Masarykova univerzita

Ekonomicko-správní fakulta

Studijní obor: Regionální rozvoj a správa

KOMPARACE OCHRANY KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A EVROPSKÉ UNII

Comparison of the Critical Infrastructure Protection in the Czech Republic and European Union

Diplomová práce

Vedoucí diplomové práce:
Ing. Eduard BAKOŠ

Autor:
Ing. Hana GAVENDOVÁ

Brno, duben 2009

Jméno a příjmení autora: Hana Gavendová
Název diplomové práce: Komparace ochrany kritické infrastruktury v České republice a Evropské unii
Název práce v angličtině: Comparison of the Critical Infrastructure Protection in the Czech Republic and European Union
Katedra: Regionálního rozvoje a správy
Vedoucí diplomové práce: Ing. Eduard Bakoš
Rok obhajoby: 2009

Anotace

Předmětem diplomové práce je provedení komparace ochrany kritické infrastruktury v České republice a Evropské Unii. V první části je provedena analýza současného stavu s důrazem na vývoj kritické infrastruktury v USA, Evropě, České republice a NATO. V rámci první kapitoly je také provedena explikace základních pojmů řešené problematiky. Druhá část práce popisuje kritickou infrastrukturu ve vybraných zemích EU a státech mimo EU. Ve třetí části je provedena komparace kritické infrastruktury v ČR a EU a vymezeny stěžejní rozdíly. Poslední kapitola diplomové práce srovnává metodou kontrolního seznamu kritickou infrastrukturu v ČR a na Slovensku.

Annotation

The aim of the thesis is to compare Critical Infrastructure Protection in the Czech Republic and European Union. In the first part there was describing the present state in the area of Critical Infrastructure Protection, emphatically at evolution in the USA, Europe, Czech Republic and NATO. In terms of the first chapter, there are also determinate the fundamental terms. The second part of the thesis gives account of Critical Infrastructure in the chosen countries of European Union and chosen countries outside of European Union. The third chapter compares Critical Infrastructure in the Czech Republic and European Union and there are describe the main differences. The last chapter of the diploma thesis compares the Critical Infrastructure of Czech Republic and Slovakia by the method of check list.

Klíčová slova

Kritická infrastruktura, objekty kritické infrastruktury, ochrana obyvatelstva, sektory kritické infrastruktury

Keywords

Critical Infrastructure, Objects of the Critical Infrastructure, Civil Protection, Sectors of the Critical Infrastructure

Prohlášení

Prohlašuji, že jsem diplomovou práci *Komparace ochrany kritické infrastruktury v ČR a EU* vypracovala samostatně pod vedením Ing. Eduarda Bakoše a uvedla v ní všechny použité literární a jiné odborné zdroje v souladu s právními předpisy, vnitřními předpisy Masarykovy univerzity a vnitřními akty řízení Masarykovy univerzity a Ekonomicko-správní fakulty MU.

V Brně dne 19. dubna 2009

vlastnoruční podpis autora

Poděkování

Na tomto místě bych ráda poděkovala Ing. Eduardu Bakošovi za cenné připomínky a odborné rady, kterými přispěl k vypracování této diplomové práce.

OBSAH

ÚVOD 7
1 ANALÝZA SOUČASNÉHO STAVU 9
1.1 Vývoj kritické infrastruktury na jednotlivých úrovních 11
1.1.1 Vývoj kritické infrastruktury v USA 11
1.1.2 Vývoj kritické infrastruktury v Evropě 12
1.1.3 Vývoj kritické infrastruktury v České republice 17
1.1.4 Kritická infrastruktura na úrovni Severoatlantické aliance 22
1.2 Explikace základních pojmů v oblasti kritické infrastruktury 24
1.2.1 Vymezení pojmů infrastruktura a ochrana kritické infrastruktury 25
1.2.2 Subjekty kritické infrastruktury 30
1.2.3 Objekty kritické infrastruktury 33
2 KRITICKÁ INFRASTRUKTURA VYBRANÝCH ZEMÍ 38
2.1 Kritická infrastruktura vybraných zemí Evropské Unie 38
2.1.1 Finsko 41
2.1.2 Francie 42
2.1.3 Itálie 43
2.1.4 Maďarsko 44
2.1.5 Německo 45
2.1.6 Nizozemí 47
2.1.7 Norsko 48
2.1.8 Polsko 49
2.1.9 Slovensko 50
2.1.10 Španělsko 52
2.1.11 Švédsko 53
2.1.12 Velká Británie 54
2.2 Kritická infrastruktura vybraných států světa mimo Evropskou unii 58
2.2.1 Austrálie 58
2.2.2 Kanada 59
2.2.3 Nový Zéland 60
2.2.4 Spojené státy americké 61
3 KRITICKÁ INFRASTRUKTURA V ČESKÉ REPUBLICE A JEJÍ SROVNÁNÍ S EVROPSKOU UNIÍ 64

4 SROVNÁNÍ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A NA SLOVENSKU 69
4.1 Metoda Check listu a její aplikace na vybrané státy 69
4.2 Kritická infrastruktura v České republice 70
4.3 Kritická infrastruktura na Slovensku 73
ZÁVĚR 79
SEZNAM POUŽITÝCH ZKRATEK 82
SEZNAM TABULEK 85
SEZNAM PŘÍLOH 86
SEZNAM OBRÁZKŮ 87
SEZNAM POUŽITÉ LITERATURY A DALŠÍCH PRAMENŮ 88

ÚVOD

Hlavním úkolem vlády každého státu je zajištění rozvoje země a bezpečnosti občanů. Česká republika, stejně jako další vyspělé státy, se začala aktivně zabývat možným ohrožením obyvatelstva a zranitelností hospodářských subjektů, zabezpečením základních funkcí státu a zabezpečením základních životních potřeb obyvatelstva, a to zejména v krizových situacích. Ochranu životů, zdraví lidí, majetku, životního prostředí však není možné zajistit bez správného fungování systémů, které tvoří fyzické a kybernetické zázemí státu. V této souvislosti se na konci 90. let začalo v České republice hovořit o vytipování kritické infrastruktury.

Hlavním cílem diplomové práce je popsat, analyzovat a porovnat ochranu kritické infrastruktury České republiky a vybraných zemí Evropské unie. Jedna z nejstručnějších a nejúžeji pojatých definic uvádí, že infrastruktura je síť služeb, které podporují průmysl nebo průmyslovou společnost, jako jsou cesty, komunikace nebo služby (voda, plyn, elektřina apod.)[1]. Pro plynulé zajištění fungování základních životně důležitých potřeb je nutné vymezit tu infrastrukturu, která je životně důležitá neboli kritická, a bez které by nebylo možné zabezpečit bezproblémové fungování státu. Pojem kritická infrastruktura (v pojetí Evropské unie) zahrnuje fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít vážný dopad na zdraví, bezpečnost anebo hospodářskou prosperitu obyvatelstva nebo efektivní funkcí vlády. Tuto kritickou infrastrukturu je potřeba adekvátně chránit, posilovat ji a starat se o její spolehlivý chod, neboť infrastruktura vyspělých států je vysoce zranitelná a navzájem velmi propojená.

Kritická infrastruktura je mezinárodní fenomén a útok na kterýkoliv stát může mít za následek zničení infrastruktur v širokém geografickém rozsahu. Je proto nezbytné zabezpečit fungování kritických infrastruktur autonomně, na úrovni jednotlivých národních států, nicméně s ohledem na právě výše uvedenou propojenost. V dnešní globální společnosti je také potřebné zabezpečit, aby jednotlivé státy při ochraně kritických infrastruktur, právě z důvodu

[1] LAMMING, R., BESSANT, J. *Macmillanův slovník podnikání a managementu*. Praha : Management Press, 1995. 296 s. ISBN 80-85603-47-0.

vzájemné zranitelnosti a propojenosti, spolupracovali. Evropská unie upravuje tuto oblasti řadou dílčích směrnic a členské státy si je v rámci své národní legislativy implementují. Každý stát si volí vlastní způsob a rozsah implementace, a cílem této diplomové práce je porovnat, jak Česká republika přejímá oblast ochrany kritické infrastruktury z evropské legislativy.

Dosavadní práce se většinou zaměřovaly na poskytování obecných informací z oblasti kritické infrastruktury, ale žádná z nich neposkytovala ucelený přehled kritických sektorů jednotlivých států Evropské unie a vyspělých zemí světa. To je také důvodem, proč převážná část druhé kapitoly byla přeložena z cizojazyčných odborných textů týkajících se dané problematiky.

Pro naplnění stanoveného cíle jsou v diplomové práci použity tyto obecné vědecké metody zkoumání: metoda deskripce, metoda komparace, metoda analýzy a syntézy. Uvedené metody nebyly aplikovány izolovaně, nýbrž ve vzájemné souvislosti a podmíněnosti. Metoda deskripce byla použita zejména při popisu kritických sektorů ve vybraných zemích Evropské unie a v dalších vyspělých zemích světa. Na základě provedené deskripce byla následně využita metoda komparace, kdy kritické sektory jednotlivých zemí byly srovnány a poté vytýčeny ty nejzranitelnější. V další části diplomové práce byla využita metoda komparace při provádění srovnání oblastí, produktů nebo služeb kritické infrastruktury České republiky s oblastmi a dílčími odvětvími, jež jsou označovány jako kritické v Evropské Unii. Informace získané při tomto srovnání byly analyzovány a odlišnosti v jednotlivých oblastech pak vymezeny. V diplomové práci byla dále použita tzv. metoda check listu neboli kontrolního seznamu. Tato metoda byla použita při srovnání postavení České republiky se Slovenskem. Metoda je zde rozpracována pouze ve své jednoduché formě, kdy na základě vydefinovaných otázek bylo provedeno hodnocení postavení vybrané země v procesu ochrany kritické infrastruktury.

1 ANALÝZA SOUČASNÉHO STAVU

Základní funkcí státu je zajistit ochranu a rozvoj chráněných zájmů a trvale udržitelný rozvoj lidské společnosti. Nejvyšší právní dokument ČR[2] deklaruje, že chráněnými zájmy jsou cíle státu, jež jsou prioritně ochraňovány, tedy životy a zdraví lidí, majetek, životní prostředí a bezpečnost. Právě bezpečnost je stále více zdůrazňována, a proto se hledají nástroje a prostředky pro její zajištění. Rovněž i hlavním cílem mezinárodních organizací, jako jsou např. Organizace spojených národů (OSN) či Evropská unie (EU), vlád a veřejné správy je zajištění bezpečného prostoru pro 21. století[3].

Zajištění bezpečnosti státu, fungování ekonomiky, fungování veřejné správy a zabezpečení základních životních potřeb obyvatelstva je závislé na konkrétních infrastrukturách, které jsou označovány jako kritické infrastruktury (KI). O kritické infrastruktuře se začalo hovořit na konci 90. let, kdy byly vytipovány systémy tvořící fyzické a kybernetické zázemí státu, bez jejichž správné funkce nelze provádět ani ochranu životů a zdraví lidí, majetku, životního prostředí, ani zvládnout dopady pohrom a útoků a zajistit obnovu a další rozvoj[4].

Aby stát mohl zajistit výše uvedené funkce za všech okolností, jak za „normálních“ tak i kritických podmínek, musí mít k dispozici prvky, vazby a toky systému státu, které jsou základem schopnosti státu dosáhnout za každé situace stability a nastartovat další rozvoj. Zájmem je zejména[5]:

- snížení zranitelnosti,
- ochrana lidí a kritických zdrojů a systémů, na nichž závisí existence společnosti,
- vytvoření podmínek pro prevenci a zajištění připravenosti na zvládání narušení kritické infrastruktury jako součástí programu rozvoje území,

---

[2] Ústavní zákon č. 1 ze dne 16. prosince 1992, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 1992.

