Komparace přístupů k ochraně kritické infrastruktury v České republice a Velké Británii

A Comparison of Critical Infrastructure Protection Approaches in the Czech Republic and Great Britain

Bc. Jiří Koňařík

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jiří KOŇAŘÍK**
Osobní číslo:	**A10856**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Komparace přístupů k ochraně kritické infrastruktury v České republice a Velké Británii**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma kritická infrastruktura.**
2. **Pojednejte o současném stavu problematiky kritické infrastruktury v České republice a Velké Británii.**
3. **Diskutujte o ochraně kritické infrastruktury v České republice.**
4. **Analyzujte ochranu kritické infrastruktury ve Velké Británii.**
5. **Proveďte komparaci aktuálních přístupů k ochraně kritické infrastruktury v České republice a Velké Británii.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **EU. Critical Infrastructure Protection in the fight against terrorism. In Communication from the commission to the council and the european parliament. 2004, 345, Dostupný také z WWW: [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF].**
2. **EU. Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In Council directive 2008/114/EC. 2008, 345, Dostupný tiež z WWW: [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en:PDF].**
3. **Nařízení vlády č. 462/2000 Sb., k provedení Ô 27 odst. 8 a Ô 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).**
4. **MOZGA, J.; VÍTEK, M.; KOVÁŘÍK, F., Kritická infrastruktura společnosti. 1. Hradec Králové : Gaudeamus, 2008. 156 s. ISBN 978-80-7041-299-2.**
5. **HORÁK R.; SALINGER T.; NAVRÁTIL J.; Řešení kritické infrastruktury s možností využití nástrojů EU, Ochrana obyvatel 2007, Ostrava, 2007, ISBN 80-86634-51-5**

Vedoucí diplomové práce: **Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá kritickou infrastrukturou a její ochranou v České republice a ve Velké Británii a následným srovnáním přístupů k této problematice v uvedených zemích. Práce je rozdělena na dvě hlavní části. V první části se práce zabývá historií, vývojem a právním vymezením kritické infrastruktury. V rámci první části je také provedeno rozdělení sektorů kritické infrastruktury v obou zemích a obsahuje také popis současných hrozeb. Druhá část práce se zabývá ochranou kritické infrastruktury v České republice a ve Velké Británii. V této části je pak také provedeno srovnání kritické infrastruktury a její ochrany v uvedených zemích.

Klíčová slova:

Kritická infrastruktura, ochrana kritické infrastruktury, oblasti kritické infrastruktury, hrozba, národní kritická infrastruktura.

ABSTRACT

This thesis deals with the critical infrastructure and its protection in the Czech Republic and Great Britain, and compares the approaches to this issue in those countries. The work is divided into two main parts. In the first part of the thesis deals with the history, development and legislation definition of critical infrastructure. In the first part is done the distribution of critical infrastructure sectors in both countries and also includes a description of the current threats. The second part deals with the protection of critical infrastructure in the Czech Republic and Great Britain. This section also compares the critical infrastructure and its protection in those countries.

Keywords:

Critical infrastructure, protection of critical infrastructure, critical infrastructure sectors, threat, critical national infrastructure.

Na tomto místě bych chtěl poděkovat Ing. Martinu Hromadovi, Ph.D., vedoucímu mé diplomové práce, za cenné připomínky, odborné vedení a podnětné rady, kterými velkou měrou přispěl k vypracování této diplomové práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Problematika kritické infrastruktury a její ochrany je v současnosti aktuální společenské téma. Myslím si, že mezi širokou veřejností v České republice je kritická infrastruktura pořád celkem málo známy pojem. Za posledních několik let se však v této problematice dosáhlo jistých pokroků, jak u nás tak i v jiných zemích celého světa. I přesto si myslím, že problematika kritické infrastruktury a její ochrany si zasluhuje mnohem větší pozornost, než která jí je doposud věnována.

Mnoho lidí si stále zcela neuvědomuje, jak je naše současná společnost zranitelná. K udržení současného evropského životního standardu je zapotřebí mnoho úsilí a prostředků.

V diplomové práci se zpočátku zabývám historií a vývojem kritické infrastruktury. Stručně charakterizuji základní pojmy kritické infrastruktury a následně se zabývám kritickou infrastrukturou v České republice a ve Velké Británii. Úkolem bude také rozepsat možné současné hrozby a rizika. V druhé části diplomové práce bude mým úkolem řešit ochranu kritické infrastruktury ve vybraných zemích. Budu se zabývat ochranou kritické infrastruktury v České republice a ve Velké Británii, abych následně mohl porovnat přístupy obou zemí k dané problematice.

Cílem diplomové práce bude poukázat na to, jak rozsáhlá je problematika ochrany kritické infrastruktury. Úkolem je popsat a zhodnotit přístup k ochraně kritické infrastruktury u nás a ve Velké Británii a na konec srovnat přístupy obou zemí. Důvodem, proč jsem si vybral pro srovnání Velkou Británii, je především to, že jsem chtěl vycházet z anglicky psaných dokumentů a také fakt, že této problematice se začala jako první v Evropské unii věnovat právě Velká Británie. Přesto, že jsou obě země členy Evropské unie, mají mnoho zásadních odlišností, jako například státní zřízení, velikost, počet obyvatel a ekonomické postavení. Tyto důvody také přispěly k tomu, že jsem si vybral právě Velkou Británii.

Rozhodl jsem se zaměřit na problematiku kritické infrastruktury, protože ji vnímám jako velmi důležitou oblast pro zachování základních funkcí státu a zachování důležitých potřeb pro všechny obyvatele, tedy včetně mě samotného. Problematika kritické infrastruktury a její ochrany je velice rozsáhlá a není možné ji celou popsat v této práci. Z toho důvodu tato práce obsahuje jen malou část této tématiky.

I. TEORETICKÁ ČÁST

1 KRITICKÁ INFRASTRUKTURA – ÚVOD DO PROBLEMATIKY

1.1 Historie kritické infrastruktury

Jako každé jiné odvětví, tak i ochrana kritické infrastruktury má svoji historii a svůj vývoj. S rozvojem elektroniky, internetu a počítačových sítí také roste potřeba zvyšování bezpečnosti. Zvyšování bezpečnosti na úrovni jednotlivých osob a občanů je samozřejmostí, ale stále důležitější je chránit nezbytně důležité oblasti na úrovni státu, jako je například energetika, doprava atd. Tyto prvky tvoří národní kritickou infrastrukturu a v případě selhání některého z nich to může mít pro stát závažný dopad.

V každé době byl člověk nucen si chránit svoje jmění a důležité hodnoty. Je potřeba si uvědomit, že za posledních několik století se naprosto změnila lidská obydlí. V minulosti bylo zcela obvyklé budovat opevněné sídla a pevnosti, které se vyznačovaly svoji vysokou pevností a uzavřeností proti okolnímu světu. Dalo by se říci, že ve většině případů byly pevnosti soběstačné a jen těžko dobytné. Uvnitř byl k dispozici zdroj pitné vody, zásoby potravin, suroviny na vlastní výrobu. V takovém případě bylo pro nepřítele těžké do pevnosti proniknout. Nepřítel měl tedy dvě možnosti, buď pevnost dobýt, na to však byla potřeba velké početní přesila. Druhou možností bylo obléhání tak dlouho, dokud uvnitř pevnosti nedošly zásoby a suroviny. Obyvatelé sami snižovali zranitelnost pevností a sídel stavěním mohutnějších hradeb, vodních příkopů, také zvětšováním zásob surovin, nebo zajištěním vlastních služeb uvnitř pevností.

V dnešní době je situace v tomto směru zcela odlišná. V žádném z velkých civilizovaných měst není po obvodu vystavěna hradba. Dnes jsou metropole zcela otevřené, neomezené hradbami a každý se v nich může libovolně pohybovat. Případný narušitel by mohl vstoupit do metropole zcela bez překážek. Dokonce by pro narušitele ani nebylo nutné vstupovat přímo na území města. K tomu, aby se zhroutil obyčejný život ve městě, by narušiteli stačilo napadnout kritickou infrastrukturu mimo území města. Stačilo by například narušit elektrické napájení města, zdroje vody, dodávky ropy a chod města je zcela ohromen.

Zcela jednoznačně nejdůležitějšími infrastrukturami jsou energetika, doprava a informační a komunikační technologie. Vezmeme si pro příklad elektrickou energii. V současnosti je na elektrické energii člověk zcela závislý a přitom z historického hlediska je to vynález

nový. Elektřina je tak důležitá, že dnešní život si bez ní jen těžko dokážeme představit. Všechny ostatní kritické infrastruktury jsou na elektřině rovněž závislé. Není jediného odvětví, které by ke svému chodu nevyužívalo elektrickou energii, i když ne třeba přímo tak nepřímo je využívána naprosto všude. Stačí si jen představit, co by se stalo v případě narušení dodávek elektřiny například do nemocnic, nebo kolik životů a škod by napáchal výpadek elektřiny v semaforech a jiných řídicích systémech.

Na těchto příkladech a tisíce dalších si musí každý z nás uvědomit, že vymezení kritických infrastruktur je v současnosti velice důležité a zabývat se jejich ochranou je jednou z priorit fungování každého vyspělého státu. Je potřeba si určit, které infrastruktury jsou zcela nezbytné pro fungování státu a následně se pečlivě věnovat jejich ochraně.

1.2 Novodobý vývoj kritické infrastruktury

Problémem ochrany kritické infrastruktury se lidstvo zabývá v podstatě již od nepaměti. Samotné pojmy kritická infrastruktura a ochrana kritické infrastruktury jsou novodobé označení. Je potřeba si ale uvědomit, že i před tím než tyto pojmy byly definovány, se ochrana kritické infrastruktury do jisté míry řešila vždy, samozřejmě, že čím dál více.

1.2.1 Vývoj v USA

USA a Austrálie byly prvními zeměmi, které začaly v širším hledisku vnímat potenciál a šíři problematiky kritické infrastruktury. Právě tyto dvě země odstartovaly diskuse o ochraně životně důležitých infrastruktur. Diskutovalo se o jejich ochraně, zranitelnosti a možných rizicích a hrozeb. Později vznikl ustálený pojem kritická infrastruktura. Prvním uceleným dokumentem, zabývajícím se ochranou kritické infrastruktury byla tzv. Bíla kniha. Jednalo se o směrnici 63 (direktiva PDD 63 – Presidential Decision Directive 63), která byla vydána v roce 1998 jako rozhodnutí tehdejšího prezidenta Billa Clintona. V této směrnici byly prvky infrastruktury rozděleny do sedmi stěžejních oblastí v USA.[6]

Nejdůležitější datum ovlivňující novodobý vývoj ochrany kritické infrastruktury bylo bezesporu 11. Září 2001. Teroristické útoky na World Trade Centre v New Yorku a Pentagon ukázaly, jak obrovské škody může napáchat poškození kritické infrastruktury města a jaký to může mít dopad na celou zemi. Na základě těchto kritických událostí se

podhled na celý problém kritické infrastruktury od základu změnil a to nejen ve Spojených státech. Před teroristickými útoky v USA byl kladen mnohem větší důraz na ochranu kybernetických systémů a také se pravděpodobnější jevilo možné ohrožením přírodními katastrofami.

Po teroristických útocích z 11. září 2001 byly Spojené státy přinuceny změnit svojí vnitřní bezpečnostní politiku. V roce 2001 je prezidentem G. W. Bushem vydáno Vládní nařízení na ochranu kritické infrastruktury. Nařízení mělo za úkol obranu a zabezpečení informačních systémů pro kritickou infrastrukturu a ochranu hmotných zařízení, které informační systémy podporují. V roce 2003 byla zveřejněna Národní strategie vnitřní bezpečnosti. A v roce 2003 byl vydán dokument Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení, který komplexně popisuje problematiku kritické infrastruktury a je zdrojem informací pro mnoho zemí i mimo USA. Bylo potřeba zřídit samostatné a nezávislé ministerstvo, které mělo za úkol starat se o vnitřní bezpečnost státu. V roce 2003 také ve Spojených státech vznikl Úřad pro národní bezpečnost (Department of Homeland Security). [3,6,9]

1.2.2 Vývoj v Evropě

Po USA si i další vyspělé země uvědomily svoji zranitelnost a možná rizika související se současnými hrozbami. Důležitost ochrany kritické infrastruktury se podstatně zvýšila na celém světě.

„Otázkami kritické infrastruktury se začala zabývat také administrativa v evropských zemích. Ve Velké Británii bylo v roce 1999 ustanoveno Koordinační centrum pro bezpečnost národní infrastruktury (National Infrastructure Security Coordination Centre), jehož úkolem bylo rozvíjet a koordinovat činnost k ochraně kritické národní infrastruktury. Byly identifikovány systémy, jejichž kontinuita byla důležitá pro fungování státu, resp., jejichž ztráta nebo narušení by vedlo nebo by mohlo vést k ohrožení životů, vážným negativním hospodářským a sociálním dopadům na společnost. V Německu byl ve stejném roce projednán materiál – Informačně technické ohrožení klíčových infrastruktur v Německu a v roce 2001 Nizozemská vláda schválila – Akční plán bezpečnosti a boje proti terorismu, který obsahoval projekt na ochranu kritické infrastruktury skládající se ze tří základních částí:

- rychlé zjištění míry kritičnosti infrastruktury,
- stimulování spolupráce veřejného a soukromého sektoru,
- analýzy rozdílu mezi přijatými a potřebnými ochrannými opatřeními.“[5]

V Evropě se problematikou kritické infrastruktury začala jako první zabývat Velká Británie. Bylo již vydáváno spousta strategických dokumentů a materiálů, ze kterých evropské země mohly čerpat. Bylo potřeba zlepšit přístup k ochraně kritické infrastruktury jak ve státním sektoru, tak i v sektoru soukromém. Postupně se touto problematikou začaly zabývat i další evropské státy jako například Německo, Francie, Nizozemí a podobně. Společným jmenovatelem problematiky ochrany kritické infrastruktury v tomto časovém období byl především vysoký důraz na ochranu informačních a komunikačních technologii, který souvisel s přechodem do nového milénia.

