System odpadních vod
3. Potravinářství a zemědělství	Produkce potravin
	Péče o potraviny
	Zemědělská výroba
4. Zdravotní péče	Přednemocniční neodkladná péče
	Nemocniční péče
	Ochrana veřejného zdraví
	Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5. Doprava	Silniční
	Železniční
	Letecká
	Vnitrozemská vodní
6. Komunikační a informační systémy	Pevné a mobilní telefonní sítě
	Radiová a satelitní komunikace a navigace
	Televizní a rádiové vysílání

	Poštovní a kurýrní služby
	Internet a datové služby
7. Bankovní a finanční sektor	Správa veřejných financí
	Bankovníctví
	Pojišťovnictví
	Kapitálový trh
8. Nouzové služby	Hasičský záchranný sbor ČR a jednotky požární ochrany
	Policie ČR
	Armáda ČR
	Radiační monitorování
	Předpovědní, varovná a hlásná služba
9. Veřejná správa	Státní správa a samospráva
	Sociální ochrana a zaměstnanost
	Justice a vězeňství

Zdroj: přepracováno dle Usnesení BRS č. 30, Praha, 2007 [1]

Platný seznam objektů pro obranu státu (z roku 1998) neodpovídá plně potřebám. Jeho aktualizaci řeší **Plán operační přípravy státního území**. Tyto dokumenty jsou utajovány.

Na území České republiky bylo z hlediska kritické infrastruktury stanoveno **110 nejdůležitějších objektů** celostátního významu [34].

Většina subjektů kritické infrastruktury v České republice je vlastněna a provozována soukromými subjekty. Orgány krizového řízení státu tedy musí koordinovat spolupráci mezi státním a soukromým sektorem v oblasti kritické infrastruktury.

3.2 KRITICKÁ INFRASTRUKTURA EVROPSKÉ UNIE

Vzhledem k tomu, že Evropská unie je sjednocením států Evropy a snaží se tedy co nejlépe uchopit a pojmout myšlenku jednotné Evropy jako celku, musím se zde zmínit i o snaze sjednotit kritickou infrastrukturu států Evropské unie. Evropská unie

čítá k 9. březnu 2011 přesně 27 členských států, mezi které od roku 2004 patří i Česká republika [17].

Hybným motorem pro sjednocení kritických infrastruktur států Evropské unie bylo především narušení dodávek elektrické energie (black-outs) v některých státech Evropy přírodními katastrofami a v neposlední řadě v souvislosti s následky teroristických útoků v Madridě a Londýně [55].

Na tento popud přednesla v prosinci 2004 Evropská komise projekt s názvem „**Evropský program na ochranu kritické infrastruktury**“ (EPCIP), který je kompletně rozepsán v tzv. „**Zelené knize o evropském programu na ochranu kritické infrastruktury**“ z roku 2005 [29]. Spolu s programem EPCIP byla zřízena i „**Výstražná informační síť kritické infrastruktury**“ (CIWIN).

Kritická infrastruktura na úrovni Evropské unie je dle Zelené knihy o EPCIP definována jako „*takové kritické infrastruktury, jejichž narušení způsobí vážné důsledky i za hranicemi členského státu, ve kterém se infrastruktura nachází.*“ Evropská kritická infrastruktura obsahuje materiální zdroje, služby, zařízení informačních technologií, sítě a majetek, které budou mít v případě narušení nebo zničení vážný dopad na zdraví, bezpečnost, zabezpečení, hospodářství nebo sociální blahobyt ve dvou, třech a více členských státech [29].

Nejenom z výše uvedené definice tedy vyplývá, že na úrovni EU je kritická infrastruktura dvojího charakteru. Každý členský stát má svoji vlastní Národní kritickou infrastrukturu a chrání ji pomocí společného rámce EU i vlastních zdrojů. Každý stát má tedy svůj vlastní **Národní program na ochranu kritické infrastruktury**. Zároveň však existuje **Evropská kritická infrastruktura (ECI)**, která je společná pro členské státy EU a její narušení má dopad na více členských států najednou. Z tohoto důvodu je nutná dobrá komunikace, koordinace a spolupráce na národní, evropské i mezinárodní úrovni mezi všemi zainteresovanými subjekty. Je tedy nutné dosáhnout dohody o společném seznamu definic a odvětví, kterých se ochrana kritické infrastruktury týká.

Evropský program na ochranu kritické infrastruktury také obsahuje 3 typy aktiv kritické infrastruktury [29]:

- 1) Veřejné, soukromé a státní složky infrastruktury a vzájemně závislé kybernetické a fyzické sítě,
- 2) Postupy vynakládající úsilí na kontrolu funkcí kritické infrastruktury,
- 3) Objekty mající kulturní nebo politické označení jako „mírný cíl“ hromadných událostí (sport, volný čas, kultura).

Cílem Evropského programu na ochranu kritické infrastruktury je zajistit, aby v rámci celé EU existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření.

Základními principy Evropského programu na ochranu kritické infrastruktury, jak již bylo řečeno a vysvětleno v 1. kapitole, jsou subsidiarita, doplňkovost, důvěrnost, spolupráce zainteresovaných subjektů a proporcionalita [29].

3.2.1 ODVĚTVÍ KRITICKÉ INFRASTRUKTURY EVROPSKÉ UNIE

Směrnice Evropské rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu, stanoví 11 oblastí kritické infrastruktury Evropské unie, které jsou uvedeny v tabulce č. 2:

Tabulka 2: Odvětví kritické infrastruktury EU

Odvětví kritické infrastruktury EU	
1. Energetika	Produkce ropy a plynu, rafinace, zacházení a uskladnění včetně distribuce potrubím
	Výroba elektrické energie a její rozvod
2. Jaderný průmysl	Produkce, skladování a zpracování jaderných látek
3. Informační a komunikační technologie (ICT)	Ochrana informačních systémů a sítí
	Automatizace přístrojů a kontrolních systémů (SCADA atd.)
	Internet
	Poskytování pevných telekomunikačních sítí
	Poskytování mobilních telekomunikačních sítí
	Radiová komunikace a navigace
	Satelitní komunikace
	Vysílání
4. Voda	Zásobování pitnou vodou

	Kontrola kvality vody
	Těsnění a kontrola množství vody
5. Potraviny	Zásobování potravinami a zajištění bezpečnosti potravin
6. Ochrana zdraví	Lékařská a nemocniční péče
	Léky, sera, očkovací látky a léčiva
	Biologické laboratoře a biologičtí činitelé
7. Finanční	Infrastruktury a systémy zúčtování a vypořádání obchodů s cennými papíry
	Regulované trhy
8. Doprava	Silniční
	Železniční
	Letecká
	Vnitrozemská vodní
	Zámořská a příbřežní námořní
9. Chemický průmysl	Produkce, skladování a zpracování chemických látek
	Potrubí pro přepravu nebezpečných chemických látek
10. Vesmír	Vesmír
11. Výzkumná zařízení	Výzkumná zařízení

Zdroj: přepracováno dle Směrnice Evropské rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu [28]

3.3 KRITICKÁ INFRASTRUKTURA V NĚMECKU

Kritická infrastruktura v Německu patří k jedné z nejvyspělejších kritických infrastruktur Evropy a má pokročilý systém ochrany národní kritické infrastruktury [55].

Kritická infrastruktura v Německu je definována jako „organizace a zařízení s velkým významem pro pospolitost státu, u nichž výpadek nebo poškození trvale

způsobí problémy v zásobování, podstatné narušení veřejného bezpečí nebo nastanou jiné dramatické následky [2].“

Řídícím orgánem na poli kritické infrastruktury v Německu je **Ministerstvo vnitra**, které odpovídá za ochranu kritické infrastruktury a její dodržování ostatními úřady a ministerstvy, která mají sektory kritické infrastruktury přiděleny podle svého zaměření. Těmito úřady jsou např. Spolkový úřad ochrany informační techniky, Spolkový úřad ochrany obyvatelstva a pomoci při katastrofách, Spolkový orgán technické pomocné činnosti, Spolkový úřad pro kriminální činy, Ministerstvo zemědělství, Ministerstvo pro místní rozvoj, Ministerstvo spravedlnosti nebo Ministerstvo obrany.

Spolková republika Německo má od roku 2005 ustanoven a Spolkovým kabinetem schválen „**Národní plán ochrany informační infrastruktury**“ (NPSI – Nationaler Plan zum Schutz der Informationsinfrastrukturen), který má stanoveny 3 strategické cíle: prevenci, reakci a nepřetržitost. S tímto „**Národním plánem**“ úzce souvisí tzv. **plán „KRITIS“** (Umsetzungsplan KRITIS), který byl ustanoven roku 2007 a definuje kritickou infrastrukturu a také její sektory [2].

3.3.1 SEKTORY KRITICKÉ INFRASTRUKTURY V NĚMECKU

V následující tabulce č. 3 jsou přehledně uvedeny sektory kritické infrastruktury v Německu.

Tabulka 3: Sektory kritické infrastruktury v Německu

Sektory kritické infrastruktury v Německu	
1. Transport a doprava	Letecká
	Námořní
	Železniční
	Místní, lokální
	Vnitrozemská vodní
	Pouliční
	Poštovní
2. Energie	Elektrická
	Jaderná
	Plyn
3. Nebezpečné látky	Ropa
	Chemické a biologické látky

	Přeprava nebezpečných nákladů
	Zbrojní průmysl
4. Informační technika a telekomunikace	Telekomunikace
	Informační technika
5. Finance, peněžnictví a pojišťovnictví	Banky
	Pojišťovny
	Finanční služby
	Burzy
6. Zásobování	Zdravotnictví
	Nouzové a záchranné služby
	Civilní obrana
	Zásobování potravinami
	Zásobování vodou
	Zpracování odpadu
7. úřady, správa a soudnictví	Vláda
	Úřady
	Správa
	Úřady a organizace bezpečnostních složek, armada
8. ostatní	Další důležité objekty pro společnost

Zdroj: přepracováno dle Umsetzungsplan KRITIS [3]

3.4 KRITICKÁ INFRASTRUKTURA VE VELKÉ BRITÁNII

Velká Británie spolu s již výše zmíněnou Spolkovou republikou Německo patří ke státům, které mezi prvními začaly řešit problematiku kritické infrastruktury.

Velká Británie má ustanoveno 9 sektorů kritické infrastruktury, o kterých informuje „**Centrum ochrany národní infrastruktury**“ (CPNI – Centre for the Protection of National Infrastructure) Toto Centrum poskytuje komplexní bezpečnostní informace, které tvoří národní kritickou infrastrukturu [8].