[3] PROCHÁZKOVÁ, Dana. Komplexní pohled na problematiku bezpečnosti. *Veřejná správa* [on-line]. 2004, č. 35 [cit. 2008-10-11]. Dostupný z WWW: <http://aplikace.mvcr.cz /archiv2008/2003/casopisy/vs/0435/konz_info.html>.

[4] PROCHÁZKOVÁ, Dana. Podklady pro ochranu kritické infrastruktury. In *Sborník 2. Mezinárodní konference Krizový management*. Brno, 2004. 286-306. ISBN 80-85960-71-0.

[5] MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva.* 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html>.

- zabezpečení práv občanů na spravedlivou pomoc v případě narušení KI a zajištění jejich informovanosti o připravených opatřeních k řešení krizové situace, o jejich odpovědnosti, o tom jak mohou pomoci v prevenci a jak by měli reagovat na vzniklou situaci.

Smyslem ochrany KI musí být minimalizace dopadů výpadku činnosti infrastruktur tak, aby narušení funkcí, činností nebo služeb bylo krátkodobé, málo četné, zvladatelné alespoň provizorním způsobem, územně omezené a aby postihlo co nejmenší počet obyvatel[6].

Kritická infrastruktura je vymezena jako ta část infrastruktury ve státě, která má rozhodující význam pro jeho chod. Ochrana KI se vyvíjí a mění se také priority. Dneska jsou aktuálními zejména hrozba teroristických útoků, ohrožení živelními pohromami a hrozba jaderného napadení[7]. Dostupné prameny uvádějí ještě tyto možné hrozby[8]:

- pandemie,
- spontánní sociální nepokoje,
- stávky,
- avantýry (black-outy),
- organizované ohrožení bezpečnosti,
- vojenské napadení.

Zvláštní zranitelnost je dána zejména vlivem domino efektů a kaskádových efektů, přílišnou složitosti systému a upuštění od zálohování[9].

Samostatná strategie ochrany kritické infrastruktury by se měla zabývat také způsoby prosazování zabezpečení a zásadami řešení jejího narušení. Jde o stanovení strategických směrů k zajištění minimalizace dopadů narušení KI, včetně stanovení místa a úlohy veřejných

---

[6] Vláda ČR. Usnesení vlády ze dne 25. února 2008 č. 165 k Vyhodnocení stavu realizace Koncepce ochrany obyvatelstva do roku 2006 s výhledem do roku 2015 a o Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020. Praha, 2008.

[7] ADAMEC, Vilém. Ochrana kritické infrastruktury v ČR. In *Sborník 4. Mezinárodní konference*. Brno : VIO UO, 2006, ISBN 80-7231-141-7.

[8] SCHNEIDER, Jan. *Zpravodajské služby a ochrana kritické infrastruktury* [on-line].[cit. 2008-10-10]. Dostupné na WWW: <http://www.bezpecnostnimanagement.cz/www/files/File/anotace/2D/Terorismus,%20krizove%20rizeni/ANOT_Jan_Schneider.pdf>.

[9] KOCH, Monika. Národní strategie ochrany kritických infrastruktur. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukturen,* konference 2.-3.10.2006.[CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

institucí a i výrobců či poskytovatelů služeb pro obyvatelstvo. Současně je potřebné řešit zásady spolupráce a vzájemné vztahy mezi státním a soukromým sektorem, jako nezbytnou podmínkou pro komplexní řešení problému.

1.1 Vývoj kritické infrastruktury na jednotlivých úrovních

Všeobecná shoda o strategickém významu KI určuje potřebu jednoznačně definovat tuto kategorii v mezinárodním měřítku. Analýzou dostupných dokumentů je však možné zjistit odlišnosti ve vnímání KI na federální úrovni USA, na úrovni EU a NATO a na národních úrovních[10]. V následujících kapitolách je popsán vývoj KI ve Spojených státech amerických, EU, České republice a na úrovni Severoatlantické alianci.

1.1.1 Vývoj kritické infrastruktury v USA

USA a Austrálie jsou prvními státy, které začaly vnímat potenciál a šíři problematiky KI. Právě tyto dva státy začaly diskutovat nad zranitelnosti životní infrastruktury, později označované jako kritická infrastruktura. Prvotním materiálem, který se zaměřoval na ochranu KI, byla tzv. Bílá kniha. Jde o směrnici 63 vydanou v roce 1998 jako prezidentské rozhodnutí, jejímž záměrem bylo přijetí nezbytných opatření k rychlé eliminaci zranitelnosti, a to z hlediska hmotných a kybernetických útoků na kritickou infrastrukturu[11].

V době vydání byl větší důraz přikládán možným útokům na kybernetické systémy. Bílá kniha pojímá KI jako základní systémy, které mají hmotnou a kybernetickou základnu a mají vliv na funkčnost ekonomiky a státu. Tyto systémy zahrnují oblasti telekomunikace, bankovní a finanční sektor, energie, dopravu, zásobování vodou a záchranné služby[12].

Po teroristickém útoku na World Trade Centre v New Yorku, k němuž došlo 11. září 2001, nabývají otázky ochrany kritické infrastruktury nový rozměr. V roce 2001 je vydáno „Vládní

---

[10] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj* [on-line]. 2007, roč. 10, č. 4 [cit. 2008-09-28]. Dostupný z WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.

[11] The White House. Presidental Decision Directive 63 [on-line]. 1998 [cit. 2008-09-28]. Dostupný z WWW: <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

[12] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva*. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.

nařízení na ochranu kritické infrastruktury“[13], jehož cílem je zabezpečit ochranu informačních systémů (IS) pro KI, včetně nouzové komunikační připravenosti a ochrany hmotných zařízení, které IS podporují. V roce 2003 byla vydána „Národní strategie vnitřní bezpečnosti“[14], kde je mimo jiné uvedena tato definice KI: „Systémy a zařízení, jak hmotné tak virtuální, které jsou životně důležité pro USA a zneschopnění nebo zničení takových systémů nebo zařízení by mělo vliv na snížení bezpečnosti, národní ekonomické bezpečnosti, národního veřejného zdraví nebo bezpečí, nebo na jakoukoliv jejich kombinaci“[15]. V roce 2003 byla pak také vydána „Národní strategie fyzické ochrany kritické infrastruktury a klíčových zařízení“[16], která je v současnosti nejkomplexnějším materiálem ve světě zabývající se problematikou KI[17]. Tato strategie formuluje politiku státu a zdůrazňuje, že ochrana KI a klíčových zařízení je v USA považována za jádro vnitřní bezpečnosti[18]. Uvedená strategie rozpracovává zabezpečení kritické infrastruktury v jedenácti sektorech (příloha A) a ochranu klíčových zařízení v pěti sektorech (příloha B)[19]. Strategie je považována za „systém o systémech“ a mimo jiné uvádí, že úsilí státních orgánu při ochraně kritické infrastruktury a klíčových zařízení zahrnuje vytváření takové politiky a prostředí, které podmiňuje a vyvolává aktivní přístup jak státní administrativy, tak i soukromého sektoru a občanů USA[20].

1.1.2 Vývoj kritické infrastruktury v Evropě

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[21], jehož úkolem bylo rozvíjet a koordinovat činnost k ochraně kritické národní infrastruktury. Byly identifikovány systémy, jejichž kontinuita je důležitá pro fungování státu,

---

[13] Executive Order on Critical Infrastructure Protection.
[14] The National Strategy for Homeland Security.
[15] The USA Patriot Act. Public Law 107-56. 2001. [on-line]. Electronic Privacy Information Centre. [cit. 2008-10-07]. Dostupné z WWW: <http://www.epic.org/privacy/terrorism/ usapatriot>.
[16] The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets
[17] MOTEFF, John, PARFOMAK, Paul. Critical Infrastructure and Key Assets: Definition and Identification. Congressional Research Service. 2004, 19 p.
[18] COLLINS, Pamela. *Critical Infrastructure and Continuity of Operations in a post 9/11 World.* [cit. 2009-02-17]. Dostupné z WWW: <http://www.jsc.eku.edu/docs/Finland-Infrastructure%20Protection%20%20 Presentation.ppt>.
[19] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva*. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.
[20] KRULÍK, O. *Fyzická ochrana kritické infrastruktury a klíčových aktivit* [on-line]. Dostupný z WWW: <http: //www.mvcr.cz/rs_atlantic/data/files/insp_usa_infra.pdf>
[21] National Infrastructure Security Coordination Centre

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.

V EU je ochrana KI stále v procesu utváření se jednotlivých legislativních norem. V žádné členské zemi EU neexistuje zákon, který by upravoval výlučně problematiku ochrany KI, resp. pokud existuje, není autorce znám. V EU je ochrana KI upravena dílčími směrnicemi a sděleními. Již v roce 2004 bylo vydáno první sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“[22]. Sdělení obsahuje přehled opatření, která jsou prováděna v oblasti ochrany KI, a navrhuje další opatření pro posílení stávajících nástrojů a splnění uložených úkolů. Jsou zde vymezeny pojmy hrozba a evropská kritická infrastruktura, stanoveny oblasti KI, faktory pro určování potenciální KI a oblast řízení bezpečnosti. Směrnice upozorňuje na to, že každé odvětví a členský stát si musí v rámci své příslušné oblasti působnosti a v souladu s harmonizovaným postupem EU určit infrastrukturu, která je pro něj kritická a určit organizace nebo osoby odpovědné za bezpečnost. Dále je ve sdělení pojednáno o dosavadních pokrocích při ochraně kritických infrastruktur na úrovni Společenství a uvedena další očekávaná zlepšení a rozšíření opatření zejména po útocích ve Spojených státech amerických a Evropě. Na závěr je v dokumentu pojednáno o zvyšování schopnosti EU chránit KI. Za tímto účelem bude vytvořen Evropský program na ochranu kritických infrastruktur (EPCIP) a vybudována Výstražná informační síť kritické infrastruktury (CIWIN).

Dalším materiálem v oblasti ochrany KI je „Zelená kniha o Evropském programu na ochranu kritické infrastruktury“[23] vydaná v roce 2005. Evropská unie se prostřednictvím tohoto

---

[22] Komise. Sdělení Komise Radě a Evropskému parlamentu. Ochrana kritické infrastruktury při boji proti terorismu. Brusel, 2004. KOM/2004/0702.

[23] Komise Evropských společenství. *Zelená kniha o Evropském programu na ochranu kritické infrastruktury*. Brusel, 2005.

dokumentu obrací na odborníky a laickou veřejnost za účelem získání konkrétních informací o politikách vhodných pro Evropský program pro ochranu kritické infrastruktury. Jednotlivé kapitoly Zelené knihy pojednávají o účelu a oblastech působnosti EPCIP. Dále jsou zde uvedeny základní principy a společný rámec EPCIP, definovány evropská kritická infrastruktura (ECI), národní kritická infrastruktura (NCI) a v neposlední řadě stanovena role vlastníků, provozovatelů a uživatelů KI a vymezena podpůrná opatření pro EPCIP. Hlavním cílem EPCIP je zajistit, aby v rámci celé EU existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany KI. Úroveň ochrany by neměla být stejná pro všechny KI, ale měla by být odvozená od dopadu, který by mohlo způsobit jejich případné selhání.

Dalším materiálem řešícím problematiku ochrany KI je „Sdělení komise o Evropském programu na ochranu kritické infrastruktury“[24] z roku 2006, obsahující zásady, postupy a nástroje s cílem zavést systém EPCIP. Obecným cílem navrhovaného programu je zlepšit ochranu KI v EU, kdy ochrana KI bude založena na principu stejného přístupu pro veškerá ohrožení s prioritním zaměřením na terorismus. V dokumentu je definována ECI a navržena opatření pro usnadnění rozvoje a provádění EPCIP. Je zde vymezena úloha akčního plánu EPCIP, CIWIN, skupiny odborníků, proces sdílení informací o ochraně kritických infrastruktur a určení vzájemných souvislostí. Dále je zde definována NCI, vymezeno plánování jako klíčový prvek procesu ochrany KI a stanovena doprovodná finanční opatření přispívající k provádění EPCIP.