V každé zemi však byla problematika pojímána jiným způsobem. Bylo tedy potřebné vymezit pojem evropská kritická infrastruktura. Zůstalo však zcela v kompetenci jednotlivého členského státu Evropské unie rozhodnout se, která infrastruktura je kritická. Nejaktuálnějším dokumentem EU řešící problém ochrany kritické infrastruktury je „Směrnice rady 2008/114/ES ze dne 8. Prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu“[17]

Koncept Evropské kritické infrastruktury ECI (European Critical Infrastructure) má přímý vliv na Českou republiku, jakožto členský stát Evropské unie. Koncept zahrnuje: „Fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít závažný dopad na zdraví, bezpečnost nebo hospodářskou prosperitu obyvatelstva nebo efektivní funkci vlády dvou nebo více členských zemí“[17]

EPCIP (Europe Programme for Critical Infrastructure Protection) byl v roce 2004 schválen na jednání Evropské komise jako Program ochrany evropské kritické infrastruktury. Program má za úkol řešit ochranu Evropských kritických infrastruktur, tedy infrastruktur, jejichž vyřazení nebo poškození by mělo vliv na dva a více států Evropské unie.[1]

EPCIP také vymezuje pojem Národní kritická infrastruktura NCI (National Critical Infrastructure). Jedná se o takovou infrastrukturu, která má přímý vliv na fungování jen jednotlivého státu Evropské unie. Tímto způsobem EU vybízí jednotlivé státy k vytváření svých vlastních plánů na ochranu kritických infrastruktur. Hlavním cílem programu EPCIP je rovnoměrná úroveň ochrany kritické infrastruktury v rámci celé Evropské unie.[1,5,6]

V souvislosti se schválením programu EPCIP byla vytvořena CIWIN (European Critical Infrastructure Warning Network) – Výstražná informační síť kritické infrastruktury.[5,6]

Velice důležitým dokumentem v problematice kritické infrastruktury v rámci Evropské unie je Zelená kniha o Evropském programu na ochranu kritické infrastruktury vydaný v roce 2005. Jednotlivé kapitoly Zelené knihy pojednávají o podrobnostech programu EPCIP a EU se při tvorbě Zelené knihy obracela jak na odborníky, tak i na laickou veřejnost.[1,5]

V Evropské unii se v otázce ochrany kritických infrastruktur spoléhá především na odpovědnost jednotlivých členských států.

1.3 Novodobé vnímání pojmů kritické infrastruktury

„Kritickou infrastrukturou 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. „[4]

Škody, které v takových případech nastanou, mohou mít různé příčiny. V současnosti jsou to především teroristické útoky, tedy škody způsobené úmyslným lidským jednáním. Dále to mohou být škody způsobené neúmyslným jednáním nebo přírodní katastrofy či průmyslové havárie a další. Příčin může být opravdu mnoho, ovšem zde jsem uvedl ty nejdůležitější a nejpravděpodobnější.

Zajištění bezpečnosti měst a jejich obyvatel je jednou ze základních a prioritních úloh vlády státu. Současná otevřená společnost je vůči terorismu mnohem zranitelnější než diktátorské režimy. Důvodem je tržní konkurenční ekonomika a vysoká tolerance vůči odlišně názorově orientovaným menšinám. Tyto důvody přímo zvyšují zranitelnost státu, tedy její kritické infrastruktury. Teroristické útoky, průmyslové havárie i přírodní katastrofy mhou mít za těchto podmínek daleko ničivější dopady na celou společnost.

Abychom mohli začít řešit komparaci přístupů kritických infrastruktur v České republice a ve Velké Británii, je potřeba si uvědomit a definovat co to ve skutečnosti kritická infrastruktura je, jaké byly důvody jejího vzniku a proč je v dnešní době tak důležité se její ochranou zabývat.

Vzhledem k tomu, že Česká republika i Velká Británie jsou členské státy Evropské unie, tak budu vycházet z definice uvedené ve směrnici rady 2008/114/ES, která je publikována v Úředním věstníku Evropské unie. Definice kritické infrastruktury zní následovně:

„Prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejich narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí.“[17]

Ze stejné směrnice si uvedeme i další důležitý pojem - Evropská kritická infrastruktura. Pod tímto pojmem se rozumí:

„Kritická infrastruktura nacházející se v členských státech, jejíž narušení nebo zničení by mělo závažný dopad pro nejméně dva členské státy. Závažnost dopadu se posuzuje podle průřezových kritérií. To se vztahuje i na účinky způsobená meziodvětvovými závislostmi na jiných typech infrastruktury.“[17]

V další kapitole se zaměřím na vývoj kritické infrastruktury v České republice a následně zákonným usměrněním této problematiky.

2 SOUČASNÝ STAV KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE

V této kapitole se budu věnovat problematice kritické infrastruktury v České republice a to konkrétně jejímu novodobému vývoji, oblastem kritické infrastruktury a také legislativním usměrněním kritické infrastruktury v ČR.

2.1 Novodobý vývoj kritické infrastruktury v České republice

Pojem kritická infrastruktura je samozřejmě dnes již v České republice dobře známy, ovšem spíše mezi odbornou veřejností. Nejdříve se kritickou infrastrukturou zabývaly Spojené státy a Austrálie, zanedlouho na to se začalo o kritické infrastruktuře diskutovat i v Evropě. Prvními evropskými státy, které se problematikou kritické infrastruktury zabývaly, byly Velká Británie a Německo. Později se samozřejmě o tuto problematiku zajímaly i další evropské státy, jako například Francie a Nizozemí. Kritická infrastruktura se samozřejmě dříve nebo později musela začít řešit i v České republice.

Vytváření a následné realizace bezpečnostní politiky začaly v České republice až po roce 1989. Dnes se jedná o pojem kritická infrastruktura a tehdy ještě tento pojem nebyl zaveden. V tehdejším Československu fungoval do roku 1989 tzv. systém zvyšování odolnosti národního hospodářství, který byl zaměřen na přípravu činnosti za války. Struktura tohoto systému se časem měnila. „V 90. letech 20. století se projevilo snížení důrazu na ochranu a obranu lidí a došlo ke zrušení jednotek civilní obrany (CO) v bydlištích a na pracovištích, zastavilo se provádění branné výchovy obyvatelstva a omezovaly se další činnosti související s přípravou na válku. Velkým pokrokem v této oblasti bylo přijeti tzv. krizových zákonů v roce 2000, což mimo jiné vedlo k budování integrovaného záchranného systému ČR (IZS ČR). Problematika ochrany obyvatelstva začala byt začleňována do mezinárodních struktur, a to jak do NATO, tak i do EU.“[5]

V Evropě byly jedním z hlavních impulsů pro bližší pohled na problematiku kritické infrastruktury zejména atentáty na dopravní infrastrukturu v Madridu 11. března 2004 a v Londýně 7. července 2005.

V České republice se počáteční činnosti v rámci ochrany kritické infrastruktury zaměřovaly především na ochranu počítačových sítí. A proto byl Úřadem pro veřejné informační systémy vypracován projekt Strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě.

Mezi dva důležité pracovní a poradní orgány vlády pro problematiku kritické infrastruktury můžeme zařadit Výbor pro civilní nouzové plánování (VCNP) a Bezpečnostní radu státu (BRS). Výbor pro civilní nouzové plánování spadá pod Bezpečnostní radu státu a je jedním z jejich pracovních výborů.[4]

„Bezpečnostní rada státu je stálým pracovním orgánem vlády pro koordinaci problematiky bezpečnosti České republiky a přípravu návrhů opatření k jejímu zajišťování“.[4]

V letech 1997 a 1998 zasáhly Českou republiku povodně. Na základě těchto událostí se později prováděly analýzy, které měly přispět k ochraně kritické infrastruktury. Prováděly se analýzy odezvy na povodně a také analýzy zahraničních dokumentů a materiálů týkajících se živelných pohrom. To dále vedlo ke zpracování materiálů týkajících se ochrany kritické infrastruktury.

V roce 2001 Bezpečnostní rada státu a Výbor pro civilní nouzové plánování projednali usnesení pod názvem Definice a rozsah základních funkcí státu. Toto usnesení bylo důležité v tom, že se jako první oficiální vládní spis zabýval základními funkcemi státu v případě vzniku mimořádné události (MU) nebo krizové situace (KS) nevojenského charakteru.

Výbor pro civilní nouzové plánování v roce 2002 projednával usnesení Rozsah základních funkcí státu za krizových situací a dokument Zprava o národní kritické infrastruktuře, kde se stanovilo zaměření národní kritické infrastruktury na tyto oblasti:

- systém dodavky energii (především elektřiny),
- systém dodavky vody,
- systém odpadového hospodářství,
- přepravní síť,
- komunikační a informační systémy,
- bankovní a finanční sektor,
- nouzové služby (policie, hasičské záchranné sbory, zdravotnictví),
- veřejně služby (zásobovaní potravinami, sociální služby, pohřební služby),
- statni správa a samospráva.[5]

Národní kritickou infrastrukturou České republiky rozumíme systém tvořený dvěma úrovněmi:

- úrovní sektorů (oblastí),
- úrovní produktů a služeb.[5]

Prvky kritické infrastruktury na úrovni sektorů jsou také občas označovány jako oblasti nebo odvětví kritické infrastruktury a na úrovni produktů jako segmenty kritické infrastruktury.

Po vstupu České republiky do Evropské unie v roce 2004 se samozřejmě změnilo postavení a bezpečnost republiky. Významnou změnou byl již vstup ČR do NATO v roce 1999. Česká republika po vstupu do mezinárodních organizací EU a NATO reagovala zpracovaným materiálem k problematice kritické infrastruktury. Tímto materiálem byl dokument pod názvem „Zpráva o stavu řešení kritické infrastruktury v České republice“, který vypracoval Výbor pro civilní nouzové plánování. K tomuto materiálu bylo přijato usnesení, ve kterém se porovnávaly kroky České republiky a zahraničních států v oblasti ochrany kritické infrastruktury.

Dalším krokem v problematice kritické infrastruktury v ČR bylo vypracování a projednávání dokumentu Zprava o řešení problematiky kritické infrastruktury v České republice, projednané Výborem pro civilní nouzové plánování. Vláda schválila svým usnesením v roce 2007 Směrnici k výběru objektů obranné infrastruktury a zpracování dokumentace. Problematika obranné a kritické infrastruktury se často překrývají, proto směrnice s problematikou kritické infrastruktury souvisí.

Zpráva o stavu řešení kritické infrastruktury v ČR se stala prvotním impulsem pro zpracování Komplexní strategie a následně Národního programu. Součástí této zprávy byla také podrobná analytická část zabývající se situací v jednotlivých oblastech kritické infrastruktury.

Vláda České republiky vydala svým usnesením v roce 2008 Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie ČR k řešení problematiky kritické infrastruktury a Národní programu ochrany kritické infrastruktury. Podle Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020, schválené v roce 2008 by Komplexní strategie České republiky k řešení problematiky ochrany kritické infrastruktury měla představovat dohodnutý a projednaný rámec pro tvorbu dalších koncepčních materiálů, které by ji rozvrhly do konkrétních kroků a následných opatření.

2.2 Oblasti kritické infrastruktury v České republice

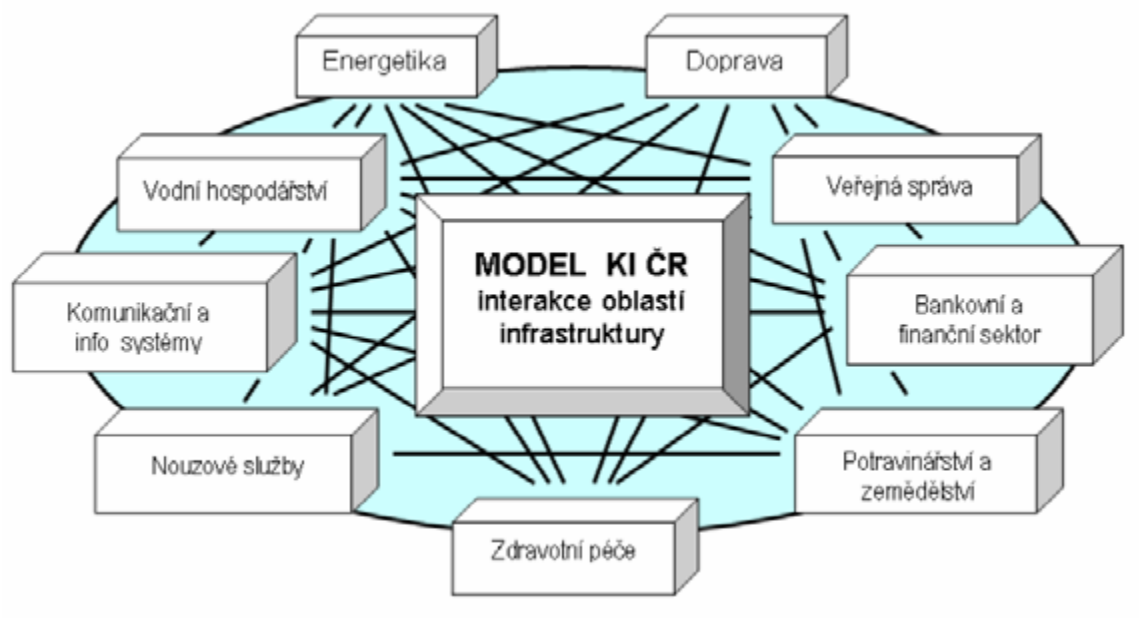
V současné době je v České republice vymezeno devět oblastí a třicet sedm produktů a služeb, které jsou z hlediska fungovaní společnosti považovány za prioritní, viz tabulka 1. Tyto oblasti byly zpracovány a projednány v dokumentu Zprava o řešení problematiky kritické infrastruktury. V dokumentu se upravily dosavadní oblasti, pro příklad se vypustila oblast 10, kterou bylo odpadové hospodářství. Tento návrh dokumentu byl projednán členy Výboru pro civilní a nouzové plánování dne 12. června 2007 a schválen.

Tabulka 1: *Oblasti národní kritické infrastruktury schválené v roce 2007*[9]

P. č.	Oblast KI	Produkt nebo služba
1.	Energetika	1.1. Elektřina 1.2. Plyn 1.3. Tepelná energie 1.4. Ropa a ropné produkty
2.	Vodní hospodářství	2.1. Zásobování pitnou a užitkovou vodou 2.2. Zabezpečení a správa povrchových vod z podzemních zdrojů vody 2.3. Systém odpadních vod
3.	Potravinářství a zemědělství	3.1. Produkce potravin 3.2. Péče o potraviny 3.3. Zemědělská výroba
4.	Zdravotnická péče	4.1. Přednemocniční neodkladná péče 4.2. Nemocniční péče 4.3. Ochrana veřejného zdraví 4.4. Výroba, skladování a distribuce léčiv a zdravotnických prostředků
5.	Doprava	5.1. Silniční 5.2. Železniční 5.3. Letecká 5.4. Vnitrozemská vodní
6.	Komunikační a informační	6.1. Služby pevných telekomunikačních sítí 6.2. Služby mobilních telekomunikačních sítí

	systémy	6.3. Radiová komunikace a navigace 6.4. Satelitní komunikace 6.5. Televizní a radiové vysílání 6.6. Poštovní a kurýrní služby 6.7. Přístup k internetu a datovým službám
7.	Bankovní a finanční systém	7.1. Správa veřejných financí 7.2. Bankovnictví 7.3. Pojišťovnictví 7.4. Kapitálový trh
8.	Nouzové služby	8.1. Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany 8.2. Policie ČR (vnitřní bezpečnost a veřejný pořádek) 8.3. Armáda ČR (zabezpečení obrany) 8.4. Radiační monitorování včetně podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření 8.5. Předpovědní, varovná a hlásná služba
9.	Veřejná správa	9.1. Státní správa a samospráva, 9.2. Sociální ochrana a zaměstnanost (soc. zabezpečení, stát., soc. podpora, soc. pomoc). 9.3. Výkon justice a vězeňství

Samozřejmě jednotlivé oblasti kritické infrastruktury jsou navzájem propojeny a jsou závislé na jiných oblastech. Například komunikační a informační systémy jsou zcela závislé na energetice nebo nouzové služby jsou závislé na dopravě a podobně. Schéma vzájemného působení jednotlivých oblastí kritické infrastruktury můžeme vidět na obrázku 1.