Národní ochranná strategie ve Velké Británii se zaměřuje především na dvě prioritní rizika, a to terorismus a narušení kyberprostoru. Pro tyto dva typy narušení kritické infrastruktury má Velká Británie vlastní postupy uvedené v dokumentech „**Protiteroristická strategie**“ (CONTEST – Counter terrorism strategy) a „**Strategie na ochranu kybernetiky**“ (Cyber Security Strategy) z roku 2009 [8].

Kritickou infrastrukturou a jejími sektory se zabývá „**Program odolnosti kritické infrastruktury**“ (CIRP – Critical Infrastructure Resilience Programme) [8].

Centrum ochrany národní infrastruktury spolupracuje se všemi složkami, které mají na starosti jednotlivá odvětví kritické infrastruktury. Odvětví jsou přidělena podle zaměření jednotlivým odborům či ministerstvům [8].

3.4.1 SEKTORY KRITICKÉ INFRASTRUKTURY VE VELKÉ BRITÁNII

V následující tabulce č. 4 jsou přehledně uvedeny sektory kritické infrastruktury ve Velké Británii.

Tabulka 4: Sektory kritické infrastruktury ve Velké Británii

Sektory kritické infrastruktury ve Velké Británii	
1. Pohotovostní služby	Policie
	Hasiči
	Ambulance
	Pobřežní policie
2. Vláda	Vláda
3. Komunikace	Telekomunikace
	Pošta
	Vysílání
4. Zdravotnictví	Zdravotnické služby
5. Voda	Voda
6. Energie	Ropa
	Plyn
	Elektřina
7. Finanční služby	Finančnictví
8. Potraviny	Potraviny
9. Doprava	Silniční
	Železniční
	Vodní
	Letecká

Zdroj: přepracováno dle Sector Resilience Plan for Critical Infrastructure 2010 [4]

3.5 KRITICKÁ INFRASTRUKTURA SLOVENSKA

Kritická infrastruktura Slovenské republiky je definována jako „*tá časť infrastruktúry (vybrané organizácie a inštitúcie, objekty, systavy, zariadenia, služby a systémy), ktorej zničenie alebo znefunkčnenie spôsobí ohrozenie alebo narušenie*

politického a hospodárskeho chodu štátu, alebo ohrozenie života a zdravia obyvateľstva [44].“

Gesce za jednotlivé sektory kritické infrastruktury spadají pod příslušná ministerstva. Hlavním orgánem je **Ministerstvo vnitra**. V roce 2006 byla navržena „**Koncepce kritické infrastruktury Slovenské republiky a způsob její ochrany a obrany**“. Tato Koncepce byla následně v roce 2007 zrealizována v podobě „**Národního programu pro ochranu a obranu kritické infrastruktury Slovenské republiky**“ [44].“

Dne 8. února 2011 byl vydán **Zákon č. 45/2011 o kritické infrastruktuře**, který byl schválen prezidentem Ivanem Gašparovičem a vstoupil v platnost dne 1. března 2011. Tento zákon ustanovuje strukturu a působnost státní správy, prvky kritické infrastruktury a vymezuje úkoly podnikatelů a fyzických osob podílejících se na chodu a ochraně kritické infrastruktury [35].

3.5.1 SEKTORY KRITICKÉ INFRASTRUKTURY SLOVENSKÉ REPUBLIKY

V následující tabulce č. 5 jsou přehledně uvedeny sektory kritické infrastruktury Slovenské republiky.

Tabulka 5: Sektory kritické infrastruktury Slovenské republiky

Sektory kritické infrastruktury Slovenské republiky	
1. Doprava	Silniční
	Letecká
	Vodní
	Železniční
2. Elektronická komunikace	Satelitní komunikace
	Sítě a služby pevných a mobilních elektronických komunikací
3. Energetika	Hornictví, hutnictví
	Elektroenergetika
	Plynárenství
	Ropa a ropné produkty
4. Informační a komunikační technologie	Informační systémy a sítě
	Internet
5. Pošta	Poskytování poštovních služeb, poštovní platební styk a správa pošt
6. Průmysl	Farmaceutický

	Hutnický
	Chemický
7. Voda a atmosféra	Meteorologická služba
	Vodní stavby
	Zabezpečení pitné vody
8. Zdravotnictví	zdravotnictví

Zdroj: přepracováno dle Zákona č. 45/2011 o kritické infrastruktuře [35]

3.6 KRITICKÁ INFRASTRUKTURA SPOJENÝCH STÁTŮ AMERICKÝCH

Kritická infrastruktura ve Spojených státech amerických je upevněna a nabývá nový rozměr po událostech 11. září 2001, kdy teroristé citelně zasáhli nejen Spojené státy americké, ale i celý svět, když provedli útoky na Světové obchodní centrum v New Yorku a další vytipované objekty. V této době začala vláda USA bouřlivě jednat o zdokonalení kritické infrastruktury státu s velkým důrazem na protiteroristické programy.

Kritická infrastruktura USA je definována jako „systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci [16].“

Kritickou infrastrukturu a systém její ochrany definuje nejnovější dokument z roku 2010 „**Kritická infrastruktura a klíčové zdroje**“, který byl vydán Ministerstvem národní bezpečnosti (Department of Homeland Security) [12]. Součástí tohoto dokumentu je tzv. „**Plán na ochranu národní infrastruktury**“ (NIPP) z roku 2009 [14].

Kritická infrastruktura v USA se skládá z 85 % z vlastnictví soukromého sektoru. Propracovaný systém komunikace dává skvělou možnost spolupráce mezi soukromým sektorem a vládními úřady, které mají správu kritické infrastruktury na starosti. Hlavním úřadem v oblasti kritické infrastruktury je již výše zmiňované Ministerstvo národní bezpečnosti. Pod jeho řízením je kritická infrastruktura spravována dalšími ministerstvy, úřady nebo agenturami, jež se zabývají specifickým sektorem kritické infrastruktury podle zaměření své činnosti [14].

3.6.1 SEKTORY KRITICKÉ INFRASTRUKTURY USA

V USA jsou rozlišovány dva pojmy týkající se kritické infrastruktury. Je to **kritická infrastruktura** a **klíčové prvky neboli aktiva či zdroje**. Klíčová aktiva jsou ojedinělé prvky zvláštního významu. Jsou to samostatná zařízení, jejichž vyřazení sice neohrozí národní ekonomiku, ale může být zdrcující z hlediska vzniklých škod, ztrát na životech nebo podkopání veřejného sebevědomí. Zvláštní významy jsou dány historickou spojitostí s nějakou událostí nebo místa, na kterých se shromažďuje velké množství lidí a kde je možný předpoklad teroristického útoku [53].

Dle **Department of Homeland Security** a „Plánu na ochranu národní infrastruktury“ se kritická infrastruktura a klíčové zdroje člení na **18 sektorů**, které jsou členěny v tabulce č. 6.

Tabulka 6: Sektory kritické infrastruktury USA

Sektory kritické infrastruktury USA	
1. Zemědělství, potraviny	
2. Bankovníctví, finance	Banky, spořitelny
	Pojišťovny
	Makléři, dealéři
	Investiční společnosti
3. Chemie	Základní chemikálie
	Speciální chemikálie
	Zemědělské chemikálie
	Farmaceutika
	Spotřební produkty
4. Obchodní zařízení	Veřejná místa, sportovní shromaždiště, herny, ubytování, venkovní události, zábava a media, nemovitosti a obchody
5. Komunikace	Telekomunikace, satelity, bezdrátové a drátové sítě
6. Kritická výroba	Primární kovovýroba
	Strojírenství
	Elektrovýroba
	Dopravní vybavení
7. Přehradní nádrže	
8. Ochrana průmyslové základny	Armádní výroba zbraní, výzkum a vývoj
9. Záchrané služby - pohotovost	Krizový management, zdravotníci, hasiči, nebezpečný materiál, výkon práva, pryrotechnici, taktické policejní týmy, pátrací týmy
10. Energie	Elektřina
	Ropa

	Zemní plyn
11. Vládní zařízení	Federální budovy, úřady, ambasády, soudy,...
12. Zdravotní péče a veřejné zdraví	
13. Informační technologie	Hardware, software, IT systémy, Internet
14. Národní památky a ikony	Trvalé objekty a geografická místa, národní dědictví, připomínka významu národa
15. Jaderné reaktory, materiály a odpad	
16. Pošta a přeprava zásilek	
17. Doprava	Letecká
	Silniční
	Námořní
	Hromadná veřejná
	Potrubní
	Železniční
18. Voda	

Zdroj: zpracováno dle Department of Homeland Security a National Infrastructure Protection Plan [14]

4 POROVNÁNÍ STAVU KRITICKÉ INFRASTRUKTURY ČESKÉ REPUBLIKY A JINÝCH ZEMÍ

V této kapitole bude provedena komparace kritické infrastruktury České republiky a jiných zemí. Kritická infrastruktura je všeobecný pojem, který ovšem není všude pojímán stejně, stejně tak jako má každý stát rozdílné a jinak prioritně určené prvky své kritické infrastruktury. Kritická infrastruktura se také liší podle úrovně legislativy, podle gescí a odpovědností za její chod, jejího financování, uvažovaných rizik a hrozeb v dané zemi. Tato kapitola má poukázat na to, že přestože téměř každý stát světa má nějakou úroveň kritické infrastruktury, existují mezi státy světa podobné i rozdílné prvky a náhledy na kritickou infrastrukturu a její stav.

4.1 KOMPARACE POJETÍ KRITICKÉ INFRASTRUKTURY

Kritická infrastruktura se pro potřeby praxe definuje různě, a v definici kritické infrastruktury se odrážejí zkušenosti a zvyklosti států: záplavy (Holandsko), problém národní obrany (Francie, Švédsko, Nový Zéland), problém hi-tech kriminality (Itálie – legislativa, poštovní a komunikační technologie), problém ohrožení rozvoje informační

společnosti (Finsko), problém ohrožení podnikatelských aktivit (Švýcarsko, Anglie), problém boje proti terorismu (Nový Zéland, USA) [46].

Definice kritické infrastruktury v **České republice** podle Ministerstva vnitra ČR zní [38]: „*Kritickou infrastrukturou jsou výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.*“

Podle **Evropské unie** je kritická infrastruktura definována takto [29]: „*Kritické infrastruktury se skládají z fyzických a informačně technologických zařízení, sítí, aktiv a služeb, jejichž porucha nebo zničení má závažné dopady na zdraví bezpečnost, ochranu a materiální blaho občanů nebo má dopady na funkčnost veřejné správy.*“

Když porovnáme tyto dvě pojetí, mohou se na první pohled zdát téměř totožné, což svým významem opravdu jsou. Základní rozdíl je však v tom, že Česká republika jako samostatný stát dbá na ochranu své vlastní národní kritické infrastruktury. Evropská unie oproti tomu jako seskupení států Evropy dbá na ochranu evropské kritické infrastruktury, což znamená, že bude zasahovat a aktivovat své obranné mechanismy a systémy až v případě, že bude ohrožena kritická infrastruktura dvou a více členských států. Tímto nelze říci, že by Evropská unie a její členské státy nepomohli při velkých problémech jiného členského státu. Pomoc je zde téměř samozřejmostí, ale tato kritická situace nebude brána jako narušení evropské kritické infrastruktury.