V červenci 2007 bylo vydáno Evropským parlamentem ´“usnesení o návrhu směrnice Rady o určování a označování evropské kritické infrastruktury a o posouzení potřeby zvýšit její ochranu“[25]. Směrnice by měla obsahovat základní definice, kritéria pro určování a označování ECI, zásady zpracování plánů bezpečnosti provozovatelů evropské KI, úlohu styčných úředníků pro bezpečnost, možnost podpory evropské KI ze strany Evropské komise a další ustanovení.

---

[24] Komise Evropských společenství. *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury.* Brusel, 2006.
[25] Evropský parlament. *Usnesení Evropského parlamentu o určování a označování KI a o posouzení potřeby zvýšit její ochranu.* Brusel, 2007.

V EU mají odpovědnost za ochranu vnitrostátních KI jejich vlastníci, provozovatelé a členské státy. Za účelem zlepšení ochrany vnitrostátních KI by měly všechny členské státy vytvořit vnitrostátní program na ochranu KI. Tyto programy by se měly zabývat zejména uvedenými otázkami:[26]

- Určení a vytvoření vnitrostátních KI členským státem podle předem definovaných vnitrostátních kritérií. Kritéria výběru by měla být založena na odborných poznatcích s přihlédnutím k rozsahu, závažnosti a časovému faktoru. Pro určení subjektů KI je třeba posoudit zejména: *Rozsah* – zde by se ztráta prvku KI hodnotila podle velikosti zeměpisné oblasti, která by mohla být ztrátou nebo nedostupností postižena. Rozlišovala by se přitom vnitrostátní, mezinárodní, regionální nebo místí KI. *Závažnost* – stupeň dopadu nebo ztráty funkce může být hodnocen jako žádný, minimální, mírný nebo velký. Mezi kritéria, která lze použit pro hodnocení velikosti, patří zejména veřejný dopad, hospodářský dopad, dopad na životní prostředí, politický dopad, psychologický dopad a dopad na veřejné zdraví. *Časové faktory* – závažnost dopadů na jednotlivé subjekty v závislosti na čase, tj. okamžitě, za 24 hod., 48 hod., za týden, později. Na základě uvedených kritérií je možné v každé oblasti a na úrovni státu stanovit, které subjekty budou patřit mezi KI;[27]
- Zahájení dialogu s vlastníky/provozovateli KI;
- Určení vzájemných zeměpisných a odvětvových závislostí;
- Vytváření případných krizových plánů souvisejících s vnitrostátními KI;

Doporučuje se, aby každý členský stát založil svůj program na ochranu KI na společném seznamu odvětví KI vytvořeném pro evropské KI.

Při provádění EPCIP budou uplatňování tyto zásady (často označované jako principy):[28]

- *Subsidiarita*. Komise bude zaměřovat své úsilí na infrastrukturu, která je kritická spíše z evropského než vnitrostátního či regionálního pohledu, odpovědnost bude položena především na národní úroveň.

---

[26] Komise Evropských společenství. *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury.* Brusel, 2006.
[27] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj* [on-line]. 2007, roč. 10, č. 4 [cit. 2008-09-28]. Dostupný z WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.
[28] Komise Evropských společenství. *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury. Brusel, 2006.*

- *Spolupráce zainteresovaných subjektů*. Všechny příslušné zainteresované subjekty se v rámci svých možností zapojí do rozvoje a provádění EPCIP. To bude zahrnovat vlastníky/provozovatele KI označených jako evropské KI a také státní či další příslušné orgány.
- *Důvěrnost*. Informace o ochraně KI jak na úrovni EU, tak na úrovni členských států budou utajovány a přístup k nim bude povolen jen v případech potřeby.
- *Proporcionalita*. Nelze chránit vše, proto opatření budou navržena pouze tam, kde byla na základě analýzy stávajících nedostatků v oblasti bezpečnosti zjištěna jejich potřebnost, a tato opatření budou úměrná úrovni a druhu daného ohrožení.
- *Odvětvový přístup*. Různá odvětví mají odlišné zkušenosti, odborné znalosti a požadavky týkající se ochrany KI. EPCIP bude rozvíjen a prováděn podle dohodnutého sezamu odvětví ochrany KI.
- *Doplňkovost*. Komise se vyvaruje zdvojování stávajícího úsilí, na úrovni EU i vnitrostátní či regionální úrovni, pokud je toto úsilí při ochraně KI prokazatelně efektivní. EPCIP bude tedy navazovat na existující odvětvová opatření a doplňovat je.

Komise vydala v roce 2007 studii „Definice kritické infrastruktury na úrovni EU v sektoru energetiky“, která analyzuje evropskou energetickou infrastrukturu (pro oblast ropných produktů, elektřiny a plynu). Studie zkoumá účinky narušení vzniklé v tomto sektoru a možné dopady, a to jak pro zemi samotnou, tak také pro sousední státy. Dále studie obsahuje posouzení zranitelnosti nejvíce kritických sektorů a vymezuje značnou část technických problémů v oblasti bezpečnostních opatření a aspektu spolehlivosti [29].

V současné době plánuje Evropská unie zvýšit ochranu tzv. kritické informační infrastruktury (Critical Information Infrastructure – CII) s cílem zajistit řádnou funkčnost kritické infrastruktury. Pod pojmem CII se označují telekomunikace, počítačové systémy (včetně programového vybavení), Internet, přenosové sítě aj. V dnešní době hraje důležitou komponentu zejména Internet, a to kvůli jeho značnému rozšíření. V této oblasti je Komisí

[29] *Energy infrastructure: Studies* [on-line]. [cit. 2009-04-20]. Dostupné na WWW: <http://ec.europa.eu/energy/infrastructure/critical_en.htm>.

připravován materiál „Ochrana Evropy před velkou škálou kybernetických útoků a narušení: zvýšení připravenosti, bezpečnosti a odolnosti“[30].

1.1.3 Vývoj kritické infrastruktury v České republice

V bývalém Československu fungoval do roku 1989 systém zvyšování odolnosti národního hospodářství směřovaný na přípravu činnosti za války. S postupem času se začala měnit struktura tohoto systému. 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 přijetí tzv. krizových zákonů v roce 2000, což mimo jiné vedlo k budování integrovaného záchranného systému ČR (IZS ČR). Problematika ochrany obyvatelstva začala být začleňována do mezinárodních struktur, a to jak do NATO, tak i do EU. V ČR se prvotní činnosti v rámci KI orientovaly na ochranu počítačových sítí, kdy na základě usnesení[31] byl Úřadem pro veřejné informační systémy zpracován projekt „Strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě“.

V roce 2001 Výbor pro civilní nouzové plánování (VCNP) a Bezpečnostní rada státu (BRS) projednali usnesení [32] s názvem „Definice a rozsah základních funkcí státu“, který se jako první oficiální vládní dokument zabýval základními funkcemi státu v případě mimořádných nebo krizových situací nevojenského charakteru. Provedená analýza odezvy na povodně v letech 1997 a 1998 a analýzy zahraniční literatury týkající se odezvy na živelní a jiné pohromy, vedly ke zpracování materiálu, který se týkal ochrany KI[33].

---

[30] Komise Evropských společenství. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Brusel, 2009.
[31] Vláda ČR. Usnesení ze dne 5. října 2000 č. 123 Návrh strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě.
[32] Vláda ČR. Usnesení ze dne 24. června 2001 č. 105.
[33] DRYMLOVÁ, Veronika. *Plán znovuobnovení kritické infrastruktury na místní úrovni* [Diplomová práce]. České Budějovice : JU, 2008. 324 s. [on-line]. Dostupné z WWW: <http://theses.cz/id/4stg5a/>.

V roce 2002 projednal VCNP usnesení „Rozsah základních funkcí státu za krizových situací“ a materiál „Zpráva o národní kritické infrastruktuře“, kde bylo stanoveno zaměření národní kritické infrastruktury na tyto oblasti:[34]

- systém dodávky energií (především elektřiny),
- systém dodávky vody,
- systém odpadového hospodářství,
- přepravní síť,
- komunikační a informační systémy,
- bankovní a finanční sektor,
- nouzové služby (policie, hasičské záchranné sbory, zdravotnictví),
- veřejné služby (zásobování potravinami, sociální služby, pohřební služby),
- státní správa a samospráva.

V roce 2003 připravilo Ministerstvo vnitra pro schůzi VCNP materiál s názvem „Projekt Analýza zabezpečení základních funkcí státu včetně ochrany životně důležité infrastruktury v případě krizových situací“. Tento materiál představoval první ucelený a souhrnný přehled situace v jednotlivých odvětvích KI, včetně právních předpisů, první definice základních funkcí státu při krizových situacích a kritické infrastruktury. Předpokládané dopady a závěry byly přijaty formou usnesení[35]. Seznam subjektů KI na národní, regionální a místní úrovni byl schválen usnesením[36] VCNP. O rok později bylo stanoveno deset oblastí a čtyřicet dva produktů nebo služeb KI (tabulka 1), u nichž je předpokladem dobrého fungování tzv. partnerství veřejného a soukromého sektoru (PPP)[37].

Národní kritickou infrastrukturu ČR je možné chápat jako systém, jenž je tvořen dvěma úrovněmi:

- úrovní sektorů (oblastí),
- úrovní produktů a služeb.

---

[34] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva*. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.

[35] Vláda ČR. Usnesení ze dne 24. června, č. 173, Praha, 2003.

[36] Vláda ČR. Usnesení ze dne 23. září, č. 179, Praha, 2003.

[37] Z anglického Public Private Partnerships. Je-li PPP aplikován odborně, tak dochází ke zvýšení kvality a efektivnosti veřejných služeb včetně výkonu státní správy. Zároveň se s jeho pomocí urychluje realizace významných infrastrukturních projektů s pozitivním dopadem na rozvoj ekonomiky.

Jednotlivé prvky kritické infrastruktury na úrovni sektorů jsou někdy označovány jako oblasti, popř. odvětví kritické infrastruktury a na úrovni produktů jako segmenty kritické infrastruktury[38].

Tabulka 1: Oblasti kritické infrastruktury v České republice[39]

Poř.	Oblasti 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 a 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.	Zdravotní péče	4.1 Přednemocniční neodkladná péče
		4.2 Nemocniční péče
		4.3 Ochrana veřejného zdraví
		4.4 Distribuce léčiv
5.	Doprava	5.1 Silniční
		5.2 Železniční
		5.3 Letecká
		5.4 Vnitrozemská vodní
6.	Komunikační a informační systémy	6.1 Služby pevných komunikačních sítí
		6.2 Služby mobilních komunikačních sítí
		6.3 Radiová komunikace a navigace
		6.4 Satelitní komunikace
		6.5 Televizní a rádiové vysílání
		6.6 Přístup k internetu a k datovým službám
		6.7 Poštovní a kurýrní služby
7.	Bankovní a finanční sektor	7.1 Správa veřejných financí
		7.2 Bankovnictví
		7.3 Pojišťovnictví
		7.4 Kapitálový trh
8.	Nouzové služby	**8.1 Policie ČR jednotky požární ochrany**
		8.2 Hasičský záchranný sbor ČR
		8.3 Zdravotnické záchranné služby
		8.4 Letecká zdravotnická záchranná služba

[38] FUCHS, Pavel. Metodika pro hodnocení kritické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infreastrukturen,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[39] Tučně vyznačené produkty a služby budou dále diskutovány

		8.5 Armáda ČR
		8.6 Radiační monitorování
		8.7 Předpovědní, varovná a hlásná služba
9.	Veřejná správa	9.1 Sociální ochrana a zaměstnanost
		9.2 Diplomacie
		9.3 Výkon justice a vězeňství
		9.4 Státní správa a samospráva
10.	Odpadové hospodářství	**10.1 Nakládání s odpady**
		10.2 Radioaktivní odpady

Pramen: Výbor pro civilní nouzové plánování: usnesení č. 190 ze dne 23. 3. 2004

Reakcí ČR na přístup mezinárodních organizací, NATO a EU, k problematice řešení ochrany KI byl materiál s názvem „Zpráva o stavu řešení problematiky kritické infrastruktury" připravený VCNP. K tomuto materiálu bylo přijato usnesení[40], ve kterém byly porovnány kroky ČR a zahraničí v oblasti ochrany KI.