Obrázek 1: *Schéma interakcí oblastí KI v ČR definovaných podle stavu v roce 2007*[10]

2.3 Legislativní usměrnění kritické infrastruktury v České republice

Kritická infrastruktura je v České republice definována v novele krizového zákona 240/2000 Sb. Tato novela nese označení 118/2011 Sb. úplné znění zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Při vymezováni oblasti kritické infrastruktury a následně produktů a služeb je možné postupovat tak, že nejprve dojde k vymezení souhrnu ucelených oblasti infrastruktury, které jsou považovány za kritické (např. energetika, doprava). Při vymezovaní se řídí definici KI, kterou navrhl Výbor pro civilní nouzové plánování, a schválila Bezpečnostní rada státu. V České republice existuje řada zákonů a vyhlášek přímo či nepřímo upravující problematiku kritické infrastruktury.

Shrnutí legislativních kroku v ČR:

- Květen 2003 – BRS (Bezpečnostní rada státu) vytvořila seznam subjektů KI
- Březen 2007 – odborná pracovní skupina VCNP (Výbor pro civilní a nouzové plánování) sjednotila termín „KI“, návrh oblastí KI
- Červenec 2007 – BRS schválila oblasti KI
- Únor 2007 – předložen harmonogram dalšího postupu zpracování

Komplexní strategie ČR k řešení problematiky KI a Národního programu na ochrany KI

- 25. února 2008 dokument zpracován schválen usnesením vlády ČR
- Národní program (červen 2009)[31]

2.3.1 Významné zákony a nařízení upravující problematiku kritické infrastruktury v ČR

118/1998 Sb. Zákon o bezpečnosti České republiky ze dne 22. dubna 1998.

Jedná se o ústavní zákon, který upravuje zajištění bezpečnosti České republiky prostřednictvím regulace nouzového stavu a stavu ohrožení státu. Dále také zřizuje bezpečnostní radu státu.

240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonu (krizový zákon) ze dne 28. června 2000.

„Tento zákon stanoví působnost a pravomoc státních orgánu a orgánu územních samosprávných celku a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností.“[12]

462/2000 Sb. Nařízení vlády k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonu (krizový zákon) ze dne 22. listopadu 2000.

Toto nařízení vlády je pro řešení problematiky ochrany kritické infrastruktury velice důležité, protože řeší náležitosti a obsah plánu krizové připravenosti.

430/2010 Sb. Zákon, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů ze dne 21. prosince 2010.

431/2010 Sb. Nařízení vlády, kterým se mění nařízení vlády č. 462/2000 Sb. k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění nařízení vlády č. 36/2003 Sb. ze dne 22. prosince 2010.

432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury ze dne 22. prosince 2010.

Směrnice rady **2008/114/ES** o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ze dne 8. prosince 2008.

„Tato směrnice představuje první etapu přístupu krok za krokem, jehož cílem je určit a označit Evropské kritické infrastruktury a posoudit potřebu zvýšit jejich ochranu. Směrnice se proto soustředí na odvětví energetiky a dopravy a měla by být přezkoumána s ohledem na posouzení jejího dopadu a nutnost zahrnout do její oblasti působnosti další odvětví, mimo jiné odvětví informačních a komunikačních technologií.“[17]

118/2011 Sb. Předseda vlády vyhlašuje úplné znění zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), jak vyplývá ze změn provedených zákonem č. 320/2002 Sb., zákonem č. 127/2005 Sb., zákonem č. 112/2006 Sb., zákonem č. 267/2006 Sb., zákonem č. 110/2007 Sb., zákonem č. 306/2008 Sb., zákonem č. 153/2010 Sb. a zákonem č. 430/2010 Sb. ze dne 1. ledna 2011.

V následující kapitole se zaměřím na analýzu současného stavu problematiky kritické infrastruktury ve Velké Británii.

3 SOUČASNÝ STAV KRITICKÉ INFRASTRUKTURY VE VELKÉ BRITÁNII

3.1 Základní informace o Velké Británii

Spojené království Velké Británie a Severního Irska (označované někdy jako Velká Británie, Británie, Spojené království nebo Anglie) je ostrovní stát přiléhající k severozápadu kontinentální Evropy. Zahrnuje ostrov Velkou Británii a severovýchodní část ostrova Irsko, kde hraničí s Irskou republikou. Na samotném ostrově se rozkládají tři země – Anglie, Wales a Skotsko. Anglie je největší a nejlidnatější země Spojeného království Velké Británie a Severního Irska. Velká Británie je největším ostrovem celé Evropy a zároveň je osmým největším ostrovem na světě.

Spojené království je ohraničeno Atlantským oceánem, respektive jeho lokálními částmi, tedy Severním mořem, Lamanšským průlivem, Keltským mořem, Průlivem svatého Jiří a Irským mořem. S kontinentální Evropou je Velká Británie spojena Eurotunelem.

Politický systém Spojeného království Velké Británie a Severního Irska je zasazen v rámci konstituční monarchie, která je složena ze čtyř zemí: Anglie, Skotska, Walesu a Severního Irska. Současnou hlavou státu je královna Alžběta II., která je zároveň hlavou dalších třinácti států Commonwealthu (Společenství národů), například Kanady, Austrálie, Nového Zélandu a Jamajky, takzvanými britskými korunními závislými územími jsou Ostrov Man a Normanské ostrovy. Jako takové jsou vlastnictvím Britské koruny, nejsou součástí Spojeného království, jsou s ním pouze spojeny federací známou jako Britské ostrovy. Pod suverenitu Spojeného království Velké Británie a Severního Irska spadá též čtrnáct takzvaných zámořských území, které jsou pozůstatky bývalé Britské říše. Hlavou vlády ve Spojeném království je premiér. Současným premiérem je David Cameron, který zastává svůj úřad od roku 2010.

Výkonná moc je realizována vládou Spojeného království a část pravomocí je přenesena na vlády Skotska, vládní úřady ve Walesu a Severním Irsku. Zákonodárná moc je nezadatelným právem vlády a dvou komor parlamentu – Sněmovny lordů a Dolní sněmovny, stejně tak i Skotského parlamentu a zastupitelstev Walesu a Severního Irska. Soudní moc je nezávislá na moci výkonné i na moci zákonodárné (několik vyšších soudců

je členy Sněmovny lordů, ale soudní moc této sněmovny je od roku 2009 na základě reformy z roku 2005 zrušena).

Ačkoliv bylo Spojené království ještě v devatenáctém století nejsilnější velmocí, obě světové války a zejména potom rozpad koloniální říše v druhé polovině dvacátého století jeho moc hodně oslabily. Přesto je stálým členem Rady bezpečnosti Organizace spojených národů (OSN), jadernou velmocí i členem skupiny G8. G8 (Group of Eight) je mezinárodní sdružení osmi nejvyspělejších států světa.

Spojené království se může pyšnit pátou největší ekonomikou na světě s druhými nejvyššími výdaji na obranu. Je tak důležitou politickou, ekonomickou i vojenskou silou. Dále je jedním ze zakládajících členů NATO. Spojené království Velké Británie a Severního Irska je stejně jako Česká republika členským státem Evropské unie. Na rozdíl od České republiky, která je součástí Evropské unie teprve od roku 2004, je Velká Británie členským státem Evropské unie již od roku 1973. Spojené království je také členem Rady Evropy a vůdčí zemí Britského společenství národů.

3.2 Vývoj kritické infrastruktury ve Velké Británii

Důležitým dnem pro vývoj kritické infrastruktury v Evropě a především ve Velké Británii byly teroristické útoky v Madridu v roce 2004. Jednalo se o sérii koordinovaných bombových útoků proti vlakovému systému v Madridu ve Španělsku. O rok později se stejné smutné události odehrály i ve Velké Británii. Dne 7. července roku 2005 došlo v Londýně k sérii teroristických bombových útoků, které si vyžádaly přes 50 obětí na životech a kolem 700 stovek zraněných lidí. Útoky byly vedeny formou sebevražedných teroristických útoků, které byly provedeny v londýnských dopravních prostředcích během ranní dopravní špičky. K výbuchům došlo v samotném centru metropole. Tři z nastražených bomb explodovaly v londýnských soupravách metra a jedna bomba byla odpálena v patrovém autobuse. Spojené království samozřejmě tyto okolnosti velice zasáhly a vyvolaly pozdější aktivitu na zvyšování ochrany kritické infrastruktury.

Národní kritická infrastruktura (CNI) ve Spojeném království zahrnuje klíčové prvky národní infrastruktury, které jsou naprosto nezbytné pro zabezpečení základních služeb ve Velké Británii. Bez těchto klíčových prvků by Velká Británie mohla utrpět vážné následky, jako jsou závažné hospodářské škody, hluboké sociální narušení, nebo dokonce ve velkém

měřítku ztráty na životech. Mnoho kritických služeb, které jsou naprosto zásadní pro fungování Spojeného království, z velké míry závisí na informačních technologiích. Jsou zajišťovány jak státním tak i soukromým sektorem.[26]

Ve Velké Británii spadá zodpovědnost za ochranu kritické infrastruktury do kompetencí Ministerstva vnitra. Ministerstvo vnitra hraje v této problematice ve Velké Británii hlavni roli, ale zdaleka ne jedinou. Řada dalších úřadů hraje významnou roli při ochraně národní kritické infrastruktury ve Velké Británii. Do roku 2006 byly za ochranu národní kritické infrastruktury proti elektronickému útoku ve Velké Británii zodpovědné dva úřady. Bezpečnostní koordinační centrum národní infrastruktury (National Infrastructure Security Co-ordination Centre - NISCC) a Rada národního bezpečnostního centra (National security Advice Centre - NSAC). Od roku 2007 jsou tyto dva úřady nahrazeny Centrem pro ochranu národní kritické infrastruktury (Centre for Protection of National Infrastructure - CPNI). Zodpovědnost za zabezpečení národní kritické infrastruktury je ve Velké Británii rozdělena právě mezi Centrum pro ochranu národní kritické infrastruktury, policii a bezpečnostní služby.[5,26]

V oblasti ochrany národní kritické infrastruktury je ve Velké Británii široce rozvinutá spolupráce mezi veřejným a soukromým sektorem. Vláda úzce spolupracuje s mnoha soukromými subjekty a Centrum pro ochranu národní kritické infrastruktury sdílí důležité informace s vlastníky národních kritických infrastruktur. Cílem této spolupráce je vytvořit mechanismus, z něhož pomocí by se mohla řada společností poučit z chyb, úspěchů a zkušeností jiných. Mezi nejvýznamnější soukromé instituce patří například Britská počítačová společnost (British Computer Society), Národní počítačové centrum (National Computing Centre) a Fórum pro bezpečný internet (Internet Security Forum).[5,26]

3.3 Oblasti kritické infrastruktury ve Velké Británii

Ve Velké Británii je stejně, jako v České republice je definováno devět oblastí národní kritické infrastruktury, viz tabulka 2. Těchto devět sektorů kritické infrastruktury bylo schváleno v roce 2010 v národním plánu na ochranu kritické infrastruktury Velké Británie. Je to Program odolnosti kritické infrastruktury (Sector Resilience Plan for Critical infrastructure). Avšak produktů a služeb je v porovnání s Českou republikou uvedených

daleko méně. Neznamená to však, že by Velká Británie měla těchto kriticky chráněných produktů a služeb méně, jen jsou obecněji rozepsané.

Tabulka 2: *Oblasti národní KI ve Velké Británii schválené v roce 2010*[23]

P. č.	Sektor KI	Produkt nebo služba
1.	Pohotovostní služby	1.1. Policie 1.2. Hasiči 1.3. Ambulance 1.4. Pobřežní police
2.	Vláda	2.1. Vláda
3.	Komunikace	3.1. Telekomunikace 3.2. Pošta 3.3. Vysílání
4.	Zdravotnictví	4.1. Zdravotnické služby
5.	Voda	5.1. Voda
6.	Energie	6.1. Ropa 6.2. Plyn 6.3. Elektřina
7.	Finanční služby	7.1. Finančnictví
8.	Potraviny	8.1. Potraviny
9.	Doprava	9.1. Silniční 9.2. Železniční 9.3. Vodní 9.4. Letecká

3.4 Legislativní usměrnění kritické infrastruktury ve Velké Británii

Hlavní roli v tvorbě a upravování zákonů souvisejících s ochranou kritické infrastruktury má Ministerstvo vnitra (Home Office) Velké Británie. To, že kritická infrastruktura není přímo ukotvena v zákoně, ale je zmíněna v různých souvisejících právních předpisech a ustanoveních, které se týkají přímo oblastí kritické infrastruktury, jako je energetika,

komunikace nebo záchranné systémy, není nic neobvyklého. Takto je to upravováno ve většině zemí s tím, že kritická infrastruktura je ukotvena pomocí národních plánů na její vytyčení a ochranu. Ve Velké Británii je to již zmíněný Program odolnosti kritické infrastruktury a například v Německu je tímto dokumentem Prováděcí plán na ochranu kritické infrastruktury (CIP Implementation Plan). Stejně tak je to například také ve Spojených státech, kde je několik dokumentů a směrnic upravujících kritickou infrastrukturu.[5]

Velká Británie vytvořila právní rámec pro ochranu informačních systémů. Obsahuje řadu právních předpisů, které jsou dále uvedeny:

- Telekomunikační zákon z roku 1997: Tento zákon upravuje Telekomunikační zákon z roku 1984 a především přijímá další opatření v boji proti podvodům v souvislosti s použitím telekomunikačního systému.