Jako další stát Evropské unie definuje svou kritickou infrastrukturu **Německo**, a to takto [2]: „*Kritickou infrastrukturou jsou organizace a zařízení s velkým významem pro pospolitost státu, u nichž výpadek nebo poškození trvale způsobí problémy v zásobování, podstatné narušení veřejného bezpečí nebo nastanou jiné dramatické následky.*“

Ve **Velké Británii** je kritická infrastruktura definována Vládou [8]: „*jako zařízení, systémy, místa a sítě nezbytné pro chod státu a pro dodávky základních potřeb, na kterých závisí každodenní život ve Velké Británii.*“

Kritická infrastruktura **Slovenska** je definována Ministerstvem vnitra SR [44] jako: „*tá časť infrastruktúry (vybrané organizácie a inštitúcie, objekty, sústavy, zariadenia, služby a systémy), ktorej zničenie alebo znefunkčnenie spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu, alebo ohrozenie života a zdravia obyvateľstva.*“

Spojené státy americké definují svoji kritickou infrastrukturu (dle „Patriot Act“) [16] jako: „*systemy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci.*“

Z těchto definic lze usuzovat na jednu jedinou věc. Přestože se státy světa liší svojí rozlohou, počtem obyvatelstva, národnostním složením obyvatelstva, svým bohatstvím, atd., v pojetí kritické infrastruktury se překvapivě shodují. Ať už se liší v některých drobných slovech či souslovích, jako zařízení, služby, systémy, sítě, aktiva, atd., shodují se na tom, že kritickou infrastrukturou vlastně jsou důležité prvky, které zabezpečují základní chod společnosti v krizových situacích, a které je potřeba chránit a v případě jejich selhání zabezpečit nouzový chod, který zajistí zajištění všech nutných základních potřeb. Z tohoto pohledu je velmi pěkně nahrazen pojem kritická infrastruktura Austrálií nebo Novým Zélandem, kteří ji nazývají „**život podporující síť**“ (lifeline support network). Tento název je dle mého velmi výstižný, jelikož většina z prvků kritické infrastruktury je v dnešní moderní společnosti tvořena „sítěmi“.

4.2 KOMPARACE LEGISLATIVY A ODPOVĚDNOSTI ZA CHOD KRITICKÉ INFRASTRUKTURY

Ve své knize *Bezpečnost a krizové řízení* z roku 2006 uvádí autorka Dana Procházková, že: „*V České republice doposud není k dispozici právní dokument, který by upravoval nouzové plánování a vymezoval vztah mezi ním a krizovým řízením.*“ Dále také uvádí, že: „*Výrazně chybí zákon na ochranu kritické infrastruktury* [52].“

Tato situace v **České republice** přetrvává nadále, kritická infrastruktura jako taková není řešena přímo zákonem o ní. Hlavním právním dokumentem v této oblasti zatím zůstává **zákon č. 240/2000 Sb., o krizovém řízení** a o změně některých zákonů (krizový zákon). Problematika kritické infrastruktury je ve většině případů upravována vyhláškami nebo usneseními [49].

Oproti tomu, sousední **Slovenská republika** vydala a schválila v roce 2011 **zákon č. 45/2011, o kritické infrastruktuře**. Tento nepřiliš obsáhlý zákon vymezuje kritickou infrastrukturu, její organizaci a působnost, povinnosti zodpovědných osob, postupy bezpečnostního plánu a prvky kritické infrastruktury [44].

To, že kritická infrastruktura není přímo ukotvena v zákoně, ale je zmíněna v různých souvisejících právních předpisech, které se týkají přímo oblastí kritické infrastruktury, jako je plynárenství, energetika, nebo záchranné systémy, není nijak neobvyklé. Takto je to upravováno ve většině zemí s tím, že kritická infrastruktura je ukotvena pomocí národních plánů na její vytyčení a ochranu. Např. v **Německu** je tímto plánem **plán „Kritis“**, ve **Velké Británii** je to **„Program odolnosti kritické infrastruktury“** (Sector Resilience Plan for Critical Infrastructure), atd.. Stejně tak ve **Spojených státech amerických** je několik dokumentů a směrnic upravujících kritickou infrastrukturu, např. dokument **„Kritická infrastruktura a klíčové zdroje“** (Critical Infrastructure and Key Resources) nebo **„Plán na ochranu národní infrastruktury“** (National infrastructure protection plan).

Ani **Evropská unie** nemá přímo zákon, který by tuto oblast spravoval. V Evropské unii je za zásadní považován dokument **„Zelená kniha o evropském programu na ochranu kritické infrastruktury“**. Tento dokument však podává spíše návod a východiska k řešení evropské kritické infrastruktury, ale není žádným striktně daným zákonem. V tomto ohledu jsou v rámci Evropské unie velké nedostatky.

Jak je tedy vidět z výše uvedeného srovnání, není vždy nutné mít kritickou infrastrukturu jasně ukotvenou v zákoně. Většina států vystačí s dokumenty, které se kritickou infrastrukturou zabývají a řeší ji. Přesto by ukotvení v zákoně nebylo na škodu, jelikož zákon je nutné dodržovat. Tím by se mohlo vyřešit spousta konfliktů mezi veřejnými orgány a soukromými vlastníky kritické infrastruktury, kteří se přou o to, kdo má za chod a správu kritické infrastruktury odpovědnost, kdo má jaké pravomoci a povinnosti, a v neposlední řadě, jak bude chod kritické infrastruktury a její správa financována.

Z hlediska odpovědnosti a řízení kritické infrastruktury je organizace téměř všude stejná. Hlavní odpovědnost za kritickou infrastrukturu většinou nese některé z ministerstev, ve většině případů Ministerstvo vnitra a bezpečnosti státu. Odpovědnost za sektory kritické infrastruktury pak připadají na jednotlivá ministerstva dle jejich zaměření. V případě nouze jsou zřizovány bezpečnostní rady. Ve většině států je navíc zřízen orgán, který řeší přímo kritickou infrastrukturu a možnosti nastání krizové situace. V České republice je to např. Bezpečnostní rada státu, v Německu je to Spolkový úřad ochrany obyvatelstva pomoci při katastrofách, atd.

Vzhledem k tomu, že kritická infrastruktura je ve většině států vlastněna převážně soukromým sektorem, musí být spolupráce mezi veřejnou správou

a soukromým sektorem provázaná a organizovaná. Soukromý sektor totiž opravdu vlastní většinu kritické infrastruktury, což je např. ve Spojených státech amerických až 85 % kritické infrastruktury a v Německu téměř 90 %.

4.3 KOMPARACE PRVKŮ A SEKTORŮ KRITICKÉ INFRASTRUKTURY

Jak již bylo několikrát zmíněno, sektory a prvky kritické infrastruktury nejsou ve všech zemích totožné. Většina prvků se shoduje, některé však v kritické infrastruktuře daného státu chybí nebo jsou přidány navíc. To je způsobeno většinou tím, že každý stát má vlastní priority ochrany určitých zařízení a systémů a také tím, že každý stát uvažuje dle jiných rizik a hrozeb, které jsou dané zemi nejbližší. V praxi to pak vypadá tak, že např. Česká republika dává větší význam oblasti kritické infrastruktury, která je zaměřena na riziko vzniku povodní, sucha nebo vichřice. Oproti tomu např. Německo se hodně zaměřuje na ochranu informačních technologií, Spojené státy americké zase na boj proti terorismu, atd..

4.3.1 STRUKTURA PRVKŮ A SEKTORŮ (PODOBNOSTI A ODLIŠNOSTI) VE VYBRANÝCH ZEMÍCH

Zde bude názorně poukázáno na to, jaké podobnosti a odlišnosti jsou mezi jednotlivými prvky kritické infrastruktury ve vybraných zemích.

Jak vyplynulo z provedené analýzy, velmi podobné jsou si především sektory:

- Energetika (ropa, plyn, elektřina),
- Vodní hospodářství (voda, kanalizace),
- Potravinářství a zemědělství,
- Zdravotní péče,
- Doprava, logistika,
- Komunikace a informační systémy,
- Finanční sektor,
- Veřejná správa a nouzové služby.

Tyto sektory jsou v různých obměnách a variacích zastoupeny téměř ve všech kritických infrastrukturách.

Sektory, které jsou zastoupeny pouze v některých kritických infrastrukturách a jsou odlišné, jsou především:

- Různé druhy průmyslu (jaderný, chemický, zbrojní, hutnický, strojírenský,...),
- Vesmír,
- Výzkum,
- Atmosféra, ovzduší,
- Kulturní památky a objekty veřejné správy jako objekty zvláštního významu.

Pro srovnání prvků jsem si vybrala země a společenství, které byly již prezentovány v této práci. Jsou to Česká republika, Německo, Velká Británie, Slovensko, Spojené státy americké a Evropská unie.

V přehledné tabulce č. 7 chci poukázat na podobnosti a odlišnosti sektorů a prvků kritické infrastruktury v těchto státech.