Dalším krokem v problematice KI bylo zpracování a projednání dokumentu „Zpráva o řešení problematiky kritické infrastruktury" projednaného VCNP jako usnesení[41]. V roce 2007 vláda schválila svým usnesením[42] „Směrnici k výběru objektů obranné infrastruktury a zpracování dokumentace". Tato směrnice s problematickou KI souvisí, neboť problematika obranné a kritické infrastruktury se často překrývají[43].

Součástí „Zprávy o řešení problematiky kritické infrastruktury v České republice", která se stala impulzem pro vypracování Komplexní strategie a následně Národního programu, byla podrobná analytická část, která se zabývala situací v jednotlivých oblastech kritické infrastruktury, a dále zde byl řešen stav této problematiky v ČR v obecné rovině[44].

[40] Vláda ČR. Usnesení ze dne 21. června, č. 222, Praha, 2006.
[41] Vláda ČR. Usnesení ze dne 21. března, č. 244, Praha, 2007.
[42] Vláda ČR. Usnesení ze dne 19. prosince, č. 1436, Praha, 2007.
[43] KLABAN, Vladimír. Kritická infrastruktura, možnosti jejího vymezení a stanovení potencionálních hrozeb. In *Problematika řešení mimořádných událostí a krizových situací v regionech*, konference 4.-5. 9. 2008. Univerzita Tomáše Bati ve Zlíně, 2008.
[44] MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva.* 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html>.

Vláda ČR v roce 2008 vydala svým usnesením[45] „Harmonogram dalšího postupu zpracování dokumentů Komplexní strategie ČR k řešení problematiky KI a Národní programu ochrany KI“. Dle Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020[46], přijaté v roce 2008 (dále jen Koncepce) by „Komplexní strategie České republiky k řešení problematiky ochrany KI“ měla představovat konsensuální rámec pro zpracování dalších koncepčních materiálů, které by ji rozvrhly do konkrétních kroků a následných opatření. Jedním z komplexních kroků by byl Národní program ochrany kritické infrastruktury, který by byl založen na zpracování dílčích strategií, koncepcí a analýz stanovených pro jednotlivé oblasti KI. Z nich by následně vycházely konkrétních úkoly, jejich nositelé a termíny plnění.

V současné době je vymezeno devět oblastí a třicet sedm produktů a služeb[47], jež jsou z hlediska fungování společnosti považovány za prioritní. Při porovnání s oblastmi KI uvedenými v tabulce 1 došlo ke změnám u položek, které jsou vyznačeny tučně. Pro oblast KI č. 4 *Zdravotní péče* došlo ke změně u produktu 4.4. *Distribuce léčiv.* Tato položka byla nahrazena *Výrobou, skladováním a distribuci léčiv a zdravotnických prostředků*. Oblast KI č. 8 *Nouzové služby* byla změněna a upřesněna dle tabulky č. 2 a oblast KI č. 10 *Odpadové hospodářství* již dále není považována za oblast KI.

Tabulka 2: Vymezení produktu a služeb pro oblast kritické infrastruktury Nouzové služby

Poř.	Oblasti KI	Produkt nebo služba
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 vč. Podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření
		8.7 Předpovědní, varovná a hlásná služba

Pramen: Usnesení BRS č. 30 ze dne 3. července 2007

[45] Vláda ČR. Usnesení ze dne 25. února č. 170 o Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury. Praha, 2008.
[46] Ministerstvo vnitra-generální ředitelství HZS ČR. Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020. Praha, 2008.
[47] Vláda ČR. Usnesení ze dne 3. července, č. 30, Praha, 2007.

Výše uvedená Koncepce řeší v kapitole 4.1.3 problematiku KI. Zároveň se tvoří systémy a opatření k zachování funkčnosti jednotlivých oblasti KI, připravuje se legislativní opora ochrany KI a již došlo k vytvoření:

- definice a pojmů KI (kap. 1.2.1),
- přehledů subjektů KI na národní, regionální a místní úrovni (kap. 1.2.2)
- Národní strategie informační bezpečnosti,
- krizových a typových plánů zahrnujících aspekty KI dle schválené metodiky,
- odborné pracovní skupiny pro koordinaci bezpečnostního výzkumu ustanovené v rámci Výboru pro civilní nouzové plánování.
- dále probíhá budování IS krizového řízení, došlo k vytvoření příspěvků k tvorbě Evropského programu pro ochranu KI a k návrhu směrnice o Evropské kritické infrastruktuře.

1.1.4 Kritická infrastruktura na úrovni Severoatlantické aliance

Výbor pro civilní ochranu Severoatlantické aliance projednal v roce 2003 informační zprávu, která je zaměřena na definování vzájemných závislostí jednotlivých prvků KI a ohodnocení těchto závislostí z pohledu zabezpečení rozhodujících činností v případě vzniku závažných mimořádných událostí. Zpráva pojednává o tzv. schopnosti státu reagovat na mimořádnou událost, resp. krizovou situaci a vytyčuje deset schopností, které by mohly ovlivňovat prvky KI:[48]

- centrální schopnost reakce,
- zásobování (doplňování) základních služeb,
- místní schopnost reakce,
- dekontaminace,
- místní očista,
- vakcinace a ošetřování,
- péče o hromadně zraněné,
- hromadná evakuace,
- zjišťování ohrožení a jejich pojmenování,
- informování, varování a vyrozumění veřejnosti.

[48] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj* [on-line]. 2007, roč. 10, č. 4 [cit. 2008-09-28]. Dostupný z WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.

Jednání výboru dospělo k závěru, že z výše uvedených schopností jsou nejvíce kritické hromadná evakuace a informování, varování a vyrozumění veřejností[49].

Členské a partnerské státy NATO se svými příspěvky omezily na zprávy o postupu jednotlivých států v uvedené oblasti. Přestože Iniciativa NATO stále trvá, budoucí postup NATO se bude směřovat na mezinárodní spolupráci v oblasti vzdělávání k dosažení potřebných znalostí z oblasti kritické infrastruktury účastníků z civilní i vojenské sféry[50].

V rámci Severoatlantické aliance je problematika kritické infrastruktury řešena Hlavním výborem civilního nouzového plánování NATO (Senior Civil Emergency Planning Committee – SCEPC) a jeho podvýbory. SPEPC pověřil podvýbory přezkoumáním všeobecných aspektů ochrany kritické infrastruktury a možných následků v případě jejího narušení. Podvýbory vypracovali dokumenty a studie, ve kterých se odkazují na to, že volba přístupu a celková implementace je v působnosti každého členského státu a členské státy NATO by se měly prioritně zaobírat touto problematikou[51].

V rámci NATO existuje pod hlavičkou Civilního a nouzového plánovaní program ochrany kritické infrastruktury, který se zaměřuje na ochranu funkčnosti, odolnosti a spolehlivosti této infrastruktury. Ochrana KI je jednou z klíčových oblastí Civilního nouzového plánování NATO ve spolupráci s Euroatlantickou radou partnerství. Hlavní filozofií NATO v této oblasti je sdílení informací nejen o možném ohrožení této infrastruktury, ale i způsobech její ochrany a případné obnovy[52].

Dílčí závěr

Nad zranitelnosti kritické infrastruktury začaly již v devadesátých letech jako první diskutovat USA a Austrálie. Začaly být vydávány strategické materiály zabývající se touto

---

[49] VALÁŠEK, Jarmil. Ochrana kritické infrastruktury. In *Sborník referátů 4. energetického kongresu ČR*. Praha, 2004.

[50] MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva.* 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html>.

[51] Ministerstvo vnitra SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2007. 24 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.

[52] DRYMLOVÁ, Veronika. *Plán znovuobnovení kritické infrastruktury na místní úrovni* [Diplomová práce]. České Budějovice : JU, 2008. 324 s. [on-line]. Dostupné z WWW: http://theses.cz/id/4stg5a/>.

problematikou, ve kterých byla např. formulována strategie zabezpečení kritické infrastruktury a požadována politika a prostředí, které bude podmiňovat aktivní přístup nejen státní administrativy, ale i soukromého sektoru. Z evropských zemí se začala otázkami KI jako první země zabývat Velká Británie. Postupně se přidávaly další státy jako je např. Německo a Nizozemí. Kritická infrastruktura je na jednotlivých úrovních pojímána odlišně. Pro potřeby EU byla vymezena evropská kritická infrastruktura, avšak každý členský stát EU si musí v rámci své oblasti působnosti určit infrastrukturu, která je pro něj kritická. V ČR začaly být vydávány materiály související s problematikou ochrany KI od roku 2001. Od té doby byla přijata řada usnesení, ve kterých došlo k ustanovení oblastí KI. Při jejich vymezování byl vzat v úvahu požadavek, aby národní KI byla v identická nebo alespoň ve stěžejních částech stejná jako evropská KI.

1.2 Explikace základních pojmů v oblasti kritické infrastruktury

Jak již bylo výše uvedeno, v ČR není doposud pojem kritická infrastruktura a problematika její ochrany legislativně upravena, tzn., že není schválen žádný zákon přímo upravující ochranu kritické infrastruktury. Zároveň také nejsou stanoveny právně závazné zásady pro výběr objektů a subjektů KI, jejich kompetence a povinnosti.

Pro legislativní účely bude nutno definovat pojem KI, což by mělo probíhat systematicky. V první fázi bude lepší výměr KI předimenzovat, než něco pominout. V druhé fázi musí nastat razantní redukce, vedená ekonomickými aspekty. Tak by mělo být vymezeno skutečně nezbytné minimum, protože ochrana KI musí být ekonomicky realizovatelná. Pro zajištění vyšší spolehlivosti a odolnosti KI je nutné v rámci jejího vymezení a definování stanovit strukturální součásti, klíčové objekty a jejich prvky. Těmi jsou takové součásti KI, jejichž vyřazení může ovlivnit funkčnost a spolehlivost KI jako celku a jejichž nahrazení nebo uvedení do původního stavu je spojeno s obtížemi a komplikacemi.

K ochraně KI lze v našich podmínkách nejlépe využit systém krizového řízení vycházejícího z krizového zákona[53], který řeší problematiku ochrany obyvatelstva. Základní východiska pro

[53] Ministerstvo vnitra ČR. Zákon č. 240 ze dne 28. června 200 o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. Praha, 2000.

stanovení právního rámce jsou vymezena ústavním pořádkem, kdy veřejná moc může ukládat fyzickým a právnickým osobám povinnosti pouze na základě a v mezích zákona[54].

Má-li veřejná moc, ať je to stát, samospráva nebo orgány a instituce EU, zájem prosadit jakákoliv opatření, je nutné předem analyzovat potřeby, definovat práva a povinnosti a ty pak také efektivně vynucovat. Dále musí veřejná moc shromažďovat a poskytovat potřebné informace a všechny uvedené činnosti materiálně, personálně a finančně zajistit. Je možné říct, že ve vztahu k vlastníkům a provozovatelům se uplatňují zejména dva principy. Prvním z nich je nedotknutelnost vlastnictví a jeho ochrana a na druhé straně stojí veřejný zájem, který vlastnická práva omezuje. Vlastníci a provozovatelé nemohou očekávat, že stát bude jejich majetek prioritně chránit a zajišťovat ho sám a výlučně z veřejných prostředků. Tímto způsobem by totiž docházelo k znevýhodňování ostatních skupin vlastníků.