- Zákon o ochraně dat z roku 1998: Tento zákon upravuje zpracování informací týkající se fyzických osob, včetně získávání, držení, použití nebo vyzrazení těchto informací.

- Elektronický komunikační účet z roku 2000: Účet obsahuje ustanovení k usnadnění používání elektronické komunikace a elektronického ukládání dat.

- Teroristický zákon z roku 2000: Tento zákon se týká terorismu. Obsahuje dočasná ustanovení pro Severní Irsko o stíhání a trestání některých trestných činů souvisejících s terorismem. Ustanovuje také záměrné poškození nebo zneužití elektronických systémů jako závažný trestný čin.

- Policejní a justiční zákon z roku 2006: Tento zákon obsahuje ustanovení pro řadu položek týkající se policejní činnosti, trestné činnosti, a veřejného nepořádku. Mění také Zákon o počítačovém zneužití z roku 1990.[26]

Velká Británie je stejně jako Česká republika členskou zemí Evropské unie a proto je pro ni také velice důležitá směrnice Evropské rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

Důležité je také, že velká Británie vychází z dokumentů jako je Zelená kniha o Evropském programu na ochranu kritické infrastruktury, kde jednotlivé kapitoly pojednávají o účelu a oblastech působnosti evropského programu EPCIP. Evropská komise stanovuje zásady a nástroje potřebné pro provádění Evropského programu na ochranu kritické infrastruktury (EPCIP), který se zaměřuje na evropskou infrastrukturu i infrastrukturu jednotlivých států.

4 BEZPEČNOSTNÍ HROZBY SOUČASNÉHO SVĚTA

V následující kapitole se budu věnovat problematice bezpečnostních hrozeb současného světa. Půjde především o hrozby, které mohou přímo ohrožovat Českou republiku a její kritickou infrastrukturu, nebo další členské země Evropské unie, jako například Velkou Británii. Mohou však stejně ohrožovat i jiné země nejen v Evropě, ale na celém světě. Na základě bezpečnostních analýz a geografického prostředí České republiky lze identifikovat pro ČR specifické hrozby a určit, které jsou reálnější a které naopak jsou méně pravděpodobné. V podstatě každá země na základě bezpečnostních analýz identifikuje specifické hrozby pro danou oblast.

ČR jako zodpovědný člen mezinárodních organizací a uskupení zahrnuje mezi bezpečnostní hrozby i ty, které nemají přímý dopad na její bezpečnost, ale ohrožují její spojence, například další členské státy Evropské unie.

4.1 Vymezení základních pojmů

Hrozba

„Hrozba je primární, mimo nás nezávisle existující, neodvozená. Je to vnější fenomén, který může nebo chce poškodit nějakou konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a tomu, jak si danou hodnotu ceníme. Odpověďmi na hrozby jsou opatření, která je eliminují a nastolují tak pocit bezpečí.“ [6]

Vztah pro určení hrozby:

Hrozba = schopnost útočníka x zranitelnost x úmysl [6]

Riziko

„Míra pravděpodobnosti a tvrdosti nepříznivých vlivů na lidský život, zdraví, majetek nebo životní prostředí. Kvantitativně vyjádřeno jako: riziko = ohrožení možnou ztrátou. Riziko může být též vyjádřeno jako pravděpodobnost nepříznivé události a jejích následků, pokud k ní dojde.“ [6]

Vztah pro určení rizika:

Riziko = ohrožení x zranitelnost [6]

4.2 Bezpečnostní hrozby

Protikladem k pojmům hrozba a riziko je bezesporu pojem bezpečnost, respektive je často s těmito pojmy spojována. Pro bezpečnost je důležité si jednotlivé hrozby podrobněji popsat. V této části mé diplomové práce právě jednotlivé hrozby současného světa stručně popíšu.

4.2.1 Terorismus

Hrozba terorismu jako metody násilného prosazování politických cílů či jiných záměrů je trvale velmi vysoká. Charakteristickým rysem terorismu je existence nadnárodních sítí volně propojených skupin, které i bez jednotného velení sdílejí určitou ideologii, cíle a plány k jejich naplnění, finanční zdroje a informace. Tyto teroristické skupiny jsou schopny přímo ohrozit lidské životy a zdraví, ale také kritickou infrastrukturu země. Hrozba terorismu je vnímána zvláště po teroristických útocích v USA i Evropě velmi vážně.[1,27]

4.2.2 Šíření zbraní hromadného ničení a jejich nosičů

Některé státní i nestátní uskupení či jednotlivci usilují otevřeně nebo skrytě o získání zbraní hromadného ničení a jejich nosičů. Šíření těchto prostředků může mít závažné bezpečnostní důsledky kdekoliv na světě. Specifickou hrozbu pak představuje případné použití balistických řízených střel a střel s plochou dráhou letu nesoucích konvenční nebo nekonvenční nálož. Schopnost těchto řízených střel zasáhnout z velké vzdálenosti území České republiky nebo jejích spojenců klade značně vysoké nároky na aktivní i pasivní protiopatření.[1,6,27]

4.2.3 Kybernetické útoky

„Rostoucí závislost na informačních a komunikačních technologiích zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům. Tyto útoky mohou představovat nový způsob vedení války nebo mohou mít kriminální či teroristickou motivaci a mohou být použity k destabilizaci společnosti. Úniky strategicky důležitých informací, zásahy do

informačních systémů státních institucí či strategických podniků a společností, které zajišťují základní funkce státu, mohou ohrozit strategické zájmy ČR.“[27]

4.2.4 Nestabilita a regionální konflikty

„Nevyřešené konflikty se všemi negativními důsledky mohou mít přímý i nepřímý vliv na bezpečnost ČR. Neřešené spory etnického, teritoriálního nebo politického a ekonomického charakteru mají potenciál vyústit do ozbrojených konfliktů či svádět některé státy k budování sfér vlivu a zároveň oslabovat mechanismy kooperativní bezpečnosti i politické a právní závazky v oblasti evropské bezpečnosti.“[27]

4.2.5 Negativní aspekty mezinárodní migrace

Negativním jevem je především nelegální migrace a její možné dopady, například napojení na organizovaný zločin. Pozitivní přínosy legální migrace pro kulturní, politický a ekonomický rozvoj společnosti může zeslabit nedostatečná integrace přistěhovalců. Nedostatečná integrace imigrantů může být zdrojem sociálního napětí, které může směřovat například v nežádoucí radikalizaci členů přistěhovaleckých komunit.[1,6,27]

4.2.6 Organizovaný zločin a korupce

„Širší rozměr získává v současném bezpečnostním prostředí organizovaný zločin, který prostřednictvím obchodních i osobních vztahů překračuje hranice států. Narůstá schopnost kriminálních sítí narušovat instituce a hodnoty právního státu, infiltrovat orgány státní správy a ohrožovat bezpečnost občanů. Často se tak děje prostřednictvím korupce. Organizovaný zločin společně s korupčními praktikami může nabýt podoby vlivových, klientelistických, nebo korupčních sítí a vést k podkopání samotných základů společnosti. Výsledkem může být ztráta důvěry občana v poctivost a nestrannost fungování veřejných institucí, pokřivení tržních vazeb, ekonomický úpadek a destabilizace státu. Nejasná hranice mezi politickou a kriminální motivací živenou korupcí navíc často vede k propojování struktur organizovaného zločinu s teroristickými sítěmi.“[27]

4.2.7 Ohrožení funkčnosti kritické infrastruktury

S ohledem na vysoký stupeň vzájemného propojení jednotlivých oblastí je kritická infrastruktura ohrožena komplexně. Kritická infrastruktura je ohrožena přírodními, technologickými a jinými hrozbami. Především funkčnost energetické infrastruktury je ohrožována jak politickými tlaky, tak hrozbami kriminálního charakteru. Příkladem takových ohrožení jsou politicky motivované manipulace s dodávkami strategických surovin nebo vstup cizího kapitálu s rizikovým původem a cíli do kritické infrastruktury České republiky, sabotáže či hospodářská kriminalita.[1,27]

4.2.8 Přerušení dodávek strategických surovin nebo energie

„V rychle se měnícím globálním světě získávají otázky zajištění energetické a surovinové bezpečnosti stále větší význam. Soutěžení o přístup ke zdrojům strategických, zejména energetických surovin, se stává nedílnou součástí mezinárodních vztahů. Prioritou je vytvářet předpoklady pro nepřerušované diverzifikované dodávky strategických surovin a v domácím prostředí pak předpoklady pro stabilní dodávky elektrické energie a pro tvorbu strategických rezerv státu. Rostoucí důležitost má i oblast potravinové bezpečnosti a zajištění přístupu ke zdrojům pitné vody.“[27]

4.2.9 Pohromy přírodního a antropogenního původu a jiné mimořádné události

Extrémní projevy počasí a pohromy přírodního a antropogenního původu ohrožují nejen bezpečnost, životy a zdraví obyvatel a jejich majetku, ale mohou mít také vážný dopad na ekonomiku země, zásobování základními surovinami, pitnou vodou či poškození kritické infrastruktury. V případě rozšíření nemocí s pandemickým potenciálem se zvyšuje zranitelnost populace a jsou poté kladeny mnohem větší nároky na ochranu veřejného zdraví a zajištění základní zdravotní péče.[1,27]

Než přejdu k praktické části tak bych bylo vhodné si shrnout základní informace a poznatky. V této teoretické části jsem se zabýval vývojem a problematikou kritické infrastruktury jak v České republice, tak ve Velké Británii. Nastínil jsem i vývoj kritické infrastruktury v USA a v Evropě popsal současné bezpečnostní hrozby. Pojednal jsem také o legislativě této problematiky, kde je nejvýznamnějším dokumentem vzpomínaná

směrnice Evropské rady 2008/114/ES. Pro Evropskou unii je také velice důležitý program EPCIP, který je také v teoretické části vysvětlen. Důležité v této části byla také analýza oblastí kritické infrastruktury v České republice a ve Velké Británii, na tyto informace budou navazovat další kapitoly. V následující praktické části se budu podrobněji věnovat problematice ochrany kritické infrastruktury v České republice ve velké Británii a následným srovnáním.

II. PRAKTICKÁ ČÁST

5 ÚVOD DO PROBLEMATIKY OCHRANY KRITICKÉ INFRASTRUKTURY

V této kapitole mojí diplomové práce se zaměřím na problematiku ochrany kritické infrastruktury v České republice. Doposud jsem se zabýval spíše tím, co to kritická infrastruktura je, jejím vývojem, historií v České republice a Velké Británii a možnými současnými hrozbami. Následující část mé práce bude řešit již problematiku ochrany kritické infrastruktury, která navazuje na předchozí kapitoly práce.

5.1 Důvody ochrany kritické infrastruktury

Jak jsem již zmínil v této práci, tak infrastruktury strategického významu, tedy kritické infrastruktury jsou pro správné fungování a bezproblémový chod společnosti v dnešní době naprosto nezbytné. Ovšem to se netýká jenom jejich existence, ale je především potřeby zajistit jejich bezchybný provoz. K tomu, aby provoz kritických infrastruktur v jednotlivých oblastech probíhal v souladu s danými požadavky společnosti, je prováděna v těchto systémech pravidelná kontrolní činnost.

Velice důležitým předpokladem pro správné fungování provozu infrastruktury je také její odpovídající zabezpečení. Tento proces se nazývá ochrana kritické infrastruktury. Každá infrastruktura je ve své podstatě do jisté míry vždy vystavena určitým hrozbám, které jsou pro různé oblasti či infrastruktury specifické. Ovšem nesmíme zapomínat na to, že z každé hrozby nám také vyplývá jisté riziko.

Zabezpečit životně důležité prvky kritické infrastruktury je rozhodně jedním z nejdůležitějších úkolů společnosti a je potřeba se tím vážně zabývat. Cílem ochrany kritických infrastruktur by mělo být zajištění fungování prvků kritické infrastruktury za běžných podmínek i v případě mimořádných událostí.

Kritická infrastruktura je tvořena jednotlivými objekty KI, které jsou rozdělené do oblastí. Oblasti kritické infrastruktury jsou v každém zemi jiné a jsou rozděleny podle platné legislativy v daném státě. Již jsem se věnoval oblastem kritické infrastruktury v České republice a ve Velké Británii.

Jak již bylo v této práci uvedeno, úkolem společnosti je zabezpečit a chránit kritické infrastruktury. Ochrana kritické infrastruktury by měla být prováděna tak, aby fungovala za jakékoliv situace i v kritických situacích a mimořádných událostech.

5.2 Princip ochrany kritické infrastruktury

Základními principy ochrany kritické infrastruktury je snížení zranitelnosti prvku kritické infrastruktury nebo zvýšení odolnosti proti negativním dopadům mimořádných událostí. V ideálním případě je to kombinace jak snížení zranitelnosti, tak i zvýšení odolnosti prvků kritické infrastruktury. Pro tyto případy je velice důležité mít v záloze připravená opatření na zmírnění nebo případně odstranění škod, ale také mít připravena preventivní opatření.

„Smyslem ochrany KI musí být minimalizace dopadů její destrukce tak, aby narušení funkcí, činností nebo služeb bylo krátkodobé, málo četné, zvladatelné, nebo provizorním způsobem a územně omezené tak, aby postihlo co nejmenší počet obyvatelstva. V důsledku existence mezinárodní závislosti a provázání jednotlivých oblastí KI je nutné zabezpečit narušení oblasti, která má vliv na další oblasti a může tak mít i mezinárodní dopady. Jako příklad lze uvést narušení dodávek elektřiny, plynu, pohonných hmot nebo výpadky telekomunikačních sítí. Proto ochrana KI vyžaduje sdílení odpovědností veřejné správy s privátním sektorem a výměnu informací mezi veřejnou správou a dalšími relevantními organizacemi a také mezinárodní spolupráci.“[32]

Ochranou kritické infrastruktury (CIP) se rozumí proces, který při zohlednění všech rizik a hrozeb směřuje k zabezpečení fungovaní subjektů kritické infrastruktury a vazeb mezi nimi.

5.3 Úrovně ochrany kritické infrastruktury

Máme v podstatě tři úrovně kritické infrastruktury. Lze si to představit jako pyramidu, kde soukromý sektory by představoval spodní největší část pyramidy, tvořící základ přes národní KI až evropskou kritickou infrastrukturu.

5.3.1 Kritická infrastruktura na úrovni EU (ECI)

Nejvyšší úrovní pro Českou republiku představuje kritická infrastruktura na úrovni EU (ECI – European Critical Infrastructure).