Tabulka uvádí sektory a prvky kritické infrastruktury podle jednotlivých států a společenství: ČR – Česká republika, EU – Evropská unie, D – Německo, VB – Velká Británie, SK – Slovensko, USA – Spojené státy americké

Tabulka 7: Sektory a prvky kritické infrastruktury dle vybraných zemí

Sektor	prvek	státy
Energetika	Elektřina	ČR, EU, D, VB, SK, USA
	Plyn	ČR, EU, D, VB, SK, USA
	Teplo	ČR, EU
	ropa	ČR, EU, D, VB, SK, USA
Voda	Zásobování vodou	ČR, EU, VB, SK, USA
	Povrchové a podzemní vody	ČR, EU
	Odpadní vody	ČR
	Vodní stavby	SK, USA
Potravinařství a zemědělství	Potraviny	ČR, EU, VB, USA
	zemědělství	ČR, USA
Zdravotní péče	Přednemocniční a nemocniční péče	ČR, EU, D, VB, SK, USA
	Veřejné zdraví	ČR, USA
	farmaceutika	ČR, EU, SK, USA
Doprava	Silniční	ČR, EU, D, VB, SK, USA

	Letecká	ČR, EU, D, VB, SK, USA
	Železniční	ČR, EU, D, VB, SK, USA
	Lodní	ČR, EU, D, VB, SK, USA
	Místní, veřejná	D, USA
	Potrubní	USA
Komunikace a informační systémy	Telefonní sítě	ČR, EU, D, VB, SK, USA
	Navigace, satelity	ČR, EU, SK, USA
	Rádio a televize	ČR, EU, VB
	Pošta	ČR, D, VB, SK, USA
	Internet	ČR, EU, USA
	Informační technika	D, SK, USA
Finanční sektor	Veřejné finance	ČR, EU, D, VB
	Kapitálový trh	ČR, EU
	Banky, pojišťovny	ČR, D, USA
	Investiční společnosti, makléři	USA
Nouzové služby	Hasiči, policie, armáda	ČR, D, VB, USA
	Monitorování radiace	ČR
	Varovná služba	ČR
Veřejná správa	Státní správa	ČR, D, VB
	Sociální ochrana	ČR
	Justice, vězeňství	ČR, USA
	Úřady	D
Jaderný průmysl	Jaderné látky	EU
	Jaderná energie	D, USA
Výzkum	Biologické laboratoře	EU
	Výzkumná zařízení	EU, USA
Chemický průmysl	Výroba a skladování chemických látek	EU, D, SK, USA
	Přeprava nebezpečných látek	EU, D, USA
Vesmír		EU
Zbrojní průmysl		D, USA
Zásobování	Zásobování potravinami	D
	Zásobování vodou	D
	Zpracování odpadu	D
Hutnictví		SK
Atmosféra	meteorologie	SK
Veřejná zařízení	Shromaždiště, zábavní služby	USA
Kritická výroba	Strojírenství, dopravní vybavení	USA
Vládní zařízení	Budovy úřadů, soudů	USA
Národní památky a ikony		USA

Zdroj: vlastní analýza dle Usnesení BRS č. 30 (Praha, 2007), Směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu,

4.3.2 SROVNÁNÍ PRVKŮ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE, EVROPSKÉ UNII A SPOJENÝCH STÁTECH AMERICKÝCH

Pro další názornou komparaci, která má přinést další pohled na kritickou infrastrukturu a její prvky, je vybráno srovnání České republiky, Evropské unie, která v rámci evropské kritické infrastruktury zaštiťuje českou národní kritickou infrastrukturu a Spojených států amerických, jak uvádím v tabulce č. 8. Toto srovnání je velice zajímavé z toho důvodu, že Česká republika je státem Evropské unie, a přesto některé prvky kritické infrastruktury nejsou totožné. Spojené státy americké jsou do této komparace zahrnuty úmyslně z toho důvodu, že je to zámořský stát na jiném kontinentu s odlišnou kulturou, a tedy srovnání Evropy a Ameriky může být přínosné a poukázat na rozdíly v propracovanosti a detailech kritické infrastruktury.

Tabulka 8: Srovnání prvků kritické infrastruktury v České republice, Evropské unii a Spojených státech amerických

	Česká republika	Evropská unie	Spojené státy americké
Energetika	ANO	ANO	ANO
Vodní hospodářství	ANO	ANO	ANO
Potravinářství a zemědělství	ANO	ANO	ANO
Zdravotní péče	ANO	ANO	ANO
Doprava	ANO	ANO	ANO
Komunikační a informační systémy	ANO	ANO	ANO
Bankovní a finanční sektor	ANO	ANO	ANO
Nouzové služby	ANO	NE	ANO
Veřejná správa	ANO	ANO	ANO
Jaderný průmysl	NE	ANO	ANO
Chemický průmysl	NE	ANO	ANO
Vesmír a výzkum	NE	ANO	NE
Ochrana práv a pořádku	NE	ANO	NE
Ochrana průmyslu	NE	NE	ANO
Národní památky	NE	NE	ANO

Přehradní nádrže	NE	NE	ANO
Poštovní a kurýrní služby	NE	NE	ANO
Veřejná zařízení	NE	NE	ANO
Krizové řízení výroby	NE	NE	ANO

Zdroj: vlastní analýza dle Usnesení BRS č. 30, Praha, 2007 a Zelené knihy o Evropském programu na ochranu kritické infrastruktury, Brusel, 2005 a National Infrastructure Protection Plan, Washington, 2009

Z následující tabulky je patrné, že Česká republika ve srovnání s Evropskou unií má některé sektory kritické infrastruktury společné a v některých prvcích se liší. Oproti České republice i Evropské unii mají Spojené státy americké propracovanou kritickou infrastrukturu zahrnující i odlišné sektory kritické infrastruktury. V některých sektorech se shodují či podobají.

Podobnými oblastmi kritické infrastruktury České republiky, Evropské unie a Spojených států amerických jsou oblasti:

- **Energetika:** V pojetí České republiky je energetika členěna do oblastí elektřina, plyn, teplo a ropa. Evropská unie nezahrnuje v této oblasti problematiku tepla. Stejně tak USA nezahrnují v energetice problematiku tepla.
- **Voda, vodní hospodářství:** Z pohledu ČR obsahuje vodní hospodářství zásobování pitnou a užitkovou vodou, zabezpečení a správu povrchových a podzemních vod a systém vod odpadních. EU pojímá problematiku vody podobně, tedy zajištění pitné vody, kontrolu kvality vody a kontrolu množství vody. USA se zaměřuje především na kontrolu kvality vody vzhledem k možnostem ohrožení bioterorismem. USA zvláště má vyhrazen sektor kritické infrastruktury přehradní nádrže.
- **Potravinářství a zemědělství:** ČR se v tomto sektoru zabývá produkcí potravin, péčí o potraviny a zemědělskou výrobou. EU má tento sektor zaměřen pouze na potravinářství, produkci potravin, bezpečnost a ochranu potravin. USA se zaměřuje na ochranu jak potravinářství, tak i zemědělství.
- **Zdravotní péče:** ČR pojímá zdravotní péči z hlediska péče přednemocniční, nemocniční, ochrany veřejného zdraví, léčiv a zdravotnických prostředků.

EU pojímá tuto oblast totožně, navíc v ní ale zahrnuje ještě sféru laboratorní oblasti. Stejně jako v ČR a EU je pojímána i v USA.

- **Doprava:** Je téměř totožná. ČR, EU i USA zahrnují do oblasti dopravu silniční, železniční, leteckou a vnitrostátní vodní. Vzhledem k neexistenci jiných než vnitrostátních vod v ČR není u nás řešena doprava oceánská a námořní, v EU a USA řešena je. USA navíc v rámci dopravy řeší i oblast hromadné veřejné dopravy a dopravy potrubní.
- **Komunikační a informační systémy:** V ČR zahrnují pevné a mobilní telefonní sítě, radiovou a satelitní komunikaci a navigaci, televizní a radiové vysílání, poštovní a kurýrní služby, internet a datové služby. EU v této sféře řeší také internet, pevné a mobilní telefonní sítě, radiovou komunikaci a navigaci, navíc ještě ochranu sítě, automatizovaný kontrolní systém, satelitní komunikaci a rozhlas. EU má poštovní a kurýrní služby řešeny ve sféře veřejné správy. USA mají tuto oblast rozdělenou. Zvlášť mají Komunikaci, která obsahuje také např. satelity, bezdrátové a drátové sítě. Zvlášť jsou pak řešeny informační systémy, které řeší internet, IT systémy, hardware a software. Poštovní a kurýrní služby jsou také zvláštní oblastí kritické infrastruktury.
- **Bankovní a finanční sektor:** V ČR zahrnuje správu veřejných financí, bankovníctví, pojišťovnictví a kapitálový trh. Z hlediska EU se jedná o platební služby soukromé a státní. V tomto sektoru se naší kritické infrastruktury podobá spíše USA, které zde také řeší banky, pojišťovny, spořitelny, úvěrové společnosti, burzy cenných papírů nebo investiční společnosti.
- **Veřejná správa:** V ČR se týká státní správ a samosprávy, sociální ochrany a zaměstnanosti, justice a vězeňství. Pro EU je definována jako vládní funkce, armáda, veřejné služby, nouzové služby, poštovní a kurýrní služby. Sjednocuje v sobě tedy to co např. ČR má odděleně jako nouzové služby a komunikační služby a stejně tak USA má nouzové služby a dokonce i poštovní a kurýrní služby jako zvláštní sektor. V USA sektor veřejné správy zahrnuje hlavně správu budov jako takových, ambasád, laboratoří, soudů a zařízení důležitých pro veřejnou správu.

Další **sektory** kritické infrastruktury jsou již **odlišné**:

- **Nouzové služby:** EU je nemá zahrnutý jako zvláštní sektor, obsahuje je sektor veřejné správy. V ČR tyto služby zahrnují Hasičské záchranné sbory, jednotky požární ochrany, Policii, Armádu, radiační monitorování, předpovědní a varovnou službu. V USA je tento sektor totožný, zahrnuje krizový management, zdravotníky, hasiče, přepravu nebezpečného materiálu, pyrotechniky, policii, pátrací jednotky a navíc zahrnuje i výkon práva.
- **Jaderný průmysl:** Pro ČR není řešen. EU ho má řešen v rámci jedné oblasti spolu s chemickým průmyslem. Týká se produkce nukleárních látek. USA tuto oblast má řešenu jako jaderné reaktory, materiály a odpad pro účely energetické, výzkumné a zdravotnické.
- **Chemický průmysl:** Pro ČR není řešen. EU ho má řešen v rámci jedné oblasti spolu s jaderným průmyslem. Týká se produkce chemických látek a jejich rozvodů. USA člení pak tento segment do dalších podle druhu produktu na základní chemikálie, speciální chemikálie, zemědělské chemikálie, farmaceutika a spotřební produkty.
- **Vesmír a výzkum:** V ČR není řešen. EU tuto problematiku zahrnuje. USA tuto oblast také neupravuje.
- **Ochrana práv a pořádku:** Je řešena pouze v EU, kde zahrnuje právo a pořádek a služby justice. V USA není řešena a v ČR je zahrnuta spíše v rámci veřejné správy, ale ne jako samostatná oblast.
- **Ochrana průmyslu:** Tato oblast je specifická pouze pro USA a týká se především ochrany armádní průmyslové základny, výroby zbraní, výzkumu a vývoje.
- **Národní památky:** Tato oblast je specifická pouze pro USA. Zahrnuje památky, které poukazují na národní hrdost, tradice, dědictví národa a jsou symboly státu.
- **Přehradní nádrže:** Specifická oblast kritické infrastruktury pro USA. Tato oblast zahrnuje plavební komory, povodňové a větrné bariéry, zásobárny vody. Je zvlášť vyčleněna mimo oblast vody.
- **Poštovní a kurýrní služby:** Oblast kritické infrastruktury USA. ČR nemá tuto oblast samostatně, ale zahrnuje ji oblast komunikace. V EU je oblast zahrnuta ve veřejné správě.