Důležitou otázkou při řešení ochrany KI je její financování. Bude žádoucí, aby se na financování ochrany KI podílely dotčené subjekty, kterými jsou zejména domácí a zahraniční vlastníci a provozovatelé, veřejná moc, orgány a instituce EU a pojišťovny. Je ale také nutno stanovit kdo a jakým způsobem bude hradit náklady spojené se zvýšením odolnosti a bezpečnosti infrastruktury unijního významu za jakou jsou považovány např. strategické plynovody, ropovody, hlavní rozvody elektrické energie a jaderné elektrárny[55].

1.2.1 Vymezení pojmů infrastruktura a ochrana kritické infrastruktury

Jedna z nejstručnějších a nejúžeji pojatých definic uvádí, že *infrastruktura* je síť služeb, které podporují průmysl nebo průmyslovou společnost, jako jsou cesty, komunikace nebo služby (voda, plyn, elektřina apod.)[56].

Jiná definice uvedená ve Velké ekonomické encyklopedii[57] pracuje s pojetím infrastruktury, která zahrnuje materiální a nemateriální charakteristiky ekonomiky financované z veřejných

---

[54] Česká národní rada. Ústavní zákon č. 1 ze dne 16. prosince 1992, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. Praha, 1992.
[55] KLABAN, Vladimír. Kritická infrastruktura, možnosti jejího vymezení a stanovení potencionálních hrozeb. In *Problematika řešení mimořádných událostí a krizových situací v regionech*, konference 4. - 5. 9. 2008. Univerzita Tomáše Bati ve Zlíně, 2008.
[56] LAMMING, R., BESSANT, J. *Macmillanův slovník podnikání a managementu*. Praha : Management Press, 1995. 296 s. ISBN 80-85603-47-0.
[57] ŽÁK, M. *Velká ekonomická encyklopedie*. 2. vyd. Praha : Linde, 2002. 888 s. ISBN 80-7201-381-5.

zdrojů zvyšující produktivitu soukromého sektoru. Materiální infrastruktura představuje např. dopravní, energetické a vodní sítě a nemateriální infrastruktura v sobě zahrnuje např. systém ochrany vlastnických práv či vzdělávací systém.

V České republice je v systému krizového řízení vymezen pojem infrastruktura v systému hospodářských opatření pro krizové stavy[58], kde se infrastrukturou k přípravě a přijetí hospodářských opatření pro krizové stavy rozumí:

- stavby určené pro účely hospodářských opatření pro krizové stavy ve vlastnictví ČR, k nimž má právo hospodaření správní úřad,
- stavby sloužící pro účely hospodářských opatření pro krizové stavy, k nimž má ČR zřízeno břemeno a které jsou ve vlastnictví právních nebo podnikajících fyzických osob,
- technické zabezpečení staveb podle první odrážky vnitřními rozvody inženýrských a telekomunikačních sítí, počínaje přípojkou k veřejnému rozvodu těchto sítí,
- technologické vybavení staveb podle první odrážky,
- pozemní komunikace, dráhy, přístavy a letiště, sloužící pro dopravní obsluhu staveb podle první odrážky.

Pojmy kritická infrastruktura a obranná infrastruktura vnímá široká veřejnost jako vzájemně zastupitelné, avšak jejich skutečný význam je odlišný. V oblasti ochrany *kritické infrastruktury* jde o ochranu státu z vnitřního pohledu, zatímco *obraná infrastruktura* se zabývá ochranou státu z vnějšího pohledu, resp. vojenského[59]. Kritická infrastruktura řeší hlavní prvky systému státu, a pokud jeden z nich selže tak se to negativně odrazí na straně zbylých prvků.

Z hlediska resortního je možné rozčlenit infrastrukturu na bezpečnostní a obrannou. *Bezpečnostní infrastruktura* je vymezena jako soubor nemovitých i strategických movitých objektů, pozemků, zařízení a jejich vybavení, určených pro řízení a zabezpečení

[58] Ministerstvo vnitra ČR. Zákon č. 241 ze dne 29. června 2000 o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů. In *Sbírka zákonů České republiky*. Praha, 2000.
[59] MALANÍK, Luboš. *Ochrana kritické infrastruktury České republiky*. [Diplomová práce]. Zlín, 2008. 115 s. [on-line]. Univerzita Tomáše Bati ve Zlíně. Dostupné z WWW: < http://theses.cz/id/qlhx9p/>.

bezpečnostních složek, pro jejich operační rozvinutí při zabezpečování standardních operačních postupů a plánů[60].

Obranná infrastruktura je vymezena jako soubor stacionárních objektů, pozemků a zařízení určených pro řízení a zabezpečení ozbrojených sil, jejich mobilizační rozvinutí a pro zabezpečení operačních plánů. Jedná se zejména o:[61]

- objekty a zařízení alianční infrastruktury na území ČR,
- objekty důležité pro obranu státu a jejich příslušenství,
- pozemní komunikace,
- železnice,
- letiště,
- telekomunikační zařízení,
- produktovody,
- provozní zařízení a vybavení, které je předurčeno k zajištění obrany státu,
- nemovité věci ve vlastnictví státu, právnických a fyzických osob, určené jako prostředky k zajištění státu.

Obrannou infrastrukturu je možné členit ze dvou hledisek:

- z hlediska působnosti,
- z hlediska aliančního předurčení a působnosti.

Obranná infrastruktura se z hlediska působnosti člení na *vojenskou* a *nevojenskou obrannou* infrastrukturu. Nevojenská obranná infrastruktura je charakterizována jako vymezená část obranné infrastruktury v působnosti jednotlivých ministerstev.

Z hlediska aliančního předurčení a působnosti se může obranná infrastruktura členit na *národní obrannou* a *vojenskou* infrastrukturu. Národní obranná infrastruktura je určená část hospodářské infrastruktury. Je budována a financována příslušným státem výhradně pro

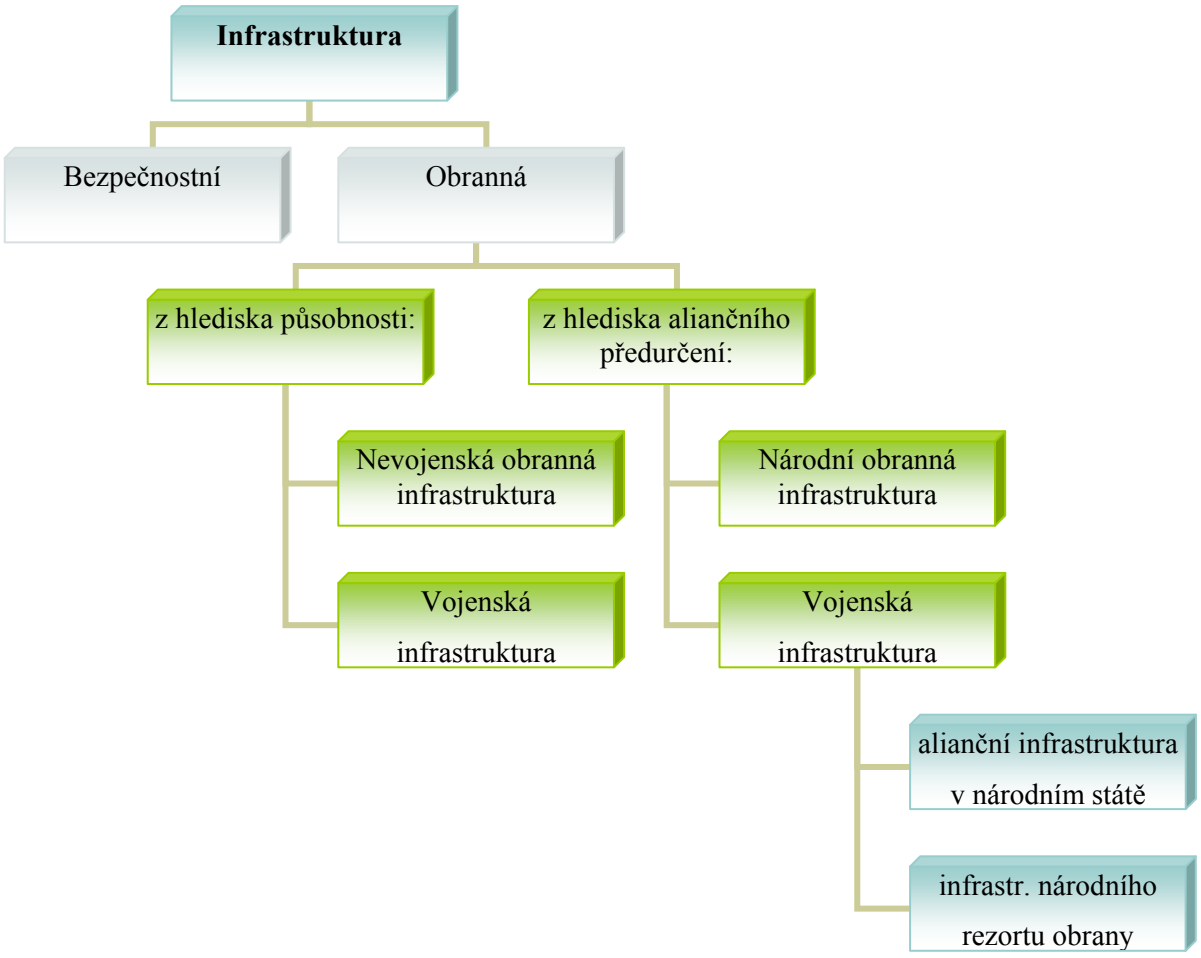
---

[60] URBÁNEK, Jiří. F. Nové hodnocení kritické infrastruktury z hlediska AČR. In *Sborník IV. Konference s mezinárodní účastí Instituce a zařízení regionu v systému ochrany obyvatelstva*. Brno, 2006. 212-217 s. ISBN 80-7231-175-1.

[61] URBÁNEK, Jiří. F., KELLNER, Josef, NAVRÁTIL, Josef. Úloha Univerzity obrany při ochraně kybernetické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukture,*konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

využívání vlastními ozbrojenými silami včetně sil předurčených do NATO, zatímco vojenská infrastruktura zahrnuje i nemovitosti pro operační přípravu státního území, včetně pozemků, se kterými hospodaří národní resort obrany. V členských státech NATO je vojenská infrastruktura tvořena nejen *infrastrukturou národního resortu obrany*, ale také *aliančí infrastrukturou v národním státě*, která je specifikována jako souhrn objektů a zařízení zapsaných v inventáři NATO. Dále je v obrázku 1 znázorněno a vymezeno základní členění infrastruktury.

Obrázek 1: Základní členění infrastruktury státu



Pramen: autorka dle URBÁNEK, Jiří. F. KELLNER, Josef, NAVRÁTIL, Josef. Úloha Univerzity obrany při ochraně kybernetické infrastruktury. In Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukture, konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

Infrastruktura státu se skládá z prvků, které samy o sobě jsou systémy s dalšími prvky[62]. Kritická infrastruktura v jednotlivých státech nejčastěji zahrnuje:

- energetické systémy,
- systémy zásobování vodou a potravinami,
- bankovní a finanční sféru,
- dopravní systém a logistiku,
- informační a komunikační systémy,
- systém veřejné správy.