Česká republika je členem Evropské unie a spadá tedy do Evropského programu na ochranu kritické infrastruktury (EPCIP). Tento program definuje tzv. evropskou kritickou infrastrukturu. Evropské kritické infrastruktury jsou takové prvky kritické infrastruktury, které zásadně důležité pro Evropskou unii, a které by v případě jejich narušení nebo zničení postihly dva a více členských států. Narušení nebo zničení takovéto infrastruktury s sebou nese přeshraniční dopady, které vyplývají ze vzájemných závislostí mezi propojenými infrastrukturami napříč všemi různými odvětvími.[1,3]

5.3.2 Národní kritická infrastruktura (NCI)

Národní kritická infrastruktura (NCI – National Critical Infrastructure) je na rozdíl od Evropské kritické infrastruktury zcela v kompetenci jednotlivých členských států Evropské unie. To znamená, že kritická infrastruktura České republiky, jejíž narušení nebo zničení by mělo dopad přímo a pouze na Českou republiku je zcela v kompetenci České republiky. Evropská unie do národní kritické infrastruktury tedy nijak nezasahuje a přímo za ní zodpovídají jednotlivé členské státy.

V České republice mají odpovědnost za jednotlivé oblasti kritické infrastruktury jednotlivá ministerstva, podle jejich působnosti a kompetencí. Nejvyšším orgánem z hlediska bezpečnosti České republiky je Bezpečnostní rada státu.[1,3]

5.3.3 Soukromý sektor – role vlastníků, provozovatelů a uživatelů KI

„Označení kritická infrastruktura představuje pro vlastníky a provozovatele dané infrastruktury určitou odpovědnost. Z označení infrastruktury jako ECI nebo NCI vyplývají
pro její vlastníky a provozovatele čtyři hlavní povinnosti:

1) Oznámení příslušnému orgánu členského státu, že infrastruktura může být kritická;

2) Určení vedoucího představitele (představitelů) vystupujícího jako styčný úředník pro bezpečnost mezi vlastníky, provozovateli a příslušným orgánem ochran KI v členském státě. Styčný úředník pro bezpečnost se bude podílet na rozvoji bezpečnostních a krizových plánů. Měl by být rovněž hlavním styčným úředníkem s příslušným odvětvovým orgánem v členském státě a podle potřeby i s donucovacími orgány;

3) Zřízení, implementace a aktualizace Operačního plánu pro bezpečnost

4) Je-li to vyžadováno, účast na vypracování krizového plánu KI s orgány odpovědnými za civilní obranu v příslušném členském státě a s donucovacími orgány.“ [1]

5.4 Subjekt a objekt kritické infrastruktury

Pro lepší pochopení problematiky ochrany kritické infrastruktury je vhodné si definovat a popsat dva důležité pojmy. Subjekt kritické infrastruktury a objekt kritické infrastruktury.

5.4.1 Subjekt kritické infrastruktury

Pod pojmem subjekt kritické infrastruktury se rozumí vlastník nebo provozovatel objektů kritické infrastruktury.

Je velice důležité si uvědomit, že do procesu ochrany kritické infrastruktury vstupují subjekty na různých úrovních. V České republice se dá říci, že v procesu ochrany kritické infrastruktury hrají důležitou roli tři základní úrovně. Nejvyšší úrovní je ochrana kritické infrastruktury na úrovni Evropské unie, potom úroveň národní kritické infrastruktury a v neposlední řadě je to soukromý sektor, tedy soukromí vlastníci a provozovatelé.

Subjekty kritických infrastruktur lze rozdělit podle stanovených kritérií do několika základních kategorií:

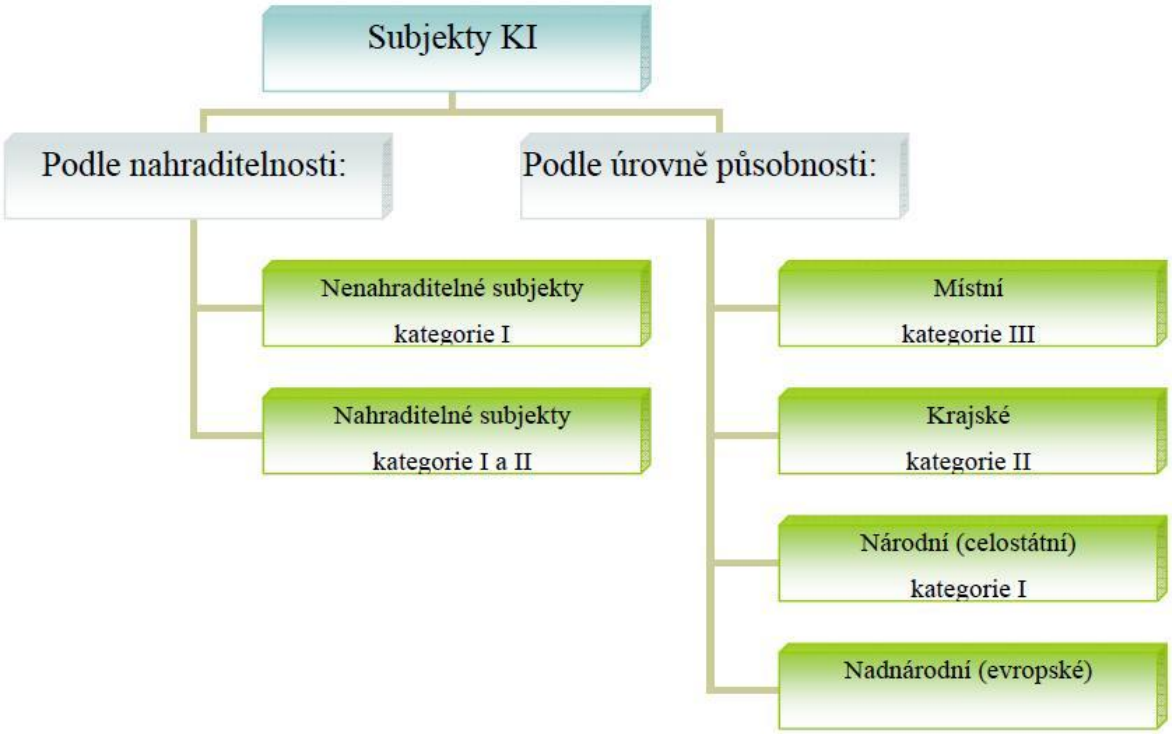
„Nenahraditelnost – při narušení je nutné subjekt opravit, rekonstruovat nebo znovu vystavět. Činnost nelze v krátkém časovém období nahradit – do obnovy činnosti bude řešeno jak naplňovat některé základní potřeby, např. dodavky elektřiny, plynu.

Nahraditelnost – při narušeni nebo zničeni jsou nutné opravy, rekonstrukce nebo znovuvýstavba. Subjekt či činnost je možně nahradit jiným subjektem nebo provizorním způsobem v dostačující kvalitě.

Úroveň působnosti - subjekty podle úrovně jejich působnosti, resp. potřebnosti dělíme na místní, krajská, národní - celostátní KI, nadnárodní - evropská KI. Subjekty zařazené do místní úrovně budou označovány jako subjekty KI kategorie III, krajské úrovně jako subjekty KI kategorie II a celostátní úrovně jako subjekty KI kategorie I. Jako zvláštní

kategorie jsou řešeny subjekty evropské KI.“[5]

Na obrázku 2 můžeme přehledně vidět, jak jsou rozděleny subjekty kritické infrastruktury do jednotlivých kategorií podle určujících kritérií.



Obrázek 2: *Kritéria určující rozděleni subjektů KI do jednotlivých kategorií*[5]

5.4.2 Objekt kritické infrastruktury

Objektem kritické infrastruktury se rozumí určitá stavba nebo zařízení, které zajišťuje správné fungování kritické infrastruktury. Objekty KI jsou tedy stavby a jiné zařízení veřejné infrastruktury, které vlastní či provozují subjekty kritické infrastruktury.

Objekty kritické infrastruktury můžeme podle rozsahu postiženého území a podle rozsahu dopadů narušení kritické infrastruktury dělit takto:

1. Rozdělení podle rozsahu postiženého území:
    a. Objekty národního významu
    b. Objekty krajského významu[5]

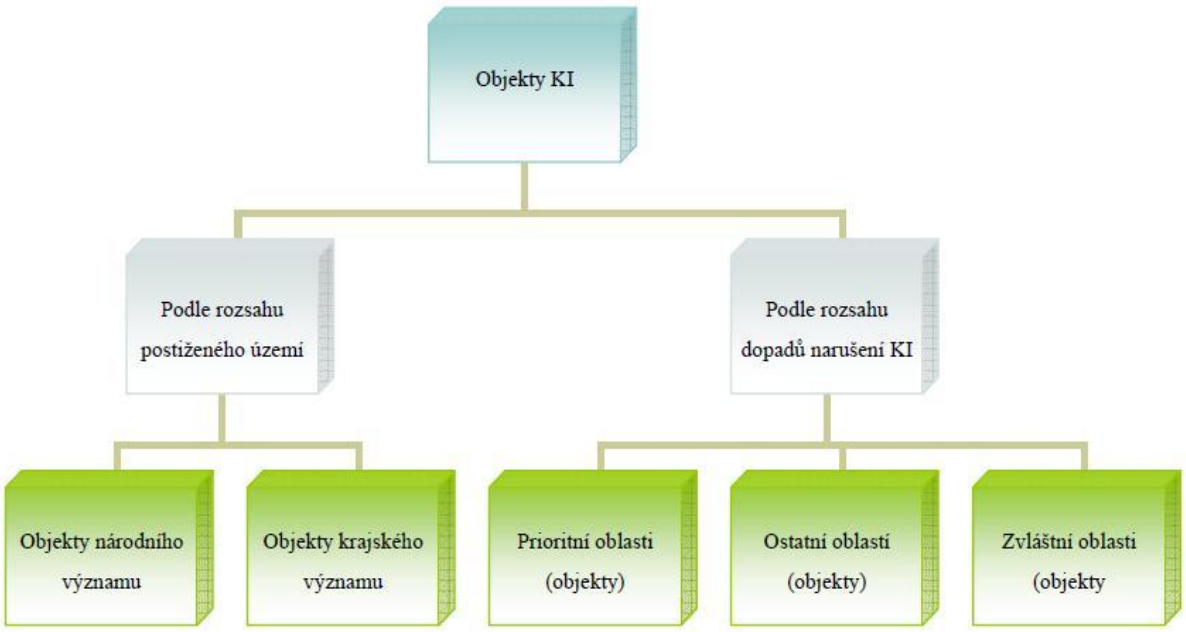
2. Rozdělení podle rozsahu dopadů narušení kritické infrastruktury:

a. Prioritní oblasti nebo objekty
b. Ostatní oblasti nebo objekty
c. Zvláštní oblasti nebo objekty[5]

Narušení objektů národního významu by samozřejmě mělo mnohem větší dopady než narušení objektů krajského významu. Narušení objektů národního významu by mělo dopad na zajištění bezpečnosti, ekonomiky, základních životních potřeb na území dvou a více krajů v ČR.

Při rozdělení objektů KI podle rozsahu dopadů narušení kritické infrastruktury je nejdůležitější kategorie prioritní oblasti nebo objekty. V případě narušení prioritních oblastí nebo objektů by jejich fungování bylo nenahraditelné nebo obtížně nahraditelné. Narušení by také ovlivnilo jiné oblasti kritické infrastruktury. Ostatní a zvláštní oblasti a objekty by byly v tomto případě nahraditelné alternativními objekty nebo jiným řešením, avšak také by jejich narušení ovlivnilo společenský život. Při narušení zvláštních objektů či oblastí by byl společenský život ovlivněn pouze za určitých okolností nebo ve specifických případech.

Na obrázku 3 lze přehledně vidět rozdělení objektů kritických infrastruktur v České republice podle rozsahu postiženého území a také podle rozsahu dopadů narušení kritických infrastruktur.



Obrázek 3: *Základní rozdělení objektů kritické infrastruktury* [5]

6 PŘÍSTUP K OCHRANĚ KRITICKÉ INFRASTRUKTURY ČESKÉ REPUBLIKY

„V podmínkách bezpečnostní politiky ČR je rozvíjeno především krizové řízení, které je pojato jako souhrn řídících činností věcně příslušných orgánů, které jsou zaměřeny na analýzu a vyhodnocení rizik, plánování, organizování, realizaci a kontrolu činností, prováděných v souvislosti s přípravou na řešení a s řešením krizové situace. Za krizovou situaci je považována mimořádná událost, při níž je vyhlášen některý z krizových stavů (stav nebezpečí, nouzový stav, stav ohrožení státu a válečný stav). Krizové řízení je rovněž vnímáno jako komplex opatření a úkolů, které pro zajištění ochrany a bezpečnosti obyvatelstva při vzniku mimořádných, resp. krizových situací plní orgány veřejné správy ve spolupráci s dalšími organizacemi.“[11]

Krizové řízení můžeme chápat jako cílevědomou lidskou činnost, která je zaměřená na přípravu a řešení krizových situací a mimořádných událostí. Jedná se o rozsáhlý proces, kterého se účastní mnoho subjektů nejen ze všech úrovní veřejné správy, ale i ze soukromého sektoru.

6.1 Orgány krizového řízení

„Orgány (vláda ČR, ministerstva a ostatní správní úřady, Česká národní banka, orgány krajů, obcí a určené orgány s územní působností), které ve prospěch svého zřizovatele zabezpečují analýzu a vyhodnocení možných ohrožení jeho bezpečnosti, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravnými opatřeními a řešením krizových situací.“[4]

6.2 Ochrana kritické infrastruktury z hlediska plánu krizové připravenosti subjektu KI

Krizový plán, plán krizové připravenosti a plán krizové připravenosti subjektu kritické infrastruktury patří mezi hlavní nástroje ochrany kritické infrastruktury v České republice.

Požadavky na plány krizové připravenosti a jejich náležitosti je stanoveno v nařízení vlády 462/2000 Sb.