- **Veřejná zařízení:** USA vymezuje tuto oblast kritické infrastruktury jako ochranu veřejných míst, sportovišť, heren, ubytovacích zařízení, venkovních akcí, médií, nemovitostí a obchodů. ČR ani EU tuto oblast neupravují.
- **Krizové řízení výroby:** V USA zahrnuje tato kritická výroba kovovýrobu, výrobu strojů, elektrických přístrojů a dopravních strojů. ČR ani EU tuto oblast neupravují.

Z tohoto porovnání tedy vyplývá, že některé sféry kritické infrastruktury jsou pro ČR, EU a USA podobné. Další oblasti kritické infrastruktury se prolínají a někdy jsou zařazeny do jiných oblastí nebo nejsou vyčleněny samostatně. USA má kritickou infrastrukturu členěnou velice podrobně a má ji detailněji propracovanou, i vzhledem k možnosti teroristického útoku.

4.4 FINANCOVÁNÍ KRITICKÉ INFRASTRUKTURY

Ve většině případů vyvstává otázka, z jakých zdrojů je kritická infrastruktura financována. Udržování veškerých objektů kritické infrastruktury v chodu i v době, kdy není potřebná, stojí nemalé finanční obnosy. Vzhledem k tomu, že velká část kritické infrastruktury je v soukromém vlastnictví, měla by být řešena otázka financování těchto soukromých subjektů. Provozovatel kritické infrastruktury se na provozu zařízení samozřejmě podílí, ale vzhledem k tomu, že kritická infrastruktura je ustanovena státem, měl by většinu těchto objektů a jejich funkčnost financovat státní rozpočet.

Financování kritické infrastruktury by mohlo být provedeno podobně jako financování krizových opatření, které uvádí **§ 25 zákona č. 240/2000 Sb., o krizovém řízení**. Tento zákon uvádí, že [49]: „*finanční zabezpečení krizových opatření na běžný rozpočtový rok se provádí podle zvláštního předpisu*“. Tímto zvláštním předpisem jsou zákony č. 218/2000 Sb., o rozpočtových pravidlech a zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů. Za tímto účelem ministerstva a další správní úřady ve svých rozpočtech na příslušný rok vyčleňují objem finančních prostředků potřebný k zajištění přípravy na krizové situace. Ministerstvo financí pak se souhlasem Ministerstva vnitra navrhuje účelovou rezervu finančních prostředků na řešení krizových situací a odstraňování jejich následků.

Ve většině případů jsou v České republice k financování kritické infrastruktury využívány **zdroje Evropské unie**. Od roku 2007 do roku 2013 financování kritické

infrastruktury probíhá prostřednictvím rámcového programu „**Bezpečnost a ochrana svobod**“. V rámci tohoto programu je stanoven specifický program „**Prevence, připravenost a zvládnání následků teroristických útoků**“. V rámci tohoto programu bylo navrženo vyčlenit z rozpočtu Evropské unie 137,4 milionů eur na financování tohoto specifického programu. Díky tomuto programu mohou národní, regionální i místní orgány předkládat své projekty na zlepšení bezpečnosti a chodu kritické infrastruktury, jež má být z tohoto programu také financována [27].

Další možností financování kritické infrastruktury České republiky ze zdrojů Evropské unie je pilotní projekt „**Boj s terorismem**“. Z tohoto projektu jde přes $\frac{2}{3}$ finančních zdrojů na přípravu Evropského programu na ochranu kritické infrastruktury (EPCIP).

Dalšími **zdroji Evropské unie**, které byly vyčleněny na kritickou infrastrukturu, jsou finanční prostředky na rozvoj transevropské dopravní sítě (TEN-T) v celkové výši 170 milionů eur. Během roku 2010 bylo vybráno pro financování 51 projektů, na kterých se podílí 24 členských států. Cílem tohoto programu je celkové zlepšení dopravní infrastruktury a zaměřuje se na tři oblasti: mořské dálnice, říční informační služby a systémy řízení letového provozu [61].

Slovenská republika má financování kritické infrastruktury upravováno v rámci **zákona č. 45/2011, o kritickej infraštruktúre** [44]. V § 9, odstavci 4 je uvedeno, že *„provozovatel má nárok na finanční příspěvek na plnění povinností souvisejících s výkonem bezpečnostních opatření na ochranu prvku podle bezpečnostního plánu, a to vůči ústřednímu orgánu na úseku kritické infrastruktury, do sektoru, kterému patří provozovatel, který mu ústřední orgán určí a tato povinnost mu nevyplývá z jiného všeobecně závazného právního předpisu. Pravidla poskytnutí finančního příspěvku budou určeny zvláštním předpisem, který vydá příslušný ústřední orgán.“*

Spojené státy americké mají financování kritické infrastruktury vypracovány pomocí **grantových programů**. Každý rok vláda investuje a uvolňuje finanční prostředky na různé oblasti kritické infrastruktury v určité výši a zajišťuje tak jejich údržbu. Např. v roce 2006 v **programu na ochranu kritické infrastruktury** (Infrastructure Protection Plan) bylo uvolněno 373 milionů dolarů na prevenci teroristických útoků, velkých havárií a dalších stavů nouze. Z toho bylo 136 milionů dolarů v rámci **programu ochrany dopravy** (Transit Security Grant Program) na železniční, lokální a trajektovou dopravu. V roce 2007 bylo uvolněno na ochranu kritické infrastruktury 445 milionů dolarů pro oblast průmyslu a další kritické

infrastruktury. V roce 2008 bylo uvolněno 844 milionů dolarů na oblasti kritické infrastruktury, jako jsou přístavy, přeprava, místní doprava. I v roce 2010 a 2011 jsou uvolňovány další finanční zdroje na ochranu kritické infrastruktury v různých grantových programech. Tyto grantové programy spravuje a prezentuje Ministerstvo národní bezpečnosti (Department of Homeland Security) [15].

Z tohoto všeho vyplývá, že většina kritických infrastruktur zemí světa je financována vládou státu, kdy se na financování může spolupodílet i provozovatel subjektu kritické infrastruktury. Na financování se také mohou podílet různé programy, dotace atd. Problém financování je ve spoustě zemí stále nedořešen a visí nad ním mnoho otazníků.

5 FORMULOVÁNÍ ZÁVĚRŮ, ZHODNOCENÍ A NÁVRHY

Jak již vyplynulo z celé této práce, je pro občany kritická infrastruktura životně důležitá. Je kritickým prvkem fungování státu a zabezpečuje základní lidské potřeby v období krize.

Z vývoje kritické infrastruktury vyplývá, že požadavek na správné fungování páteřních systémů státu není ničím novým. O zabezpečení majetku, zdraví a života lidí se snažili představitelé státu již v dávných dobách. Ve spoustě zemí světa je však historie kritické infrastruktury poměrně krátká. Důraz na kritickou infrastrukturu byl všeobecně pokládán spíše až po skončení druhé světové války a pak ještě později, mezi 80. a 90. lety 20. století. Vzhledem k tomu, že dodnes není kritická infrastruktura v některých státech ještě pevně dořešena a také se soudobá společnost neustále mění, můžeme počítat s dalším vývojem kritické infrastruktury, jak po stránce legislativní, tak po stránce její struktury. Historie kritické infrastruktury proto není uzavřenou kapitolou, ale bude se dále vyvíjet.

Kritická infrastruktura je dnes již pevně zakořeněný pojem, který se nechá různě definovat. Ve své podstatě je tento pojem vždy stejný, jak již bylo několikrát v této práci řečeno. Z provedené analýzy vyplynulo, že rámci vybraných států světa je řešení kritické infrastruktury podobné. V čem se může pojetí kritické infrastruktury lišit, nebo být stejné, je podrobněji rozebráno v kapitole 3 a 4.

Pojetí kritické infrastruktury jednotlivých států se dle provedeného zjištění velmi shoduje v definici kritické infrastruktury. Drobné odlišnosti jsou zde dány historickou

zkušeností a odlišností ve vnímání významu hrozeb. Česká republika např. pokládá větší důraz na ochranu před živelnými pohromami. Velká Británie a Německo zabezpečují nejvíce oblast informačních technologií vzhledem k možnosti útoku hackerů a dalších kyberteroristů. Spojené státy americké se naproti tomu velice zaměřují na boj s terorismem.

Po zhodnocení legislativy jednotlivých států nezbyvá, než podat návrh, aby byla legislativa kritické infrastruktury dořešena a na úrovni státu sjednocena. Legislativa kritické infrastruktury ve spoustě států není zcela ucelena. Vystává zde pak množství problémů, které souvisejí s povinnostmi osob při řešení krizí a také tím, kdo udílí pokyny k zavedení opatření pro zodolnění prvků kritické infrastruktury. Vážné poté také komunikace mezi subjekty kritické infrastruktury. Z provedené analýzy vyplynulo, že největším problémem je otázka financování kritické infrastruktury, kdy není způsob a rozsah financování přímo dán a vzniká pak řada nedorozumění a dalších problémů u subjektů kritické infrastruktury.

Pokud zhodnotíme strukturu kritické infrastruktury vybraných států, je možné hodnocení opřít o podrobnost vymezení prvků kritické infrastruktury. Velmi vyspělá je kritická infrastruktura Spojených států amerických, která má stanovenou propracovanou strukturu prvků a sektorů jednotlivých odvětví. Z analýzy dokumentů je zřejmé, že celá struktura kritické infrastruktury je propojena a komunikuje mezi sebou. Prvky jsou velmi detailně členěny, snaží se tedy neopomenout žádnou důležitou oblast. Otázka financování a chodu kritické infrastruktury je také velmi pěkně propracována. Většina financování spadá do grantových programů. Dokumenty, které řeší kritickou infrastrukturu, jsou hluboce zakořeněny v podvědomí lidí a apelují na národní hrdost amerických občanů. Jedná se většinou o prezidentské direktivy nebo plány, jež jsou velmi rozsáhlé a propracované do detailů.

Kritická infrastruktura např. Německa a Velké Británie není řešena tak detailně, avšak snaží se také poskytnout co největší záběr do všech oblastí, které mají co dělat se zabezpečením chodu státu. Kritická infrastruktura je zde lehce orientována jinak, s menším důrazem na boj s terorismem.