Česká republika nemá pojem kritická infrastruktura v zákonných ani v podzákonných normách definován, proto při vymezování oblastí KI a následně produktů a služeb je možné postupovat tak, že nejprve dojde k vymezení souhrnu ucelených oblastí infrastruktury, které jsou považovány za kritické (např. energetika, doprava). Při vymezování se řídit definicí KI, kterou navrhla odborná pracovní skupina kritické infrastruktury a schválila Bezpečnostní rada státu. Kritickou infrastrukturou podle této definice rozumí „výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu, zabezpečení základních životních potřeb obyvatelstva a další oblasti nezbytné pro zachování základních funkcí státu“[63]. Následně se pak vymezují strukturální součásti KI (např. jaderná energetika) a její podsoučásti (JE Temelín). Pro efektivní postup je nezbytné stanovit klíčové prvky strukturální podsoučásti KI. Klíčovým prvkem se rozumí „objekt, jehož zničení, vyřazení či ochromení jako celku je reálné a vede k významnému omezení dané strukturální součásti KI“. Vyřazení podsoučásti JE Temelín z provozu je možné, ale stěží lze realizovat totální vyřazení tohoto celku. Vyřazení JE Temelín z provozu lze do určité míry nahradit z jiných zdrojů, tak aby nedošlo k závažným dopadům.

Při rozhodování o prioritách zvyšování odolnosti infrastruktury hraje významnou roli otázka důležitosti příslušné oblasti KI. A jak stanovit, která oblast je důležitější? To záleží na mnoha podmínkách, zejména to tom, zda je mírová situace nebo válečný stav, a následně na tom, na jaké úrovni oblasti KI řešíme, zda na úrovni státu, kraje nebo obce. Významným rysem

---

[62] PERNICA, P. *Logistický management – teorie a podniková praxe*. Praha: Radix. 1998. ISBN 80-8603113-6.
[63] Informace o dokumentech z bezpečnostní oblasti projednávaných vládou a BRS [on-line]. Praha, 2008 [cit. 2008-10-07]. Dostupné z WWW: <http://www.chmi.cz/katastrofy/bezradst1607.pdf>

výzkumu kritičnosti je multidisciplinární charakter projektů v této oblasti a aplikace postupů z oborů spolehlivosti a řízeni rizik[64].

Zvláštní skupinu představuje *kritická informační infrastruktura* (CII), která zahrnuje prvky, jako jsou telekomunikace, výpočetní technika a software, dále pak internet, optická vlákna, satelity apod.[65].

Ochranou kritické infrastruktury (CIP) se pak rozumí proces, který při zohlednění všech rizik a hrozeb směřuje k zajištění fungování subjektů kritické infrastruktury a vazeb mezi nimi. *Ochrana kritické informační infrastruktury* (CIIP) je pak podskupinou ochrany kritické infrastruktury a soustřeďuje se na ochranu systémů a zařízení a na vzájemně propojené počítače, sítě a služby, které poskytují.

V pojetí EU definice KI zahrnuje „fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít vážný dopad na zdraví, bezpečnost anebo hospodářskou prosperitu obyvatelstva nebo efektivní funkcí vlády“. Pro ČR jako členský stát EU má však větší vliv koncept ECI, který zohledňuje příhraniční efekty. Zahrnuje „fyzické prostředky, obslužná a informační technologická zařízení, sítě a objekty (prvky) infrastruktury, jejichž poškození nebo zničení by mohlo mít vážný dopad na zdraví, bezpečnost nebo hospodářskou prosperitu obyvatelstva nebo efektivní funkcí vlády dvou nebo více členských zemí“[66].

1.2.2 Subjekty kritické infrastruktury

Je důležité si uvědomit, které subjekty jsou do procesu tvorby strategie ochrany KI na jednotlivých úrovních zapojeny.

1. Při tvorbě evropské strategie je to Evropská unie. EU plní úlohu koordinátora celého procesu ochrany KI, a dále plní úlohu hlavního tvůrce ochrany, kontrolora a má také funkci represivní, protože při nedodržení či nesplnění podmínek může ukládat sankce.

---

[64] FUCHS, Pavel. Metodika pro hodnocení kritické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infreastrukturen* ,konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[65] KARDA, Ladislav, KUDLÁK, Aleš. *Analýza, metody a nástroje řešení krizových situací*. České Budějovice : Jihočeská univerzita, 2007.

[66] Komise Evropských společenství. Zelená kniha o Evropském programu na ochranu kritické infrastruktury [on-line]. Brusel, 2005.

2. Na národní úrovni je to stát. Ten rovněž plní dvě úlohy, kdy na jedné straně má stát povinnost chránit občany, majetek a životní prostředí, na druhé straně je stát sám zřizovatelem řady subjektů KI.
3. Soukromí vlastníci podniků či organizací a provozovatelé. Ti jsou označováni jako subjekty KI. Jde o vlastníky a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby KI.
4. Důležitou roli hrají také fyzické osoby, kterých se výpadek funkce subjektů KI významně dotýká.

Při tvorbě jakékoliv strategie týkající se ochrany KI je nutné vzít v úvahu, že podstatná část subjektů KI je v soukromých rukou, což znamená, že bez úzké spolupráce státního a soukromého sektoru není realizace strategie ochrany KI možná. Subjekty soukromého sektoru bude vždy zajímat, co jim to přinese a kdo to vše zaplatí. Důležité bude subjekty KI přesvědčit, že vynaložení prostředků na jejich ochranu pro ně bude přínosem, neboť tím získají konkurenční výhodu. Ta spočívá v tom, že za krizové situace bude mít subjekt KI minimalizované ztráty a bude prakticky moci bez přerušení výrobní činnosti nabízet své produkty ve prospěch řešení krizové situace[67].

Jde zejména o to, aby opatření stanovená rezorty odpovědnými za danou oblast KI byla akceptována příslušnými subjekty a realizována na objektech KI. Právnické osoby a podnikající fyzické osoby, které jsou zařazeny mezi subjekty KI, mají povinnost zpracovat stanovenou dokumentaci ochrany KI a zabezpečit realizaci opatření, která z ní vyplývají. Úkolem státního a zejména soukromého sektoru je:
- implementace státní politiky,
- hodnocení vlastní zranitelnosti a závislosti,
- opatření krizového plánování a řízení,
- rozdělení odpovědnosti,
- výměna informací s vládou a dalšími organizacemi.

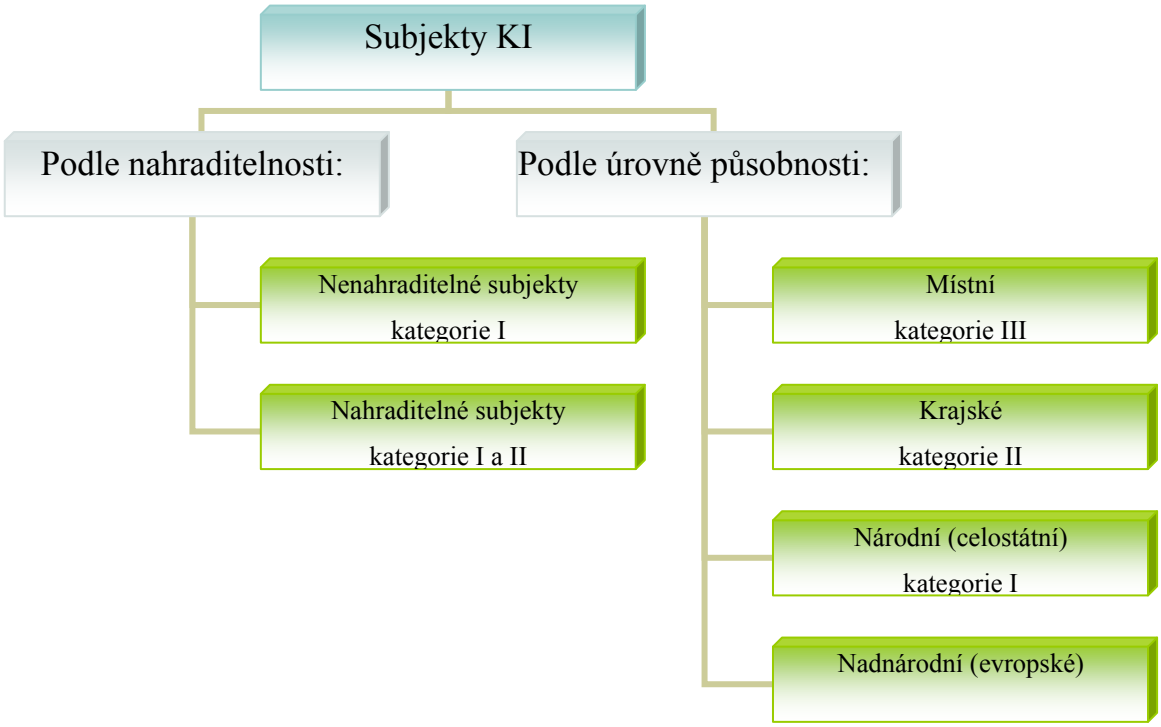
[67] KOTÍK, David. *Ochrana kritické infrastruktury Evropské unie.* [Diplomová práce]. Zlín, 2008. 87 s. [on-line]. Univerzita Tomáše Bati ve Zlíně. Dostupné také z WWW: <http://theses.cz/id/9xl4cn/>.

Propojený systém legislativních, organizačních a technických opatření prováděných veřejnou i soukromou sférou v oblastech KI, umožni za krizové situace zabezpečit základní životní podmínky a potřeby obyvatelstva.

Subjekty KI je možné rozdělit do několika kategorií. Rozdělení se provádí dle stanovených kritérií:

a) *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. dodávky elektřiny, plynu. Může, ale nemusí být vyhlášen krizový stav, budou vyhlašovány regulační stupně, stavy nouze nebo stavy omezení, která mohou být až celostátního charakteru. Podle tohoto kritéria se zařazují subjekty do kategorie I.
b) *Nahraditelnost* – při narušení nebo zničení jsou nutné opravy, rekonstrukce nebo znovuvýstavba. Subjekt či činnost je možné nahradit jiným subjektem nebo provizorním způsobem v dostačující kvalitě. Může, ale nemusí být vyhlášen krizový stav, regulační stupně, stavy nouze nebo různá omezení jsou vyhlašována v omezeném rozsahu v návaznosti na postižené území. Podle tohoto kritéria se zařazují subjekty do kategorie I a II.
c) *Úroveň působnosti* - subjekty podle úrovně jejich působnosti, resp. potřebností 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.

Obrázek 2: Kritéria určující rozdělení subjektů kritické infrastruktury do jednotlivých kategorií



Pramen: autorka dle KOTÍK, David. Ochrana kritické infrastruktury Evropské unie. [Diplomová práce]. Zlín, 2008. 87 s. [on-line]. Univerzita Tomáše Bati ve Zlíně. Dostupné také z WWW: <http://theses.cz/id/9xl4cn/>.

1.2.3 Objekty kritické infrastruktury

Objekty KI jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty KI. Z hlediska náročnosti na zabezpečení ochrany objektů KI a zásad řešení jejich narušení se předpokládá dvojí diferenciace objektů KI:[68]

1. Členění podle rozsahu postiženého území. Jedná se o tyto kategorie objektů:
   a) *objekty národního významu* - jejichž narušení by mělo dopad na zajištění bezpečnosti státu, ekonomiky, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva na území státu, resp. dvou a více krajů. Následky případné nefunkčnosti objektů jsou řešeny subjekty, které je vlastní nebo provozují samostatně nebo ve spolupráci s ministerstvy a ústředními správními úřady, které odpovídají

[68] MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva*. 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html>.

za vymezené oblasti a podoblasti. Nástrojem pro řešení vzniklé situace jsou krizové plány ministerstev a ústředních správních úřadů.

b) *objekty krajského významu* - jejich narušení by mělo dopad na zajištění základních funkcí území kraje nebo jeho části. Následky nefunkčnosti objektů řeší subjekty, které je vlastní nebo provozují samostatně nebo ve spolupráci s krajem, v jehož správním obvodu se objekt nachází nebo ve spolupráci s HZS kraje.