6.2.1 Plán krizové připravenosti subjektu kritické infrastruktury

Plán krizové připravenosti je plánovacím dokumentem právnické osoby nebo podnikající fyzické osoby. Účelem tohoto dokumentu je zajistit plnění opatření vyplývajících z krizového plánu. [27]

Oproti tomu plán krizové připravenosti subjektu kritické infrastruktury je plánovacím dokumentem subjektu kritické infrastruktury. Plán krizové připravenosti subjektu kritické infrastruktury je důležitým nástrojem k zajištění připravenosti subjektu kritické infrastruktury na krizové situace, které mohou ohrozit funkci prvku kritické infrastruktury. [32]

Pokud by nastala situace, že subjekt kritické infrastruktury je zároveň právnická nebo podnikající fyzická osoba je možné plán krizové připravenosti subjektu kritické infrastruktury a plán krizové připravenosti sloučit do jediného výsledného dokumentu, musí však obsahovat náležitosti obou těchto plánů. [27]

6.2.1.1 Obsah plánu krizové připravenosti subjektu KI

Plán krizové připravenosti subjektu kritické infrastruktury se skládá ze tří základních částí:

- Základní část
- Operativní část
- Pomocná část[13]

Základní část plánu krizové připravenosti subjektu KI se dále skládá z následujících částí:

- Vymezení předmětu činnosti právnické nebo podnikající fyzické osoby a úkolů a opatření, které byly důvodem zpracování plánu krizové připravenosti
- Charakteristika krizového řízení
- Přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost právnické nebo podnikající fyzické osoby
- Seznam prvků kritické infrastruktury
- Identifikace možných ohrožení funkce prvku kritické infrastruktury[13]

Základní část plánu krizové připravenosti subjektu kritické infrastruktury nám v podstatě popisuje základní náležitosti. Popisuje působnost, odpovědnost a úkoly zpracovatele tohoto plánu. Zde jsou uvedeny i údaje jako adresa a spojení na zpracovatele. Dále plán popisuje charakteristiku organizace krizového řízení a její organizační strukturu. Základní část také vyhodnocuje všechna možná rizika spojená s možným ohrožením prvků kritické infrastruktury a uvádí seznam prvků kritické infrastruktury, včetně jejich identifikace.[13]

Konkrétním metodikám analýzy rizik použitelných v dané problematice se budu věnovat v následující kapitole.

Operativní část plánu krizové připravenosti subjektu KI se dále skládá z následujících částí:

- Přehled opatření vyplývajících z krizového plánu příslušného orgánu krizového řízení a způsob zajištění jejich provedení
- Způsob zabezpečení akceschopnosti právnické nebo podnikající fyzické osoby pro zajištění provedení krizových opatření a ochrany činnosti právnické nebo podnikající fyzické osoby
- Postupy řešení krizových situací identifikovaných v analýze ohrožení
- Plán opatření hospodářské mobilizace u dodavatelů mobilizační dodávky
- Přehled spojení na příslušné orgány krizového řízení
- Přehled plánů zpracovávaných podle zvláštních právních předpisů využitelných při řešení krizových situací[13]

Operativní část plánu krizové připravenosti subjektu kritické infrastruktury obsahuje výše uvedené náležitosti, ale především se zaměřením na ochranu funkce prvku kritické infrastruktury a dále stanovená opatření na ochranu prvku kritické infrastruktury. V této části plánu se také uvádí přehled opatření zaměřených na snížení rizika narušení funkce prvku kritické infrastruktury a dále jsou zde uvedeny postupy realizace těchto opatření za krizové situace.

Pomocná část plánu krizové připravenosti subjektu KI se dále skládá z následujících částí:

- Přehled právních předpisů využitelných při přípravě na mimořádné události nebo krizové situace a jejich řešení
- Přehled uzavřených smluv k zajištění provedení opatření, které byly důvodem zpracování plánu krizové připravenosti
- Zásady manipulace s plánem krizové připravenosti
- Geografické a podklady
- Další dokumenty související s připraveností na mimořádné události nebo krizové situace a jejich řešením[13]

Pomocná část plánu krizové připravenosti subjektu kritické infrastruktury obsahuje výše uvedené náležitosti se zaměřením na ochranu funkce prvku kritické infrastruktury.

6.3 Analýza rizik

„Nejdůležitějším krokem k eliminaci rizik a ke snížení možných dopadů rizik je nutné provést analýzu rizik. Analýza rizik je proces, který stanovuje pravděpodobnost uskutečnění hrozeb a dopadu na aktiva. Má za úkol identifikovat pravděpodobnost některé mimořádné události, jakož i možné dopady a škody. Jakékoliv účinné řešení problému je založeno na správně provedené analýze rizik„[11]

Analýza rizik je důležitým nástrojem k tomu, abychom mohli identifikovat zdroj rizik následně se pak vůči vzniklým rizikům účinně a efektivně bránit. Pomocí analýzy rizik se rizika roztřídí a vytvoří se žebříček různých rizik od nejvyšších rizik až po ty nejnižší. Na základě získaných výsledků se provede konečné hodnocení rizik. Metody pro analýzu rizik se obecně dělí na metody kvantitativní a metody kvalitativní. Existuje mnoho různých metod a také mnoho různých způsobů získávání dat a informací.

6.4 Metody pro hledání rizik

Metody pro hledání rizik uvedeny níže jsou vhodné pro hledání rizik a kritických míst v systému. Je také důležité si uvědomit, že nelze přesně určit, které metody je vhodné na hledání rizik a které na hledání kritických míst v systému. Výsledek použité metody hledání rizik by měl být především jednoduchý, přehledný a hlavně srozumitelný nejenom expertům, ale i laické veřejnosti. Takových to metod je spousta, v následujících

podkapitolách popíšu metody, které jsou vhodné pro použití v oblasti ochrany kritické infrastruktury.

6.4.1 Kontrolní seznam (Check list)

Kontrolní seznam je postup založený na neustálé kontrole realizace předem stanovených podmínek a opatření. Seznamy kontrolních otázek jsou obvykle generovány na základě charakteristik sledovaného systému nebo činností, které souvisejí se systémem a potenciálními dopady, selháním prvků systému a vznikem škod. Struktura kontrolních otázek se může měnit od jednoduchého seznamu až po složitý formulář.

Kontrolní seznam je vhodný pro rychlé a přesné vyhodnocení rizik. V zahraničí i u nás se začíná používat stále častěji.[11,21]

6.4.2 Analýza stromu událostí (ETA – Event Tree Analysis)

„Analýza stromu událostí je postup, který sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Metoda ETA je graficko-statistická metoda. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu.“[11]

Analýza stromů událostí je spíše vhodná pro vyhodnocení složitějších procesů, které mají více úrovní bezpečnostních systémů. Výsledkem této analýzy jsou scénáře a soubory poruch nebo chyb.

6.4.3 Analýza selhání a jejich dopadů (FMEA – Failure Mode and Effect Analysis)

Analýza selhání a jejich dopadů slouží k důkladné kontrole jednotlivých prvků projektovaného návrhu systémů a také jeho provozu. Je to postup, který je založený na rozboru způsobu selhání a jejich dopadů. Tato analýza nám umožňuje hledat dopady a příčiny na základě systematicky a strukturovaně vymezených selhání zařízení.

Tato analýza se využívá především pro zdůvodněné případy a vážná rizika. Vyžaduje výpočetní techniku a speciální software s konkrétní databází informací.[11,21]

6.4.4 Analýza stromů poruch (FTA – Fault Tree Analysis)

Analýza stromů poruch je postup založený na soustavném zpětném rozboru událostí. Tento zpětný rozbor využívá řetězec příčin, které mohu vést k vybrané vrcholové události. Analýza stromu událostí je metoda graficko-analytická. Postup této metody názorně zobrazuje strom poruch prostřednictvím rozvětveného grafu a předem dohodnuté symbolice a popisům.

Výsledkem analýzy stromů poruch by mělo být nalezení poruch zařízení a lidských chyb, nebo jejich kombinací, které by mohly vést k nehodě.[5,11]

6.4.5 Analýza lidské společnosti (HRA – Human Reliability Analysis)

„Analýza lidské spolehlivosti je postup na posouzení vlivu lidského činitele na výskyt živelních pohrom, nehod, havárií, útoků apod. nebo některých jiných dopadů. Koncept analýzy lidské spolehlivosti HRA směřuje k systematickému posouzení lidského faktoru (HumanFactors) a lidské chyby (HumanError). Ve své podstatě přísluší do zastřešující kategorie konceptu předběžného posuzování PHA. Zahrnuje přístupy mikroekonomické (vztah „člověk-stroj“) makroekonomické (vztah systému „člověk-technologie“). Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Uplatnění metody HRA musí vždy tvořit integrovaný problém bezpečnosti provozu a lidského faktoru v mezních situacích různých havarijních scénářů, tzn. Paralelně a nezávisle s další metodou rizikové analýzy.“[11]

6.4.6 Analýza příčin a dopadů (CCA – Causes and Consequences Analysis)

Analýza příčin a dopadů je kombinací analýzy stromů událostí a stromů poruch. Účelem této metody je najít základní příčiny a dopady pravděpodobných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a popisy možných koncových stavů nehod. Předností této analýzy je její použití jako komunikačního prostředku - diagram příčina dopadů nám přehledně zobrazuje vztahy mezi koncovými stavy nehody (nepřijatelnými dopady) a jejich základními příčinami. Díky kombinaci stromů poruch i stromů událostí může být výsledná grafická forma této analýzy velice detailní.

Používá se zvláště v případech, kdy logika analyzovaných poruch a nehod je poměrně jednoduchá.[11]

7 PŘÍSTUP K OCHRANĚ KRITICKÉ INFRASTRUKTURY VE VELKÉ BRITÁNII

V případě Velké Británie je přístup k ochraně kritických infrastruktur velmi významně ovlivněn hrozbou terorismu, která se právě v červenci 2005 ukázala jako reálná. Tehdy došlo v Londýně k sérii teroristických bombových útoků v Londýnském metru, které si vyžádaly přes pět desítek obětí a přes sedm set zraněných lidí.

Pro Velkou Británii ovšem není terorismus jako současná hrozba žádným novým pojmem. Terorismus je ve Strategii Spojeného království (United Kingdom´s Strategy) prezentovanou ministerským předsedou v Parlamentu identifikován jako reálná hrozba, které musí Velká Británie čelit. Jedná se především o hrozby ze strany islámského terorismu. Tuto skutečnost podpořily právě teroristické útoky v Londýně z července 2005, které byly provedeny právě členy muslimské komunity.

Jak je zmiňováno v tomto dokumentu, pro Spojené království Velké Británie a Severního Irska není teroristická hrozba ničím novým. V dokumentu se rovněž zmiňuje problém teroristických útoku v Severním Irsku. Proto je skutečností to, že pro národní infrastrukturu Spojeného království je teroristická hrozba vnímána jako největší ohrožení kritické infrastruktury.

V oblasti ochrany kritické infrastruktury je ve Velké Británii široce rozvinuta spolupráce mezi veřejným a soukromým sektorem. Vláda velmi úzce spolupracuje s mnoha soukromými subjekty a Centrum pro ochranu národní kritické infrastruktury (Centre for Protection of National Infrastructure - CPNI) sdílí informace a data s vlastníky národních kritických infrastruktur.

7.1 Centrum pro ochranu národní kritické infrastruktury – CPNI

CPNI funguje jako základní a hlavní prvek v oblasti bezpečnostního poradenství, ve kterém se zaměřuje na snížení zranitelnosti kritické infrastruktury. Tato zranitelnost je vnímána na základě národních bezpečnostních hrozeb, jako je terorismus a špionáž. Poradenství je poskytováno z těchto tří oblastí:

- Informační bezpečnost

- Fyzická bezpečnost
- Personální bezpečnost[25]

Informační bezpečnost:

„Téměř každá firma spoléhá na zachování důvěrnosti, integrity a dostupnosti svých dat. Ochrana informací, ať už se koná elektronicky nebo jiným způsobem, by měla být v centru bezpečnostního plánování organizace. Klíčové otázky, jak udržet informační bezpečnost pod stálou kontrolou, jsou:

- Kdo by chtěl přístup k našim informacím a jak by ho získal?
- Jaký by mohl mít prospěch z jejich využití?
- Jaké je možné poškození nebo ztráta dat?
- Jaký by byl dopad na činnost organizace?“ [25]

Fyzická bezpečnost:

Úkolem fyzické bezpečnosti je zabránit přímému útok na pozemek, nebo omezit možné škody a zranění, které můžou nastat v případě takových incidentů.

Pro většinu organizací CPNI doporučuje rozumnou kombinaci dobrého hospodaření a vhodných investic do kamerových systémů, zabezpečovacích systémů a osvětlení a podobně. Taková opatření jsou schopna odradit pachatele a ochránit před dalšími trestnými činy, jako například vandalismus nebo krádeže.

Personální bezpečnost:

„Osobní bezpečnostní opatření pomáhají organizacím řídit rizika zaměstnanců nebo dodavatelů majících legitimní přístup do prostor organizace, informací a personálu k neoprávněným účelům.“ [25]

7.2 Základní dokumenty pro ochranu kritické infrastruktury ve Velké Británii

K tomu, abych byl schopný analyzovat přístup k ochraně kritické infrastruktury Velké Británie je potřeba najít a vycházet z určitých aktuálních a platných dokumentů týkajících se této problematiky.

7.2.1 Národní bezpečnostní strategie – NSS (National Security Strategy)

Národní bezpečnostní strategie je ve Velké Británii zaměřena především na dvě hlavní rizika. Jedná se o terorismus a kybernetické útoky. Pro tyto dva typy ohrožení kritické infrastruktury má Velká Británie své vlastní postupy. Tyto postupy jsou uvedené v dokumentech Protiteroristická strategie (CONTEST – Counter terrorism strategy) a Strategie na ochranu kybernetiky (Cyber Security Strategy) z roku 2009. Program odolnosti kritické infrastruktury (CIRP – Critical Infrastructure Resilience Programme) se zabývá kritickou infrastrukturou a jejími sektory.[5,26]

„V příloze této strategie je popsána metodologie pro hodnocení národních bezpečnostních rizik – National Security Risk Assessment (NSRA). Hodnocení rizik zahrnuje rozhodnutí o relativním dopadu a pravděpodobnosti každého rizika ve srovnání s ostatními. Jde o přizpůsobenou metodiku používanou pro sestavování britského Národního registru rizik - National Risk Register (ten se zaměřuje pouze na domácí mimořádné situace civilního charakteru). Metodika NSRA zahrnuje posouzení dopadu události (na základě ekonomických důsledků, obětí a sociálních/strukturálních faktorů)a pravděpodobnost výskytu této události v průběhu určené lhůty. Největší váha byla přiřazena rizikům se schopností způsobit okamžité a přímé škody na britském území, hospodářství, lidu, klíčových institucích a infrastrukturách.“ [25]

7.2.2 Strategie boje proti terorismu – CONTEST

Cílem Strategie boje proti terorismu je snížit riziko z mezinárodního terorismu. CONTEST zahrnuje subjekty z vládních úřadů, záchranných služeb, dobrovolných organizací, podnikatelského sektoru a dalších partnerů nejen z Velké Británie, ale z celého světa.

CONTEST je rozdělena do čtyř základní oblastí:

- prevence,
- sledování,
- ochrana
- příprava[25]

CPNI se podílí na oblasti ochrany. Tato oblast zahrnuje snížení zranitelnosti Velké Británie a jejích zájmů v souvislosti se zahraničním teroristickým útokem.