Kritická infrastruktura resp. její struktura a plán v České republice je velmi pěkně vypracována. Svoji strukturou se může rovnat vyspělejším a ekonomicky bohatším státům. Gesce za chod kritické infrastruktury jsou zde také dány. Nelze však bohužel vidět dále, jak je kritická infrastruktura udržována v chodu a nakolik je provozuschopná. Potřebný by v České republice byl jednoznačný návrh, který by určit,

jak bude kritická infrastruktura financována, kterým subjektům, a v jaké výši. Stejně tak by se mělo jasněji definovat, kdo se bude zabývat prvky kritické infrastruktury, která je součástí soukromého sektoru.

Málo propracovaná se zdá kritická infrastruktura Evropské unie. Zde je u pojetí kritické infrastruktury spíše podán jakýsi návrh na to, jak by měla společná kritická infrastruktura pracovat, je ukázán návod, jak ji řešit na evropské i národní úrovni, ale postupy nejsou jednoznačně stanoveny. Velkou oporou je však Evropská unie z hlediska financování kritické infrastruktury, kdy poskytuje členským státům finanční podporu, dotace a různé granty.

Struktura kritické infrastruktury je dle mého názoru ve většině států dostatečná, lehčí nedostatky je možné nalézt na poli dodržování postupů, povinností a odpovědnosti v kritické infrastruktuře a také ve financování kritické infrastruktury.

ZÁVĚR

V této práci byla na vybraných zemích ilustrována kritická infrastruktura, její ochrana, její vývoj, prvky a sektory.

Důležitou roli v kritické infrastruktuře hraje stát. Stát jako instituce, by měl umět poskytnout svým obyvatelům pocit, že je krizová situace řešena nejlepším možným způsobem. Občané bez pomoci státu nemají takové možnosti, potýkat se s problémy obrovských rozměrů, které ochromí většinu z nich. Na státu tedy je, aby zajistil chod páteřních systémů a chod společnosti v krizových situacích. Měl by se snažit zajistit lidem základní potřeby, jako jsou světlo, teplo, voda, jídlo, možnost dopravit se do svých domovů, poskytnout jim zdravotní péči, postarat se o jejich ochranu a bezpečí.

Na státu také bývá odpovědnost za jeho další fungování. Stará se tedy i o ekonomické bezpečí státu, výstrahu občanům, komunikaci a výzkumné aktivity.

První část práce se zaměřila na historický vývoj a souvislosti, které vedly a nadále povedou k formování pojetí kritické infrastruktury ve vybraných zemích světa. Pojem infrastruktura byl znám již dávno, pojem kritická infrastruktura je však téměř novodobý pojem, jehož pojetí, definování a význam není ještě plně ustálen. Kritická infrastruktura se tedy bude dále vyvíjet a zdokonalovat, a proto je nutné znát historické spojitosti, které vedly k současné situaci v pojetí kritické infrastruktury.

Ve druhé části práce bylo uvedeno základní pojmosloví, které je nutné znát, aby bylo možné dále s pojmem kritická infrastruktura a jejím pojetím, pracovat. Tato část také členila jednotlivé prvky kritické infrastruktury, které jsou v menších či větších obměnách obsaženy v pojetí kritické infrastruktury vybraných zemí. Seznámení s prvky kritické infrastruktury je nutné vzhledem k pochopení propojení „sítí“ kritické infrastruktury a její vzájemné závislosti.

Třetí část práce se zabývala již pojetím kritické infrastruktury ve vybraných zemích. Pro tuto práci byla k deskripci vybrána Evropská unie a 4 její členské státy, Česká republika, Slovenská republika, Spolková republika Německo a Velká Británie. Další vybranou zemí byly vzhledem k propracovanosti kritické infrastruktury Spojené státy americké. Na společenství Evropské unie a vybraných zemích byl proveden popis pojetí kritické infrastruktury a její struktura.

Čtvrtá část práce se zabývala porovnáním, která vyplynula z analýzy v předchozích kapitolách. Porovnání pojetí kritické infrastruktury se odehrávalo z hlediska pojetí, legislativy, prvků a sektorů kritické infrastruktury a jejího financování ve vybraných zemích, které byly již zmíněny v kapitole č. 3.

Poslední část práce se zabývala formulací závěrů, zhodnocením stavu pojetí kritické infrastruktury a návrhy, které by mohly vést ke zlepšení struktury kritické infrastruktury.

Cíl této práce, ilustrovat pojetí kritické infrastruktury v mezinárodním srovnání a provést jeho komparaci, **byl tedy splněn.**

POUŽITÁ LITERATURA

- [1] **BRS.** *Zpráva o stavu zajištění bezpečnosti České republiky.* Praha : Úřad vlády ČR, 2006.
- [2] **BSI.** Schutz Kritischer Infrastrukturen in Deutschland. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] [Cit.: duben 19, 2011.]
https://www.bsi.bund.de/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html.
- [3] **Bundeskabinett.** Bundesamt für Sicherheit in der Informationstechnik. *Umsetzungsplan KRITIS.* [Online] 2007. [Cit.: březen 9, 2011.]
https://www.bsi.bund.de/cln_183/DE/Themen/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html.
- [4] **Cabinet Office.** *Sector Resilience Plan for Critical Infrastructure 2010.* [Online] březen 2010. [Cit.: březen 9, 2011.] <http://www.dri-italy.com/public/sector-resilience-plan.pdf>.
- [5] **Centre for Security Cooperation.** RACVIAC. *RACVIAC - SE Europe.* [Online] [Cit.: duben 19, 2011.] <http://www.racviac.org/>.
- [6] **Česká národní banka.** Měnová politika. *Česká národní banka.* [Online] 2003-2011. [Cit.: 19. duben 2011.] http://www.cnb.cz/cs/menova_politika/.
- [7] **Český telekomunikační úřad.** ČTÚ. [Online] 2008. [Cit.: duben 19, 2011.] <http://www.ctu.cz/>.
- [8] **CPNI.** Centre for the Protection of National Infrastructure. *Centre for the Protection of National Infrastructure.* [Online] [Cit.: únor 23, 2011.] <http://www.cpni.gov.uk/>.
- [9] **ČT 24.cz.** Nejenom ropa, boje v Libyi hýbou i cenami plynu. *LinksTip.com.* [Online] duben 8, 2011. [Cit.: duben 18, 2011.]
[http://www.linkstip.com/cz/tip/?t=Nejenom+ropa%2C+boje+v+Libyi+h%C3%BDbou+i+cenami+plynu+\(08.04.2011+21%3A54+\)&u=238526](http://www.linkstip.com/cz/tip/?t=Nejenom+ropa%2C+boje+v+Libyi+h%C3%BDbou+i+cenami+plynu+(08.04.2011+21%3A54+)&u=238526).

- [10] **ČTK.** Blesk.cz. *Desítky milionů Brazilců několik hodin bez proudu*. [Online] listopad 11, 2009. [Cit.: březen 13, 2011.] <http://www.blesk.cz/clanek/zpravy-novinky-zahranici/126682/desitky-milionu-brazilcu-nekolik-hodin-bez-proudu.html>.
- [11] **ČTK.** Zemětřesení v Japonsku může ohrozit ekonomický růst. *Finanční noviny.cz*. [Online] 2011. [Cit.: březen 14, 2011.] <http://www.financninoviny.cz/zpravy/zemetreseni-v-japonsku-muze-narusic-ekonomicky-rust/608049>.
- [12] **Department of Homeland Security.** *Critical Infrastructure and Key Resources*. Washington : DHS, 2010.
- [13] **Department of Homeland Security.** Homeland Security. *Department of Homeland Security*. [Online] [Cit.: únor 24, 2011.] <http://www.dhs.gov/index.shtm>.
- [14] **Department of Homeland Security.** *National Infrastructure Protection Plan*. Washington : DHS, 2009.
- [15] **Department of Homeland Security.** Open for Business - Grants. *Department of Homeland Security*. [Online] červenec 10, 2010. [Cit.: březen 23, 2011.] <http://www.dhs.gov/xopnbiz/grants/>.
- [16] **Electronic Privacy Information Centre.** Patriot Act. *EPIC*. [Online] 2005. [Cit.: březen 10, 2011.] <http://epic.org/privacy/terrorism/usapatriot/>.
- [17] **Europa.** Členské země Evropské unie. *Portál Evropské unie*. [Online] [Cit.: duben 19, 2011.] http://europa.eu/about-eu/member-countries/index_cs.htm.
- [18] **Evropská komise.** Vesmír na Zemi. *Evropská komise - podnikání a průmysl*. [Online] říjen 31, 2010. [Cit.: duben 19, 2011.] http://ec.europa.eu/enterprise/policies/space/index_cs.htm.
- [19] **ExxonMobil.** Co je zemní plyn. *Zemní plyn*. [Online] 2004. [Cit.: březen 13, 2011.] <http://www.zemniplyn.cz/plyn/>.
- [20] **FALTÝNEK, V.** Události. *Český rozhlas*. [Online] 2008. [Cit.: březen 13, 2011.] <http://www.radio.cz/cz/rubrika/udalosti/rwe-transgas-vypadky-plynu-bez-potizi-vykryjeme>.

- [21] **GAS, s.r.o.** Zemní plyn. *Zemní plyn.cz*. [Online] 2007-2010. [Cit.: duben 19, 2011.] <http://www.zemniplyn.cz/plyn/>.
- [22] **HABJANEC, D.** Ropa. *Zdroje energie*. [Online] říjen 9, 2008. [Cit.: duben 19, 2011.] <http://zdrojeenergie.blogspot.com/2008/10/ropa.html>.
- [23] **Hasičský záchranný sbor České republiky.** Integrovaný záchranný systém. *HZS ČR*. [Online] červen 26, 2009. [Cit.: duben 19, 2011.] <http://www.hzscr.cz/clanek/integrovaný-zachranný-system.aspx>.
- [24] **HEJDOVÁ, J., ŠEBKOVÁ, A.** Současnost a budoucnost kritické infrastruktury v oblasti zdravotnictví. *Úrazová nemocnice v Brně*. [Online] únor 2009. [Cit.: únor 22, 2011.] http://www.unbr.cz/Data/files/Konf%20MeKa09/07_Hejdová.pdf.
- [25] **Kolektiv.** *Akademický slovník cizích slov*. Praha : Academia, 2000.
- [26] **Komise evropských společenství.** *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury*. Brusel : s.n., 2006.
- [27] **Komise evropských společenství.** *Sdělení, kterým se stanoví rámcový program "Bezpečnost a ochrana svobod" na roky 2007-2013*. Brusel : s.n., 2005.
- [28] **Komise evropských společenství.** *Směrnice Rady o určování a označování ECI a o posouzení potřeby zvýšit její ochranu*. Brusel : s.n., 2006.
- [29] **Komise evropských společenství.** Zelená kniha o evropském programu na ochranu kritické infrastruktury. *EUR-Lex*. [Online] listopad 17, 2005. [Cit.: únor 23, 2011.] http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf.
- [30] **KOVAŘÍK, J.** *Kritická infrastruktura a ochrana obyvatelstva*. 2007. Ochrana obyvatel. pp. 145 - 153.
- [31] **Krize.eu.** Ekonomická krize. *Krize.eu*. [Online] říjen 31, 2009. [Cit.: duben 18, 2011.] <http://krize.eu/ekonomicka-krize>.
- [32] **LÁGNER, A.** Kde se bere elektrická energie. *Příroda.cz*. [Online] červen 11, 2004. [Cit.: duben 19, 2011.] <http://www.priroda.cz/clanky.php?detail=95>.
- [33] **LINHART, J. a kol.** *Slovník cizích slov pro nové století*. Litvínov : Dialog, 2003. 412 s. ISBN 80-85843-61-7.