2. Členění podle rozsahu dopadů narušení kritické infrastruktury. Jde o tyto kategorie:

a) *prioritní oblastí nebo objekty* - jejich narušení ovlivní jiné oblasti KI a fungování je nenahraditelné nebo obtížně nahraditelné. Následky nefunkčnosti např. dodávek elektřiny, komunikačních a informačních sítí, vybraných dopravních systémů (dálniční síť, dopravní systémy velkých aglomerací) nebo jedinečných objektů KI má dopad na zajištění společenských potřeb přímo i nepřímo tím, že ovlivní fungování dalších oblastí či objektů KI.

b) *ostatní oblastí nebo objekty* - jejich narušení ovlivní společenský život. Fungování těchto objektů lze nahradit za přijetí zvláštních organizačních opatření nebo provizorně řešit s využitím nouzových služeb. Následky nefunkčnosti např. dodávek ropy, zásobování vodou a potravinami, poskytování zdravotní péče, bankovních a finančních služeb nebo veřejné správy lze zmírnit opatřeními k eliminaci rizik, a to jak rizik mimořádných událostí, tak i rizik vyplývajících z nefunkčnosti prioritních oblastí či objektů. Jde zejména o náhradní zdroje elektrické energie, zajištění spolupráce s nouzovými službami, organizační opatření k poskytování výrobků a služeb u fungujících objektů KI a jiná alternativní řešení.

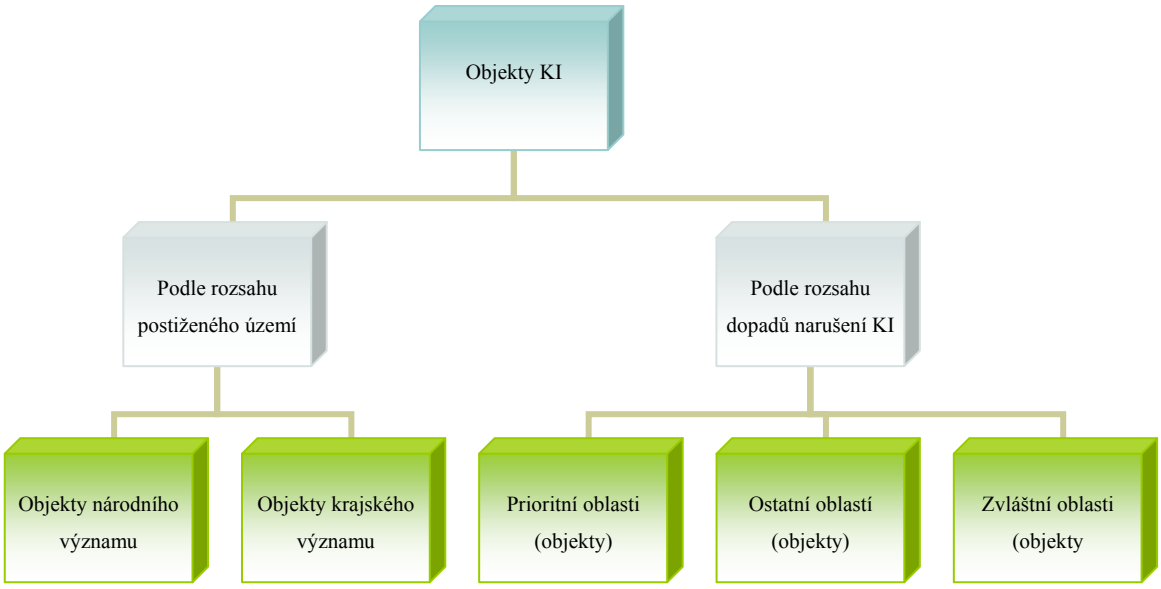
c) *zvláštní oblastí nebo objekty* - jejich narušení ovlivní společenský život pouze při specifických událostech, tj. při krizových stavech nevojenského a vojenského charakteru. Jde zejména o připravenost složek IZS na řešení mimořádných událostí, včetně jejich připravenosti poskytovat nouzové služby obyvatelstvu při narušení KI v míru i za války nebo při narušení obranné infrastruktury za války.

V ČR jsou podle směrnice MO[69] vymezeny objekty důležité pro obranu státu (ODOS). Jedná se o pozemky, stavby a další objekty strategického významu, jejichž poškozením, částečným

[69] Ministerstvo obrany ČR. *Směrnice k výběru objektu obranné infrastruktury a zpracování dokumentace*. Praha, 2007.

nebo celkovým zničením, případně neutralizací by nepřítel získal zjevné vojenské výhody a narušil by tím obranu státu.

Obrázek 3: Rozdělení objektů kritické infrastruktury



Pramen: autorka dle MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. 112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva. 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/ duben/strana_22.html>.

Obrázek 4 znázorňuje schéma, které je možné rozdělit do dvou částí. První část představuje CÍL, kdy povinnosti státu je zajistit a udržet základní funkce státu, a to i za krizových stavů. Základními funkcemi státu jsou zajištění bezpečnosti státu, fungující ekonomika, fungující veřejný sektor a zabezpečení základních životních potřeb. Dosažení tohoto cíle je závislé na konkrétních infrastrukturách, které jsou označovány jako životně důležité infrastruktury popř. kritické infrastruktury. Prostřednictvím KI jsou vymezené základní funkce státu za krizových situací naplňovány.

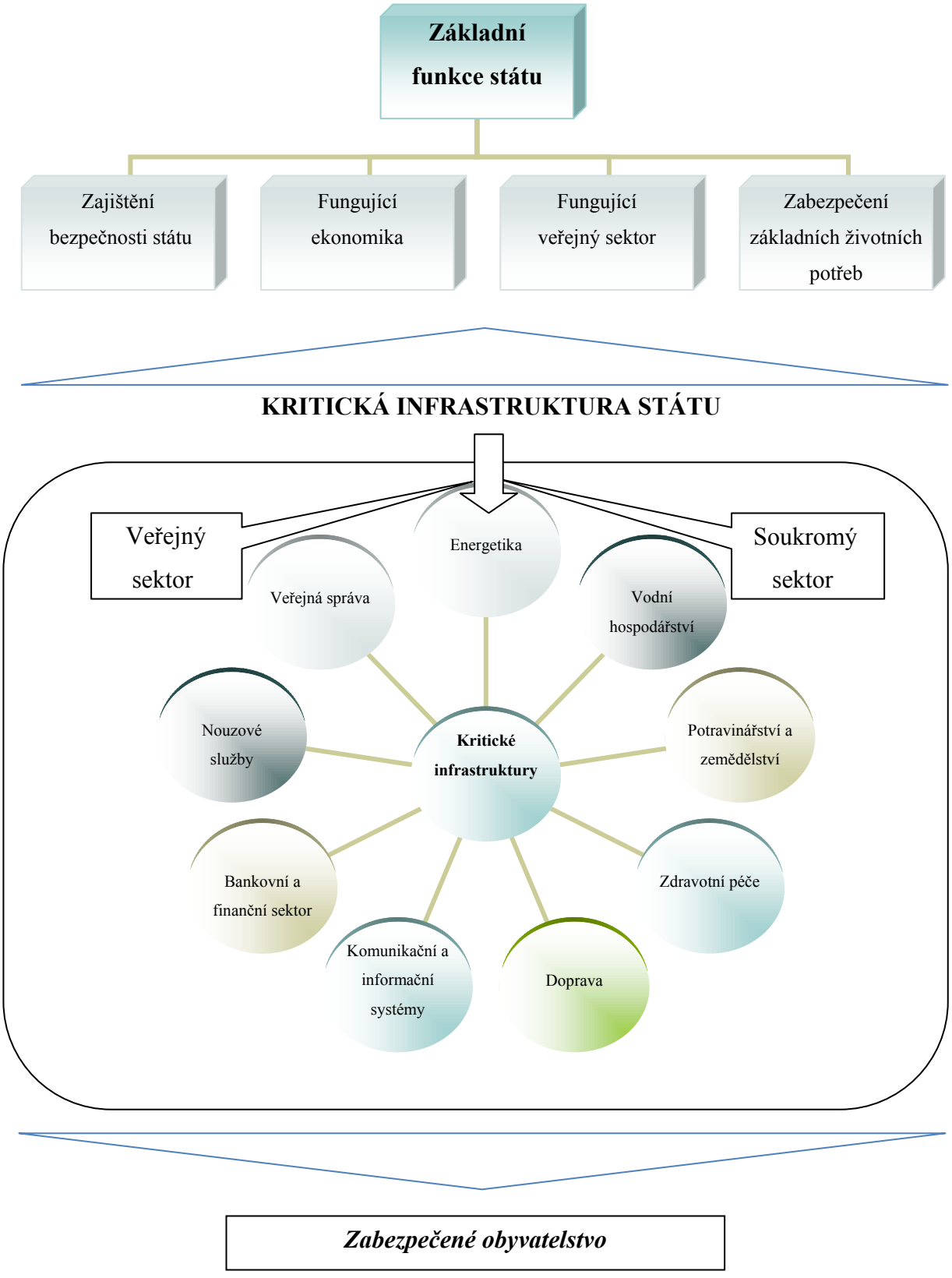
Druhá část schématu znázorňuje již samotnou kritickou infrastrukturu, což je možné označit jako PROSTŘEDEK k dosažení hlavního cíle. V ČR je kritická infrastruktura rozdělena do 9 oblastí, jimiž jsou energetika, vodní hospodářství, potravinářství a zemědělství, zdravotní péče, doprava, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby a veřejná správa. Tyto oblasti jsou definovány jako kritické, neboť jejich nefunkčnost, popř. zničení by mělo negativní vliv na bezpečnost, ekonomický a sociální blahobyt státu,

proto je nezbytné zajistit jejich ochranu. Pojem ochrana kritické infrastruktury však není v legislativě ČR doposud zakotven, ale všeobecně se tímto termínem označuje zabezpečení fungování celého systému pro obyvatelstvo. Jelikož uvedené kritické infrastruktury nejsou pouze v rukách státní správy, je důležité do celého procesu ochrany zapojit také soukromé subjekty. Výsledkem celého procesu je zabezpečené obyvatelstvo.

Dílčí závěr

V této kapitole byl popsán současný stav týkající se legislativního procesu v oblasti ochrany kritické infrastruktury. Jak bylo uvedeno, v ČR není doposud schválen žádný zákon přímo se týkající kritické infrastruktury, není definován její rozsah a způsob ochrany. Zároveň nejsou stanoveny právně závazné zásady pro výběr objektů a subjektu kritické infrastruktury, vymezení jejich kompetenci a povinností. V kapitole je dále uvedena explikace základních pojmů. Konkrétně zde je vymezen pojem infrastruktura a její základní členění, uvedena všeobecně přijímaná definice kritické infrastruktury v ČR a definice používané v pojetí EU a na federální úrovni USA. V kapitole jsou rovněž specifikovány subjekty, které jsou zapojovány do procesu tvorby strategií ochrany KI na jednotlivých úrovních a uvedena kritéria, podle kterých je možné rozdělovat subjekty KI do odpovídajících kategorií. Bude nezbytné jasně vymezit podmínky pro výběr a zařazování objektů KI do jednotlivých úrovní, pro hodnocení jejich bezpečnosti a ochrany a pro poskytování informací orgány státu.

Obrázek 4: Kritická infrastruktura státu a její ochrana



Pramen: autorka

2 KRITICKÁ INFRASTRUKTURA VYBRANÝCH ZEMÍ

V řadě vyspělých států je pojem kritická infrastruktura obecně známý a zpravidla formálně i věcně vymezený, popř. legislativně zakotvený. Pro koordinaci a řízení ochrany národní kritické infrastruktury jsou v jednotlivých zemích stanovovány jak odpovědné resorty, tak také resorty spolupracující. Vazby mezi těmito subjekty jsou za účelem dosažení maximální efektivity při obnově postiženého území pro jednotlivé typy krizových situací, pro řízení jejich průběhu, eliminaci následků a obnovu postiženého území zpracovávány formou tzv. matic zodpovědnosti. Cílem stanovení těchto odpovědných a spolupracujících resortů je zamezení vzniku krizových situací, a v případě, že zamezení není možné, je nutné mít připravena opatření ke zmírnění dopadů krizových situací.