7.2.3 Strategie kybernetické bezpečnosti – Cyber Security Strategy

„Ke konci roku 2011 britská vláda představila strategii kybernetické bezpečnosti s názvem Ochrana a podpora Velké Británie v digitálním světě. Dokument určuje, jak bude Velká Británie podporovat hospodářský růst, chránit národní bezpečnost a každodenní život občanů vybudováním důvěryhodnějšího a odolnějšího kybernetického prostředí. Zejména zdůrazňuje klíčovou roli užší partnerství mezi veřejným a soukromým sektorem. Což je důležité zejména pro subjekty kritické infrastruktury, ale lze tento model aplikovat i v ostatních oblastech. Včasné předávání informací umožňuje subjektům lépe se připravit na potenciální útoky.

Principy strategie jsou:

- přístup založený na rizicích
- práce v partnerství s komerčním sektorem

vyvážení bezpečnosti se svobodou a soukromím“ [25]

7.2.4 Národní registr rizik – NRR (National Risk Register)

V tomto dokumentu jsou sledovány nejvýznamnější a nejdůležitější mimořádné události, kterým by mohla Velká Británie v následujících 5 letech čelit. Tyto události jsou sledovány prostřednictvím Národního hodnocení rizik (National Risk Assessment - NRA). Jedná se o hodnocení, které se provádí každý rok s tím, že se využívají poznatky a zkušenosti ze většiny ministerstev a orgánů státní správy.

Národní registr rizik je veřejně přístupný a poslední aktualizace proběhla v únoru 2012. Tato aktualizace obsahuje také nejnovější hodnocení rizik.

NRA a NRR zachycují události, by mohly ohrozit národní kritickou infrastrukturu. Rizika jsou rozděleny do tří hlavních kategorií:

- přírodní události
- závažné havárie

- nebezpečné útoky[5,25]

7.2.5 Keeping the Country Runnig: Natural Hazards an Infrastructure

Tento dokument byl vdaný právě bezpečnostní radou státu ve Velké Británii. Byl vydaný v říjnu 2011. V podstatě se jedná o průvodce ke zlepšení odolnosti kritické infrastruktury a základních služeb v oblasti kritické infrastruktury.

Kritická infrastruktura Velké Británie je komplexní propojený systém. Tento průvodce byl vytvořený pro podporu vlastníkům a provozovatelům infrastruktur, zasahujících při mimořádných událostech, různé organizace, skupiny a vládní úřady, aby společně pracovaly na zlepšení odolnosti kritické infrastruktury a poskytování základních služeb.[22]

Obsah:

Tento dokument je rozdělen na čtyři základní oddíly:

- Oddíl A: Úvod, definice a principy odolnosti infrastruktury
- Oddíl B: Zvyšování odolnosti
- Oddíl C: Praktický návod
- Oddíl D: Přílohy[22]

Oddíl A vysvětluje účel a obecné informace k této příručce, poskytuje definice a principy problematiky odolnosti infrastruktury.[22]

Oddíl B nastiňuje přístup ke zlepšení a udržení odolnosti infrastruktury. V tomto oddílu jsou mimo jiné také postupy pro analýzu rizik a identifikaci možných hrozeb, standardy pro hodnocení rizik a obsahuje také plány pro zvyšování a udržení odolnosti kritických infrastruktur.[22]

Oddíl C poskytuje praktické informace pro vládu, výbory a odpovědné orgány, vlastníky a provozovatele infrastruktur, a také orgány zasahující při mimořádných událostech. V této části je obsažen praktický návod například s pokyny pro vyhodnocení rizik nebo kontrolní

seznam pro subjekty kritických infrastruktur. Tato část také obsahuje podkapitoly, jako jsou pokyny pro sdílení informací nebo pokyny pro posuzování vzájemných závislostí.[22]

Oddíl D obsahuje tři hlavní doprovodné přílohy. Přílohy se týkají související legislativy a jsou zde také přílohy obsahující poučení z předchozích mimořádných událostí a podobně.[22]

7.3 Bezpečnostní rada státu Velké Británie

V České republice je nejvyšším stálým pracovním orgánem vlády pro problematiku bezpečnosti Bezpečnostní rada státu. Má své výbory, které připravují návrhy na zlepšení v oblasti bezpečnosti ČR.

Ve Velké Británii existuje v podstatě obdobný stálý pracovní orgán zabývající se národní bezpečností a tedy i ochranou kritické infrastruktury. Nese stejný název jako v České republice, tedy Bezpečnostní rada státu (National Security Council - NSC).

Bezpečnostní rada státu (NSC) ze Spojeného království je pracovním výborem vlády, který má za úkol dohlížet na všechny záležitosti týkající se národní bezpečnosti, zpravodajské koordinace a obranné strategie ve velké Británii. NSC byla založena dne 12. května 2010 ministerským předsedou Davidem Cameronem. Bezpečnostní rada státu bude koordinovat reakce na hrozby, kterým čelí Spojené království. NSC bude také koordinovat aktivitu příslušných vládních institucí ve vztahu k národní bezpečnosti.[20]

V současné době tvoří strukturu NSC tři pracovní výbory:

- Výbor pro analýzu ohrožení a odolnosti
- Výbor pro analýzu jaderné bezpečnosti
- Bezpečnostní výbor s mezinárodní působností[20]

Každý výbor má konkrétní úkoly. Výbory mají za úkol zkoumat a analyzovat konkrétnější oblasti v problematice národní bezpečnosti Velké Británie.

8 SROVNÁNÍ PŘÍSTUPŮ K OCHRANĚ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A VELKÉ BRITÁNII

V poslední kapitole mé práce budu provádět srovnání kritické infrastruktury a přístupy k její ochraně v České republice a Velké Británii. Tato kapitola by měla mimo jiné poukázat na to, že kritická infrastruktura je v každé zemi chápána trochu odlišným způsobem. Kritická infrastruktura je v podstatě všeobecný pojem, ale různé státy ho pojímají jinými způsoby. V každé zemi jsou odlišné legislativní rámce pro danou problematiku. V České republice i ve Velké Británii je rozdílné i rozdělení sektorů kritické infrastruktury a také zodpovědnost za její chod je v každé zemi trochu rozdílný. Důležité je také poukázat na to, že Česká republika se liší především v přístupu k analýze rizik, protože pro Velkou Británii jsou prioritní rizika a hrozby v současnosti zcela jiné než v České republice.

Pokud bych začal srovnáváním pojetí kritické infrastruktury jako takové, tak je vhodné si uvést, že každá země má svoji vlastní definici kritické infrastruktury.

Definice kritické infrastruktury v České republice je podle Ministerstva vnitra taková: „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.“[4]

Ve Velké Británii definovala kritickou infrastrukturu Vláda takto: „jako zařízení, systémy, místa a sítě nezbytné pro chod státu a pro dodávky základních potřeb, na kterých závisí každodenní život ve Velké Británii.“[19]

Uvedli jsme si definice kritické infrastruktury obou srovnávaných států. Z těchto definic lze vyvodit to, že pojetí kritické infrastruktury jako takové je v obou zemích v podstatě stejné. Ačkoliv se definice liší v některých slovech tak význam je prakticky totožný. V obou zemích se shodují na tom, že kritická infrastruktura jsou vlastně nejdůležitější prvky a systémy pro základní a bezproblémový chod státu.

8.1 Srovnání oblastí kritické infrastruktury České republiky a Velké Británie

Pro přehledné srovnání uvedu tabulku oblastí kritické infrastruktury v České republice a Velké Británii. Pro lepší názornost v tabulce uvedl i sektory kritické infrastruktury v Evropské unii.

Tabulka 3: *Srovnání sektorů KI v České republice, Velké Británii a Evropské unii*[9]

Sektory KI	Česká republika	Velká Británie	Evropská unie
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	ANO	NE
Veřejná správa	ANO	ANO	ANO
Jaderný průmysl	NE	NE	ANO
Chemický průmysl	NE	NE	ANO
Vesmír a výzkum	NE	NE	ANO
Ochrana práv a pořádku	NE	NE	ANO

Z výše uvedené tabulky je naprosto patrné, že sektory kritické infrastruktury v české republice a ve Velké Británii jsou naprosto totožné. Každá země má devět oblastí kritické

infrastruktury. V oficiálním dokumentu Velké Británie o oblastech KI (Sector Resilience Plan for Critical Infrastructure) nejsou všechny pojmenovány úplně stejně a můžeme tam najít několik rozdílností, ale můžeme konstatovat, že oblasti kritické infrastruktury v České republice a ve Velké Británii se shodují.

8.2 Srovnání z hlediska analýzy rizik

Česká republika i Velká Británie, jako členské státy Evropské unie jsou zahrnuty do programu EPCIP. Ovšem Velká Británie je především soustředěna na svoji národní kritickou infrastrukturu. Takovýto postoj lze pochopit s ohledem na historii země a také z toho důvodu, že Velká Británie je ostrovní zemí.

Pro Velkou Británii jsou určeny jako dvě nejvyšší prioritní rizika teroristické útoky a kybernetické útoky. Naproti tomu tyto současné rizika v České republice nejsou hodnoceny jako prioritní rizika. Samozřejmě že se tyto rizika také řeší a je jim věnovaná pozornost, ale není na takové hrozby kladen takový důraz jako na jiná hrozby, jako například přírodní katastrofy, především záplavy nebo průmyslové havárie.

Svým přístupem k možným hrozbám a vyhodnocením rizik je Velká Británie orientovaná jiným směrem. Jednotlivé země světa volí rozsah a intenzitu protiteroristických opatření podle řady faktorů, například své velikosti, lidnatosti, geostrategické polohy a dalších.

Dá se tedy konstatovat, že v tomto směru jsou porovnávané země docela dost odlišné. Vyhodnocení primárních hrozeb a rizik je ve Velké Británii podstatně rozdílné, důvodem tohoto faktu jsou skutečnosti, že Velká Británie událostech teroristických útocích na Londýnské metro byla prakticky přinucena směřovat svoji bezpečnostní politiku k ochraně obyvatel právě před takovými hrozbami.

8.3 Srovnání přístupů k ochraně KI na vybrané státy metodou kontrolního seznamu

Pro srovnání přístupu k ochraně kritické infrastruktury v České republice a Velké Británii použiju metodu zvanou kontrolní seznam (Check list). Tato metoda je podrobněji popsána v této práci v podkapitole analýzy rizik.

V podstatě principem této metody je formulovat seznam otázek v dané problematice. Musí to být otázky, na které se dá odpovědět buď možností ano, nebo ne. Ve vyplněném kontrolním seznamu se sečtou odpovědi kladné (Ano) a záporné (Ne) a vypočítáme procentuální poměr. Následné vyhodnocení se provádí podle jednoduché tabulky, uvedené níže, viz tabulka 4. Tabulka nám přiřazuje k procentuálnímu vyhodnocení slovní vyhodnocení.

Tabulka 4: *Vyhodnocení kontrolního seznamu*[5]

Kladné odpovědi (%)	Slovní hodnocení
95 a více	výborné
70 - 94	velmi dobré
50 - 69	dobré
20 - 49	špatné
do 20	velmi špatné/kritické

Dohromady vytvořený kontrolní seznam obsahuje 16 otázek týkající se ochrany kritické infrastruktury. Je nutné si uvědomit, že se jedná o jednoduchý seznam a pro detailnější analýzu by bylo potřeba vytvořit dlouhý seznam, nebo dokonce formulář, na kterém by pracoval tým odborníků a který by do nejmenších podrobností zkoumal danou problematiku z různých hledisek. Pro jednoduché srovnání v této oblasti je tento kontrolní seznam dostačující.

Tabulka 5: *Kontrolní seznam pro srovnání České republiky a Velké Británie* [5]

Kontrolní seznam (check list)	Česká republika		Velká Británie	
	ANO	NE	ANO	NE
Je jasně stanoveno, kdo nese zodpovědnost za KI?	x		x	
Je legislativně ustanoven orgán (úřad) pro ochranu KI?		x	x	
Je vypracovaný Národní program na ochranu KI?	x		x	
Je v současnosti již zapracována do zákonů směrnice EU 2008/114/ES?	x		x	

Jsou stanovené sektory KI?	x		x	
Je v současnosti vymezena definice KI?	x		x	
Jsou vymezeny základní pojmy KI legislativou?	x		x	
Existuje zákon o KI přímo v legislativě?		x		x
Patří oblast ochrany KI do priorit výzkumně-vývojové podpory?	x		x	
Je zajištěn subjekt pro koordinaci mezi oblastmi KI?		x	x	
Je vytvořen program na finanční podporu pro ochranu KI?		x		x
Je v oblasti KI rozvinuta spolupráce mezi veřejným a soukromým sektorem?	x		x	
Je vypracována národní databáze rizik?		x	x	
Je vytvořen program na ochranu informační infrastruktury?		x	x	
Je ustanovený odborný subjekt v problematice KI?	x		x	
Je vnímána ochrana KI jako prioritní funkce státu mezi širokou veřejností?		x	x	

Po vyhodnocení uvedeného kontrolního seznamu nám vyšly výsledky pro Českou republiku 56% a pro Velkou Británii 87% kladných odpovědí. Česká republika si zajistila hodnocení – dobré. A Velká Británie hodnocení – velmi dobré. Výsledkem by tedy bylo, že Česká republika je na tom o stupeň hůře než Velká Británie. Dalo se to očekávat vzhledem k tomu, že Velká Británie jako první evropský stát začala věnovat ochraně kritické infrastruktury velkou pozornost a později se začaly přidávat i další evropské státy.

V obou porovnávaných zemích je zodpovědné za ochranu KI Ministerstvo vnitra. V České republice však MV přeneslo odpovědnost za oblast KI na Generální ředitelství hasičského záchranného sboru (GŘ HZS).

Velká Británie je má jasně ustanovený úřad pro ochranu kritické infrastruktury, jedná se o Centrum pro ochranu kritické infrastruktury (CPNI) a vzniklo v roce 2007 sloučením Bezpečnostního koordinačního centra národní infrastruktury (National Infrastructure Security Co-ordination Centre) a Rady národního bezpečnostního centra (National Security

Advice Centre). V tomto ohledu má Velká Británie výrazně navrch, jelikož v České republice doposud není žádný orgán nebo úřad, který by se přímo zabýval ochranou KI.

Obě země mají vypracované národní programy na ochranu kritických infrastruktur a jak Česká republika, tak i Velká Británie již zapracovaly směrnici rady EU 2008/114/ES do svých zákonů. Sektory kritické infrastruktury jsou stanoveny v obou zemích a z předchozího srovnání jsme zjistili, že se prakticky shodují.