- [34] **LINHART, Petr, ROUDNÝ, Radim.** *Ochrana obyvatelstva a terorismus.* 1.vyd. Pardubice : Univerzita Pardubice, 2009. 237 s. ISBN 978-80-7395-165-8.
- [35] **Ministerstvo vnitra SR.** *Zákon č. 45/2011 o kritické infrastruktuře.* Bratislava : s.n., 2011.
- [36] **Ministerstvo dopravy ČR.** Akční plány. *Ministerstvo dopravy ČR.* [Online] 2006. [Cit.: duben 19, 2011.] http://www.mdcz.cz/cs/Strategie/Akcni_plany/akcni_plany.htm.
- [37] **Ministerstvo průmyslu a obchodu ČR.** Průmysl a stavebnictví. *Ministerstvo průmyslu a obchodu ČR.* [Online] 2005. [Cit.: duben 19, 2011.] <http://www.mpo.cz/cz/prumysl-a-stavebnictvi/>.
- [38] **Ministerstvo vnitra ČR.** *Ministerstvo vnitra ČR.* [Online] [Cit.: březen 7, 2011.] <http://www.mvcr.cz/clanek/kriticka-infrastruktura.aspx>.
- [39] **Ministerstvo vnitra ČR.** *Ministerstvo vnitra ČR.* [Online] 2010. [Cit.: březen 13, 2011.] <http://www.mvcr.cz/clanek/kriticka-infrastruktura.aspx>.
- [40] **Ministerstvo vnitra ČR.** *Národní akční plán boje proti terorismu aktualizované znění pro léta 2007 - 2009.* Praha : s.n., 2008.
- [41] **Ministerstvo zdravotnictví ČR.** Ministerstvo zdravotnictví ČR. [Online] 2010. [Cit.: duben 19, 2011.] <http://www.mzcr.cz/>.
- [42] **Ministerstvo zemědělství ČR.** e-Agri. *Potraviny.* [Online] 2009-2010. [Cit.: duben 19, 2011.] <http://eagri.cz/public/web/mze/potraviny/urad-pro-potraviny/>.
- [43] **Ministerstvo zemědělství ČR.** Vodohospodářský informační portál. [Online] 1999-2009. [Cit.: duben 19, 2011.] <http://www.voda.gov.cz/portal/cz/>.
- [44] **Ministerstvo vnitra SR.** *Národní program pro ochranu kritické infrastruktury.* Bratislava : s.n., 2007.
- [45] **MOTEFF, J., PARFOMAK, P.** Critical Infrastructure and Key Assets: Definition and Identification. *CRS Report for Congress.* říjen 1, 2004.
- [46] **MOZGA, Jaroslav, VÍTEK, Miloš, KOVÁŘÍK, František.** *Kritická infrastruktura společnosti.* 1. vyd. Hradec Králové : Gaudeamus, 2008. 155 s. ISBN 978-80-7041-299-2.

- [47] **MOZGA, Jaroslav.** Kritická infrastruktura a veřejná správa. *The science for population protection*. [Online] 2008. [Cit.: únor 22, 2011.] http://www.population-protection.eu/attachments/036_vol0_mozga.pdf.
- [48] **Parlament ČR.** Zákon č. 239/2000 Sb., o integrovaném záchranném systému. *Sagit*. [Online] červen 28, 2000. [Cit.: duben 19, 2011.] <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00239&cd=76&typ=r>.
- [49] **Parlament ČR.** Zákon č. 240/200 Sb., o krizovém řízení. *Sagit*. [Online] červen 28, 2000. [Cit.: duben 19, 2011.] <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00240&cd=76&typ=r>.
- [50] **PATOČKA, J.** Jadernou elektrárnu Fukušima 1 postihla havárie. *Deník Referendum*. [Online] březen 12, 2011. [Cit.: březen 15, 2011.] <http://denikreferendum.cz/clanek/9483-jadernou-elektrarnu-fukusima-1-postihla-havarie>.
- [51] **PROCHÁZKOVÁ, Dana.** *Plány obnovy, kritická infrastruktura, plány kontinuity a podpůrný systém pro rozhodování*. Praha : Cityplan spol. s r.o., 2006.
- [52] **PROCHÁZKOVÁ, Dana.** Základní legislativa. *Bezpečnost a krizové řízení*. Praha : Police History, 2006, pp. 166-167. 255 s. ISBN 80-86477-35-5.
- [53] **ŘÍHA, J.** *Typologické znaky kritické infrastruktury*. 2009, The Science for Population Protection.
- [54] **ROUDNÝ, Radim, LINHART, Petr.** *Krizový management I*. 1. vyd. Pardubice : Univerzita Pardubice, 2005. 97 s. ISBN 80-7194-674-5.
- [55] **ŠENOVSKÝ, Michail, ADAMEC, Vilém, ŠENOVSKÝ, Pavel.** *Ochrana kritické infrastruktury*. 1. vyd. Ostrava : SPBI, 2007. 141 s. ISBN 978-80-7385-025-8.
- [56] **SMRČKA, V.** Havárie v Opatovicích ovlivní vývoj teplárenství. *Profit.cz*. [Online] 2002. [Cit.: březen 13, 2011.] <http://www.profit.cz/clanek/havarie-v-opatovicich-ovlivni-vyvoj-teplarenstvi.aspx>.
- [57] **Správa státních hmotných rezerv České republiky.** Správa státních hmotných rezerv České republiky. *SSHR*. [Online] 2009. [Cit.: březen 7, 2011.] <http://www.sshr.cz/stranky/default.aspx>.

[58] **Vláda ČR.** *Ústavní zákon č. 1/1993 Sb., Ústava České republiky.* Praha : s.n., 1993.

[59] **Vláda ČR.** Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. *Ministerstvo obrany České republiky.* [Online] duben 22, 1998. [Cit.: duben 18, 2011.] https://www.army.cz/images/id_0000_1000/172/_stavn__z__kon__._110-1998_Sb..pdf.

[60] **Vláda ČR.** Výbor pro civilní nouzové plánování. *Vláda České republiky.* [Online] duben 15, 2008. [Cit.: únor 22, 2011.] <http://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/pracovni-vybory/civilni-nouzove-planovani/vybor-pro-civilni-nouzove-planovani-36255/>.

[61] **Zastoupení Evropské komise v ČR.** EU poskytne 170 milionů eur na projekty kritických infrastruktur v celé Evropě. *BusinessInfo.cz.* [Online] únor 21, 2011. [Cit.: březen 23, 2011.] <http://www.businessinfo.cz/cz/clanek/aktuality-z-evropske-unie/170-mil-projekty-kriticke-infrastruktury/1000661/59825/>.

SEZNAM PŘÍLOH

- Příloha A:** Sektory KI Evropské unie dle Zelené knihy o Evropském programu na ochranu kritické infrastruktury
- Příloha B:** Oblasti KI v České republice dle Usnesení BRS č. 30/2007
- Příloha C:** Oblasti KI v Německu dle National Strategy for Critical Infrastructure Protection
- Příloha D:** Sektory KI Velké Británie dle Sector Resilience Plan for Critical Infrastructure 2010
- Příloha E:** Sektory KI Slovenska dle zákona č. 45/2011 Sb., o kritickej infraštruktúre
- Příloha F:** Sektory KI v USA dle Critical Infrastructure and Key Resources 2010

Příloha A

Sektory KI Evropské unie dle Zelené knihy o Evropském programu na ochranu kritické infrastruktury

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector	Product or service
I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines
	2 Electricity generation
	3 Transmission of electricity, gas and oil
	4 Distribution of electricity, gas and oil
II Information, Communication Technologies, ICT	5 Information system and network protection
	6 Instrumentation automation and control systems (SCADA etc.)
	7 Internet
	8 Provision of fixed telecommunications
	9 Provision of mobile telecommunications
	10 Radio communication and navigation
	11 Satellite communication
	12 Broadcasting
III Water	13 Provision of drinking water
	14 Control of water quality
	15 Stemming and control of water quantity
IV Food	16 Provision of food and safeguarding food safety and security
V Health	17 Medical and hospital care
	18 Medicines, serums, vaccines and pharmaceuticals
	19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/payment structures (private)
	21 Government financial assignment
VII Public & Legal Order and Safety	22 Maintaining public & legal order, safety and security
	23 Administration of justice and detention
VIII Civil administration	24 Government functions
	25 Armed forces
	26 Civil administration services
	27 Emergency services
	28 Postal and courier services
IX Transport	29 Road transport
	30 Rail transport
	31 Air traffic
	32 Inland waterways transport
	33 Ocean and short-sea shipping
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances
	35 Pipelines of dangerous goods (chemical substances)
XI Space and Research	36 Space
	37 Research

Příloha B

Oblasti KI v České republice dle Usnesení BRS č. 30/2007

Poř	Oblast KI	Produkt nebo služba	Gesce/ Spolugesce
1	Energetika	1.1. Elektřina	MPO/ERÚ
		1.2. Plyn	MPO/ERÚ
		1.3. Tepelná energie	MPO/ERÚ
		1.4. Ropa a ropné produkty	SSHR/MPO
2	Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou	MZe
		2.2. Zabezpečení a správa povrchových vod a podzemních zdrojů vody	MZe/MŽP
		2.3. Systém odpadních vod	MZe
3	Potravinařství a zemědělství	3.1. Produkce potravin	MZe
		3.2. Péče o potraviny	
		3.3. Zemědělská výroba	
4	Zdravotní péče	4.1. Přednemocniční neodkladná péče	MZ
		4.2. Nemocniční péče	
		4.3. Ochrana veřejného zdraví	
		4.4. Výroba, skladování a distribuce léčiv a zdravotnických prostředků	
5	Doprava	5.1. Silniční	MD
		5.2. Železniční	
		5.3. Letecká	
		5.4. Vnitrozemská vodní	
6	Komunikační a informační systémy	6.1. Služby pevných telekomunikačních sítí	MPO/MI/ČTÚ
		6.2. Služby mobilních telekomunikačních sítí	
		6.3. Radiová komunikace a navigace	
		6.4. Satelitní komunikace	
		6.5. Televizní a rádiové vysílání	
		6.6. Poštovní a kurýrní služby	
		6.7. Přístup k internetu a k datovým službám	MV/MI
7	Bankovní a finanční sektor	7.1. Správa veřejných financí	MF
		7.2. Bankovníctví	ČNB
		7.3. Pojišťovnictví	MF/ČNB
		7.4. Kapitálový trh	
8	Nouzové služby	8.1. Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany	MV
		8.2. Policie ČR (vnitřní bezpečnost a veřejný pořádek)	MV
		8.3. Armáda ČR (zabezpečení obrany)	MO
		8.4. Radiační monitorování vč. podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření	SÚJB
		8.5. Předpovědní, varovná a hlásná služba	MŽP
9	Veřejná správa	9.1. Státní správa a samospráva	MV/ÚSÚ
		9.2. Soc. ochrana a zaměstnanost (soc. zabezpečení, stát.soc. podpora, soc. pomoc)	MPSV
		9.3. Výkon justice a vězeňství	MS

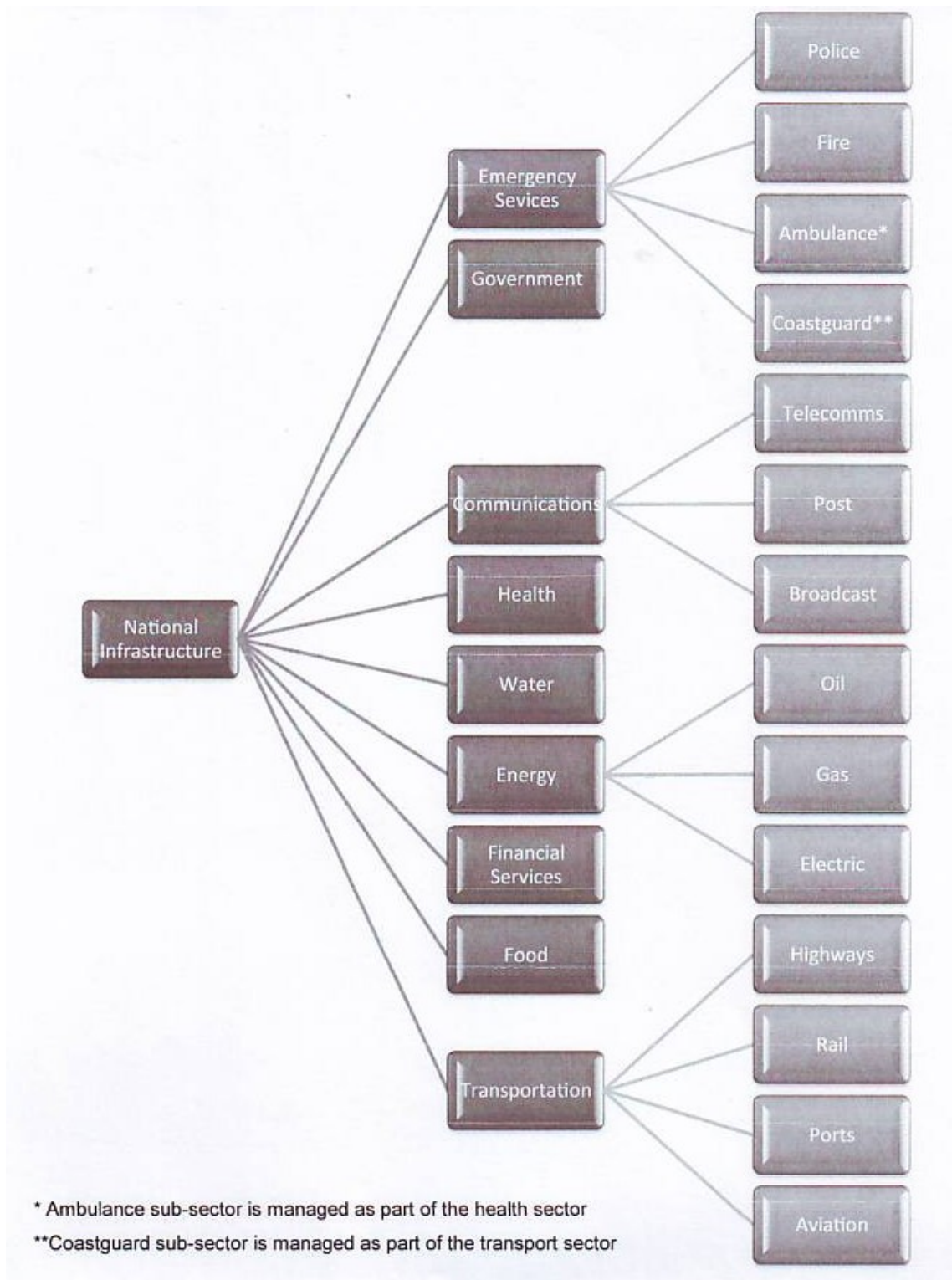
Příloha C

Oblasti KI v Německu dle National Strategy for Critical Infrastructure Protection

Technical basic infrastructure	Socio-economic services infrastructure
Power supply	Public health; food
Information and communications technology	Emergency and rescue services; disaster control and management
Transport(ation)	Parliament; government; public administration; law enforcement agencies
(Drinking-) water supply and sewage disposal	Finance; insurance business
	Media; and cultural objects (cultural heritage items)

Příloha D

Sektory KI Velké Británie dle Sector Resilience Plan for Critical Infrastructure 2010



Příloha E

Sektory KI Slovenska dle zákona č. 45/2011 Sb., o kritické infrastruktuře

Sektor	Podsektor	Ústřední orgán
1. Doprava	Cestná doprava Letecká doprava Vodná doprava Železniční doprava	Ministerstvo dopravy, výstavby a regionálního rozvoje Slovenskej republiky
2. Elektronické komunikácie	Satelitná komunikácia Siete a služby pevných a mobilných elektronických komunikácií	Ministerstvo dopravy, výstavby a regionálního rozvoje Slovenskej republiky
3. Energetika	Baníctvo Elektroenergetika Plynárenstvo Ropa a ropné produkty	Ministerstvo hospodárstva Slovenskej republiky
4. Informačné a komunikačné technológie	Informačné systémy a siete Internet	Ministerstvo financií Slovenskej republiky
5. Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	Ministerstvo dopravy, výstavby a regionálního rozvoje Slovenskej republiky
6. Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky
7. Voda a atmosféra	Meteorologická služba Vodné stavby Zabezpečovanie pitnej vody	Ministerstvo životného prostredia Slovenskej republiky
8. Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky

Příloha F

Sektory KI v USA dle Critical Infrastructure and Key Resources 2010

Critical Infrastructure Key Resources (CIKR)															
Agriculture and Food	Defense and Industrial Base	Energy	Public Health and Healthcare	Manufacturing and Services	Banking and Finance	Water	Chemical	Commercial facilities	Emergency Services	Materials, Resources and	Telecommunications	Critical Manufacturing	Aviation and Shipping Services	Transportation	Information Technology
Food Retail \$. - Units	Defense \$. - Units	Coal mining \$. - Units	Public Health \$. - Units	United States \$. - Units	Credit lending \$. - Units	Public utilities \$. - Units	Organic \$. - Units	Hotels \$. - Units	Fire Departments \$. - Units	Electric utilities \$. - Units	Telephone/Cell \$. - Units	Iron and Steel \$. - Units	United States \$. - Units	AMTRAK \$. - Units	Hardware \$. - Units
Food processing \$. - Units	Industry \$. - Units	Coal power \$. - Units	Private medical \$. - Units	Travel services \$. - Units	Commercial \$. - Units	Desalination \$. - Units	Organic industrial \$. - Units	Shopping centers \$. - Units	Law enforcement \$. - Units	Reactor and \$. - Units	Satellite data \$. - Units	Aluminum \$. - Units	High volume \$. - Units	Commuter rail \$. - Units	IT \$. - Units
Farm \$. - Units	Private for \$. - Units	Coal plants \$. - Units	Private equity \$. - Units	Lodging \$. - Units	Private equity \$. - Units	Treatment \$. - Units	Ceramics \$. - Units	Stadiums and \$. - Units	Search and \$. - Units	University and \$. - Units	Broadcasting \$. - Units	Nonferrous \$. - Units	Inter-city rail \$. - Units	Freight rail \$. - Units	Semiconductor \$. - Units
Meat/Poultry \$. - Units	Clincs \$. - Units	Coal \$. - Units	Consumer \$. - Units	Equipment \$. - Units	Private equity \$. - Units	Plants \$. - Units	Petrochemicals \$. - Units	Schools \$. - Units	Emergency \$. - Units	Medical \$. - Units	Broadband \$. - Units	Metals \$. - Units	Container \$. - Units	Commercial \$. - Units	Electronics \$. - Units
Processing \$. - Units	Private medical \$. - Units	Manufacturers \$. - Units	Building \$. - Units	Pipe and water \$. - Units	Consumer \$. - Units	Manufacturers \$. - Units	Appliances \$. - Units	Offices \$. - Units	Police \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Marine \$. - Units	Airline \$. - Units	Manufacturing \$. - Units
Food \$. - Units	Medical \$. - Units	Hydroelectric \$. - Units	Private banks \$. - Units	Compl devices \$. - Units	Building \$. - Units	Compl devices \$. - Units	Polymers \$. - Units	Universities \$. - Units	Nuclear safety \$. - Units	Systems \$. - Units	Radio \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Dairy \$. - Units	Pharmaceutical \$. - Units	Dam \$. - Units	Merchant \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Processing \$. - Units	Pharmaceutical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Dairy Farms \$. - Units	Health \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Ranching \$. - Units	Insurance \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Organic \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Farming/Sustainable \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Agriculture \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Traditional \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Fishing \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Commercial \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units
Fishing \$. - Units	Medical \$. - Units	Wind power \$. - Units	Global financial \$. - Units	Compl devices \$. - Units	Commercial \$. - Units	Compl devices \$. - Units	Plastics \$. - Units	Universities \$. - Units	Transportation \$. - Units	Control \$. - Units	Equipment \$. - Units	Metals \$. - Units	Private air \$. - Units	Private air \$. - Units	IT services \$. - Units