Velká Británie i Česká republika jsou zahrnuty do programu EPCIP, ale Velká Británie je primárně soustředěna na svoji národní kritickou infrastrukturu, což v České republice není tak patrné. To, že kritická infrastruktura není přímo ukotvena v zákoně, ale je zmíněna v různých souvisejících předpisech, které se týkají přímo oblastí kritické infrastruktury je v taktéž stejné v obou zemích.

V obou zemích je široce rozvinutá spolupráce mezi veřejným a soukromým sektorem v oblasti ochrany KI. Mnoho subjektů kritické infrastruktury, jak u nás, tak i ve Velké Británii vlastní soukromí majitelé a tak je tedy logické, že mají zájem na ochraně svých vlastních hodnot.

Dalším bodem, ve kterém nás Velká Británie převyšuje je to, že má vlastní Strategii kybernetické bezpečnosti a také Národní registr rizik. To jsou důležité dokumenty pro ochranu kritické infrastruktury a ČR je v tomto směru pozadu. Národní registr rizik není vytvořen, existuje však evropská databáze rizik zvaná MARS (Major Accident Reporting System), která slouží k uchovávání informací o závažných haváriích v EU.

Z výsledků můžeme konstatovat, že Velká Británie je v problematice ochrany kritické infrastruktury o krok napřed před Českou republikou. Ve srovnání s Českou republikou se této problematice se začala věnovat dříve a teroristické útoky na Londýnské metro jen posílily aktivitu ke zlepšení ochrany KI. Velká Británie je primárně zaměřena na hrozby terorismu a kybernetických útoků. V tomto směru se přístup České republiky odlišuje, nutno však dodat, že ČR má zpracovaný dokument s názvem Akční plán boje proti terorismu.

Mezi širokou veřejností je pojem kritická infrastruktura jistě více skloňovaný ve Velké Británii, která si na vlastní kůži zažila teroristické útoky. To přispělo, jak ke zvýšené aktivitě v této oblasti mezi odbornou veřejností, tak i k většímu povědomí o oblasti KI napříč celou společností.

ZÁVĚR

Diplomová práce je rozdělená na dvě hlavní části. Na teoretickou a praktickou část. Teoretická část je dále rozdělena na čtyři kapitoly.

První kapitola má za úkol uvést čtenáře do problematiky kritické infrastruktury, definuju zde základní pojmy a popisuju její historický a novodobý vývoj. Druhá a třetí kapitola se zabývá kritickou infrastrukturou v České republice a ve Velké Británii. Zabývám se zde vývojem, pojetím a legislativním usměrněním dané problematiky v obou uvedených zemích. V těchto kapitolách jsem také uvedl oblasti kritické infrastruktury v obou zemích, které byly předmětem následného porovnávání. Poslední kapitola teoretické části popisuje současné existující hrozby a rizika, před kterými je potřeba kritickou infrastrukturu ochránit.

Praktická část je rozdělená taktéž na čtyři kapitoly. První kapitola slouží jako uvedení do problematiky ochrany kritické infrastruktury. Zde jsou vysvětleny důležité pojmy této problematiky, bez kterých by bylo čtení diplomové práce značně obtížné a nesrozumitelné. V následujících kapitolách jsou popsány přístupy k ochraně kritické infrastruktury v České republice a ve Velké Británii. Poslední kapitola diplomové práce porovnává přístupy k ochraně kritické infrastruktury v obou zemích z různých hledisek. Srovnávám zde sektory kritické infrastruktury a také vyhodnocení možných rizik. Součástí srovnání obou zemí je také vytvořený kontrolní seznam pro obě země, který přehledně vyhodnocuje přístupy k ochraně kritické infrastruktury v České republice a Velké Británii.

Přínos práce spočívá především v podpoře řešení projektu VG20112014067 - Systém hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury, jehož cílem je výzkum v oblasti hodnocení odolnosti prvků a sítí vybraných oblastí kritické infrastruktury.

Já osobně jsem si potvrdil, jak rozsáhlá a složitá je problematika kritické infrastruktury a její ochrany. Potvrdil jsem si také skutečnost, kterou jsem nastínil již v úvodu, že problematika kritické infrastruktury a její ochrany by si zasloužila podstatně větší pozornost než v současné době má. Nestačí, aby se věnovalo této problematice jen několik málo odborníků, ale měla by se také dostat do povědomí široké veřejnosti.

ZÁVĚR V ANGLIČTINĚ

The thesis is divided into two main parts. The theoretical and practical part. Theoretical part is divided into four chapters.

The first chapter aims to introduce readers to the problems of critical infrastructure, define here the basic concepts and describes its history and modern development. The second and third chapter deals with the critical infrastructure in the Czech Republic and Great Britain. Here I deal with the development, concepts and legislative guideline of the issue in both countries. In these chapters, I also noted the critical infrastructure in both countries that were the subject of comparison. The last chapter describes the theoretical part of the current, existing threats and risks facing the need to protect critical infrastructure.

The practical part is also divided into four chapters. The first chapter serves as an introduction to the problems of critical infrastructure protection. Here are some important terms explained this issue, without which it would read the thesis considerably more difficult and incomprehensible. The following chapters describe approaches to the protection of critical infrastructure in the Czech Republic and Great Britain. The last chapter of the thesis compares the approaches to the protection of critical infrastructure in both countries from different perspectives. I compare here the critical infrastructure sectors as well as evaluation of potential risks. The comparison between the two countries also created a checklist for both countries, which clearly evaluates approaches to protect critical infrastructure in the Czech Republic and Great Britain.

The contribution of the work lies primarily in support of the project VG20112014067 - The evaluation of resistance elements and networks selected areas of critical infrastructure, aimed at research on evaluation of resistance elements and networks selected areas of critical infrastructure.

Personally, I have proved how extensive and complex the issue of critical infrastructure and its protection. I also confirmed the fact that I outlined in the introduction, that the issue of critical infrastructure and the protection it deserves much more attention than at present has. It is not enough to take up this issue just a few experts, but should also get into public awareness.

SEZNAM POUŽITÉ LITERATURY

[1] KOTÍK, David. *Ochrana kritické infrastruktury Evropské unie*. Zlín, 2008. Dostupné z: http://theses.cz/id/n87bfl/. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce doc. Ing. Luděk Lukáš, CSc.

[2] HROMADA, Martin. *Technologické aspekty ochrany kritickej infraštruktúry SR*. Zlín, 2011. Dostupné z: http://dspace.k.utb.cz/handle/10563/16414. Disertační práce. Univerzita Tomáše Bati ve Zlíně.

[3] MALANÍK, Luboš. *Ochrana kritické infrastruktury České republiky*. Dostupné z: http://dspace.k.utb.cz/handle/10563/7332. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce doc. Ing. Luděk Lukáš, CSc.

[4] MINISTERSTVO VNITRA. *Kritická infrastruktura - Ministerstvo vnitra* [online]. 2009 [cit. 2012-05-08]. Dostupné z: http://www.mvcr.cz/clanek/pojmy-kriticka-infrastruktura.aspx.

[5] GAVENDOVÁ, Hana. *Komparace ochrany kritické infrastruktury v České republice a Evropské unii*. Brno, Duben 2009. Dostupné z: http://is.muni.cz/th/50593/esf_m/Gavendova_Diplomova_prace.pdf. Diplomová práce. Masarykova univerzita. Vedoucí práce Ing. Eduard BAKOŠ.

[6] FIŠER, Lukáš. *Ochrana kritické infrastruktury USA*. 2009, Zlín. Dostupné z: http://dspace.k.utb.cz/handle/10563/9686. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce doc. Ing. Luděk Lukáš, CSc.

[7] JURÍČEK, Ivan. *Ochrana prvku kritickej infrastruktury SR před teroristickými útokmi s možnosťou využitia NVS*. 2010, Žilina. Bakalářská práce. Žilinská Univerzita Žiline.

[8] PŮLKRÁBEK, Aleš. *Ochrana bankovního sektoru jako segmentu kritické infrastruktury*. 2009, Pardubice. Diplomová práce. Univerzita Pardubice. Vedoucí práce doc. RNDr. Petr Linhart, Csc.

[9] VERNEROVÁ, Zdenka. *Pojetí kritické infrastruktury v mezinárodním srovnání*. 2011, Pardubice. Bakalářská práce. Univerzita Pardubice. Vedoucí práce Ing. Ondřej Svoboda.

[10] DVOŘÁK, Tomáš. *Ohrožení vybraných kritických infrastruktur v EU terorismem*. 2009, Ústí nad Labem. Bakalářská práce. Masarykova univerzita v Brně. Vedoucí práce Mgr. Martin Bastl, Ph.D.

[11] SVOBODA, Zdeněk. *Kritická infrastruktura a její ochrana*. 2010, Ostrava. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Ing. Danuše Kratochvílová.

[12] Zákon o krizovém řízení a o změně některých zákonu (krizový zákon). In: *240/2000 Sb.* 2000. Dostupné z: http://www.firebrno.cz/uploads/legislativa/240_2000.pdf.

[13] Nařízení vlády k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonu (krizový zákon). In: *462/2000 Sb.* 2000. Dostupné z: http://www.firebrno.cz/uploads/legislativa/462_2000.pdf.

[14] Zákon 430, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In: *430/2010 Sb.* 2010. Dostupné z: http://www.epravo.cz/_dataPublic/sbirky/2010/sb0149-2010.pdf.

[15] Nařízení vlády 431, kterým se mění nařízení vlády č. 462/2000 Sb. k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění nařízení vlády č. 36/2003 Sb. In: *431/2010 Sb.* 2010. Dostupné z: http://www.epravo.cz/_dataPublic/sbirky/2010/sb0149-2010.pdf.

[16] Nařízení vlády 432 o kritériích pro určení prvku kritické infrastruktury. In: *432/2010 Sb.* 2010. Dostupné z: http://www.epravo.cz/_dataPublic/sbirky/2010/sb0149-2010.pdf.

[17] Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. In: *L 345/75*. 2008. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF.

[18] HASIČSKÝ ZACHRANNÝ SBOR ČESKÉ REPUBLIKY. *Kritická infrastruktura a její ochrana* [online]. 2009 [cit. 2012-05-07]. Dostupné z: http://www.hzscr.cz/clanek/kriticka-infrastruktura-a-jeji-ochrana.aspx.

[19] CABBINET OFFICE. *Infrastructure and Corporate Resilience* [online]. 2011 [cit. 2012-05-8]. Dostupné z: http://www.cabinetoffice.gov.uk/infrastructure-resilience.

[20] CABBINET OFFICE. *National Security Council* [online]. 2011 [cit. 2012-05-07]. Dostupné z: http://www.cabinetoffice.gov.uk/content/national-security-council/ce.

[21] ŘÍHA, Josef. Typologické znaky kritické infrastruktury. *THE SCIENCE FOR POPULATION PROTECTION*. 2009, 1/2009. Dostupné z: http://www.population-protection.eu/attachments/033_vol1n1_riha.pdf.

[22] CABBINET OFFICE. *Keeping the Country Running: Natural Hazards and Infrastructure* [online]. 2011 [cit. 2012-05-07]. Dostupné z: http://www.cabinetoffice.gov.uk/resource-library/keeping-country-running-natural-hazards-and-infrastructure.

[23] Sector-resilience-plan. CABINET OFFICE. *Cabinet Office* [online]. 2010 [cit. 2012-05-12]. Dostupné z: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/349100/sector-resilience-plan.pdf.

[24] CABBINET OFFICE. *Cyber Security* [online]. 2011 [cit. 2012-05-06]. Dostupné z: http://www.cabinetoffice.gov.uk/content/cyber-security.

[25] UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ. *Analýza způsobů hodnocení odolnosti sítí a prvků KI ve vybraných státech*. Zlín, 2012.

[26] WENGER, Andreas, Victor MAUER a Myriam Dunn CAVELTY. CENTER FOR SECURITY STUDIES, ETH Zurich. *INTERNATIONAL CIIP HANDBOOK 2008 / 2009*. 2009, 652 s. Dostupné z: http://e-collection.library.ethz.ch/eserv/eth:31095/eth-31095-01.pdf.

[27] Metodika zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In: *462/2000*.

[28] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *URBANISMUS A ÚZEMNÍ ROZVOJ*. 2007, X, 4/2007.

[29] BÍLEK, Martin. ČEPS, akciová společnost. *Problematika kritické infrastruktury*. Praha 10, 2008.

[30] The National Security Strategy. CABINET OFFICE. *Cabinet Office* [online]. 2010 [cit. 2012-05-6]. Dostupné z: http://www.cabinetoffice.gov.uk/news/national-security-strategy.

[31] MAŇÁK, Roman. *Vývoj ochrany kritické infrastruktury české republiky*. 2009, Zlín. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Jaroslava Gregušová

[32] Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *Ministerstvo vnitra* [online]. 2008, 4/2008 [cit. 2012-05-11]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html

[33] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Bezpečnostní strategie ČR 2011* [online]. Praha, 2011 [cit. 2012-05-02]. ISBN 978-80-7441-005-5. Dostupné z: http://www.mocr.army.cz/images/Bilakniha/CSD/011.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BRS	Bezpečnostní rada státu
CCA	Causes and Consequences Analysis
CIP	Critical Infrastructure Protection
CIRP	Critical Infrastructure Resilience Programme
CIWIN	The Critical Infrastructure Warning Information Network
CPNI	Centre for Protection of National Infrastructure
ČR	Česká republika
ECI	Evropská kritická infrastruktura
ETA	Event Tree Analysis
EPCIP	European Program for Critical Infrastructure Protection
EU	Evropská unie
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
G8	Group of eight
HRA	Human Reliability Analysis
IS	Informační systém
IZS	Integrovaný zachranný systém
KI	Kritická infrastruktura
KS	Krizová situace
MARS	Major Accident Reporting System
MU	Mimořádná situace
MV	Ministerstvo vnitra
NATO	North Atlantic Treaty Organization
NCI	National Critical Infrastructure
NKI	Národní kritická infrastruktura

NSC	National Security Council
NSRA	National Security Risk Assessment
NRA	National Risk Assessment
NRR	National Risk Register
OSN	Organizace spojených národů
PČR	Polici České republiky
UK	United Kingdom
USA	United States of America
VCNP	Výbor pro civilní nouzové plánování

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBLASTI KI V ČR 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	Potravinářství 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. Bankovnictví	ČNB
		7.3. Pojišťovnictví	
		7.4. Kapitálový trh	MF/ČNB
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 P II: OBLATI KI EU DLE ZELENÉ KNIHY O EPCIP

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 III: OBLASTI KI V UK DLE SECTOR RESILIENCE PROGRAM FOR CRITICAL INFRASTRUCTURE 2011