Jak již bylo diskutováno, kritická infrastruktura představuje vysoce rozvinutý a vzájemně propojený komplex, který je vlastněn různými subjekty. Úsilím vlády je zabezpečit adekvátní ochranu KI, kdy vzájemná spolupráce dotčených subjektů a propojenost preventivních a ochranných opatření musí být požadována za účelem poskytnutí co největšího stupně ochrany KI, a to jak pro obyvatelstvo, tak pro podnikatelskou sféru a státní správu. To je důvodem, proč si každý stát vymezuje roli hlavního aktéra v procesu ochrany KI a vytváří si seznam kritických sektorů. V následujících podkapitolách je uveden přehled organizačního zajištění ochrany KI a stručně popsán celý systém ve vybraných státech EU. Převážná část informací o KI v jednotlivých státech byla převzata z cizojazyčného odborného materiálu[70], proto není-li uvedeno jinak, se předpokládá použití tohoto zdroje.

2.1 Kritická infrastruktura vybraných zemí Evropské Unie

Jednotlivé státy jsou při budování celého systému různě daleko. Každý stát si je vědom, že je nezbytné zajistit optimální koordinaci všech aktivit a aktérů v procesu ochrany KI. Tabulka 3 uvádí formy spolupráce ve vybraných státech EU z pohledu státu, kdy jednotlivá ministerstva nebo jiné orgány státní správy nesou odpovědnost za příslušnou oblast kritické infrastruktury a dále tabulka uvádí formu spolupráce státního a soukromého sektoru.

---

[70] BRUNNER, Elgin, SUTER, Manuel. *International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies.* Zurich : ETH Zurich - Center for Security Studies, 2008, 648 p. Dostupný také z WWW: <http://se2.isn.ch/serviceengine/FileContent?serviceID=11&fileid=8EAC1DE9-1B8D-DA5B-93D7-4FC32E2415B2&lng=en>.

Tabulka 3: Forma spolupráce ve vybraných státech EU z pohledu státu a z pohledu státu v kooperaci se soukromým sektorem

Stát	Organizační zabezpečení ochrany KI	Spolupráce soukromého a státního sektoru
Finsko	Ministerstvo dopravy a spojů Ministerstvo obchodu a průmyslu Národní nouzová zabezpečovací agentura Ministerstvo financí	National Emergency Supply Council (NESC) – Rada pro národní nouzové zásobování
Francie	Ústřední ředitelství pro bezpečnostní informační systémy Meziministerská komise pro bezpečnost informačních systémů	Strategic Advisory Board on Information Technologies (CSTI) – Strategický poradní výbor pro informační technologie
Německo	Spolkové ministerstvo vnitra Spolkový úřad pro informační bezpečnost Spolkový úřad pro civilní ochranu a asistenci v případě pohrom Spolková agentura kriminální policie Spolková policie Ministerská pracovní skupina pro kritickou infrastrukturu	Initiative D 21 – Iniciativa D 21
Maďarsko	Ministerstvo pro ekonomiku a dopravu Úřad ministerského předsedy Ministerstvo obrany Ministerstvo spravedlnosti a vymáhání práva	The Theodore Puskás Foundation – Fond Theodore Puskáse
Itálie	Ministerstvo vnitra Ministerstvo pro inovace a technologie Ministerstvo pro komunikaci	Association of Italian Experts for Critical infrastructures (AIIC) - Společnost italských expertů pro kritickou infrastrukturu
Nizozemí	Ministerstvo pro ekonomické záležitosti Ministerstvo vnitra Ministerstvo dopravy, veřejných věcí a vodohospodářství Ministerstvo zdravotnictví, sociální péče a sportu Generální zpravodajská a bezpečnostní služba	Platform Electronic Commerce in the Netherlands (ECP.NL) National Continuity Plan for Telecommunications (NACOTEL) and National Continuity Forum Telecommunications (NCO-T) Strategic Board for CIP (SOVI) National Advisory Centre Critical Infrastructures (NAVI)
Norsko	Ministerstvo spravedlnosti a Policie, Ministerstvo vládní administrativy a reformy Ministerstvo obrany Ministerstvo dopravy a spojů Koordinační rada pro zajištění národních informací v oblasti bezpečnosti	The Norwegian Computer Emergency Response Team (NorCERT) - Norský počítačový tým rychlé odezvy Norwegian Center for Information Security (NorSIS) - Norské centrum pro bezpečnost informací

Polsko	Ministerstvo pro vědu a vyšší vzdělávání Ministerstvo vnitra	The Polish Competence Center for E-Gov and E-Edu - Polské konkurenční centru pro E-vládu a E-vzdělávání
Španělsko	Ministerstvo průmyslu, turistiky a obchodu Ministerstvo pro státní správu Ministerstvo vnitra	The Information Society and Telecommunications Analysis Center (ENTER) – Informační společnosti a analytické centrum pro telekomunikace The Spanish Electronics, Information Technology and Telecommunications Industries Association (AETIC) – Španělska elektronická, informačně-technologické a telekomunikační průmyslová asociace
Švédsko	Ministerstvo obrany Ministerstvo průmyslu, zaměstnanosti a komunikací Ministerstvo spravedlnosti Swedish Emergency Management Agency (SEMA) – Švédská agentura krizového managementu Swedish Civil Contingencies Agency (SCCA) - Agentura pro civilní nepředvídané skutečnosti ve Švédsku	SEMA´S Private Sector Partnership Advisory Council and Board of Information Assurance The Industry Security Delegation (NSD) – Komise pro bezpečnost průmyslu Swedish Information Processing Society (DFS) – Švédská společnost pro zpracování informací
Velká Británie	Ministerstvo vnitra Centre for Protection of National Infrastructure (CPNI) - Centrum pro ochranu kritické infrastruktury (dříve Bezpečnostní koordinační centrum národní infrastruktury a Rada národního bezpečnostního centra)	CPNI´s Public-Private Partnerships – Veřejně-soukromé partnerství v CPNI The British Computer Society The Internet Security Forum The National Computing Centre

Pramen: autorka dle BRUNNER, Elgin; SUTER, Manuel. International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies. Zurich : ETH Zurich - Center for Security Studies, 2008. 648 p. Dostupný z WWW: <http://se2.isn.ch/serviceengine/FileContent?serviceID=11&fileid=8EAC1DE9-B8D- DA5B-93D7-4FC32E2415B2&lng=en>.

V následujících kapitolách je u jednotlivých zemí EU popsán stav v oblasti KI. Je zde uveden *výčet oblastí, resp. sektorů*, které daná země považuje za součást kritické infrastruktury. Dále je zde popsáno *organizační zajištění* ochrany KI s tím, že jsou zde uvedeny nejdůležitější orgány státní správy zabývající se ochranou kritické infrastruktury. U jednotlivých zemí jsou rovněž uvedeny aktivity týkající se *spolupráce mezi veřejným a soukromým sektorem* pro oblasti KI. Tyto tři stěžejní aspekty jsou pro oblasti ochrany KI považovány za klíčové a je možné z nich vypozorovat rozdílnost v národních přístupech k ochraně KI.

2.1.1 Finsko

Ve Finsku jsou kritické sektory a politika pro ochranu kritické infrastruktury definované v „Security of Supply Act" a v "Decree of the National Emergency Supply Agency of 1992". Jedná se o vládní dokumenty stanovující oficiální cíle pro rozvoj spolehlivosti dodávek, které jsou každý 5 až 6 let novelizovány. Od roku 2008 je kritická infrastruktura definována detailněji, než tomu bylo v předcházejícím období, a to i přesto, že nedošlo k rozšíření kritických sektorů. V současné době tvoří ve Finsku kritickou infrastrukturu:

- energetická síť a zásobování,
- elektronické informační a komunikační systémy, zahrnující komunikační sítě, IT systémy, elektronické masmedia, platební režimy bank a pojišťoven,
- dopravu a logistické systémy,
- zásobování vodou a jiné místní zařízení,
- výstavba infrastruktury a zařízení,
- finanční služba,
- zásobování potravinami,
- zdravotní služba,
- media.

Vláda se zaměřuje na KI ochraňující společnost. Cílem je ochrana základních struktur za použití nekritických technologií a organizací, dokonce i v průběhu poruch a nouzových situací. Ve Finsku existují tři klíčové úřady zabývající se kritickou infrastrukturou. Jde o:

- The Finnish Communications Regulatory Authority (FICORA) patřící pod Ministerstvo dopravy a spojů, který zajišťuje informační náležitosti, stejně tak jako technické regulace a standardizace.
- The National Emergency Supply Agency (NESA) pracující pod dohledem Ministerstva obchodu a průmyslu, který analyzuje hrozby a rizika ve vztahu ke kritické infrastruktuře. NESA – Národní nouzová zabezpečovací agentura – je napříč fungující administrativně-operativní úřad pro zajištění spolehlivostí dodávek Finska. Slouží k rozvoji spolupráce mezi veřejným a soukromým sektorem na poli ekonomické připravenosti, koordinace přípravy se státní správou a k rozvíjení a udržování spolehlivosti dodávek.
- The Steering Committee for Data Security in State Administration (VAHTI) je skupina expertů pracující pod ministerstvem financí, která vytváří politiku a zajišťuje praktické průvodce pro zajištění bezpečnosti informačních systémů.

V roce 1955 byla založena National Emergency Supply Council (NESC), která pracuje pod dohledem Ministerstva zaměstnanosti a ekonomiky. Jejím úkolem je plánovat a koordinovat situace v případě vzniku mimořádných událostí. Skládá se jak z předních expertů státní správy tak také z odborníků soukromé sféry. Analyzuje hrozby v oblasti zajištění bezpečnosti dodávek a plánuje opatření v případě jejich vzniku.

2.1.2 Francie

Ve Francii jsou za kritické považovány všechny sektory, které slouží k zajištění základních sociálních a ekonomických procesů. Mezi tyto kritické sektory patří:

- finance,
- průmysl,
- energetika,
- práce soudu,
- veřejné zdraví,
- práce národních civilních autorit,
- elektronické komunikační, audiovizuální media a informační technologie,
- dopravní systémy,
- zásobování vodou,
- potraviny,
- vesmír a výzkum,
- ozbrojené síly.

Francouzský regulační rámec týkající se KI je pravidelně aktualizován, jeho přístup je založen na řízení rizik, plánů prevence a odezvy. Do procesu sdílení informací je zapojen národní výbor, meziresortní komise a zástupci obrany a bezpečnosti. Zástupci z výše uvedených 12 sektorů museli vypracovat národní bezpečnostní směrnici a následně bylo odborníkům stanoveno rozvést tuto směrnici pro jednotlivé specifické oblasti do operačních bezpečnostních plánů. Pro každý kritický prvek pak byly operační bezpečnostní plány rozvedeny do jednotlivých ochranných plánů a úřadům stanoveno vypracovat vnější ochranný plán.

V srpnu 1997 ustanovil francouzský premiér Informační a komunikační asociaci. Jejím cílem bylo vybudovat informační společnost a pomoci tak Francii dostihnout ostatní země v oblasti využití Internetu. Učinit vládní služby internetově dostupné bylo hlavní cílem Vládního

akčního programu pro informační společnost (Government Action Program for an Information Society – PAGSI). Navíc zdokonalení hlavních veřejných služeb, standardizace a školení státních zaměstnanců bylo realizováno projekty z oblasti vzdělávání, kultury, výzkumu a vývoje a došlo také ke stanovení vhodnějších postupů pro bezpečnější použití informačních technologií a sítí.

Národními a mezinárodními bezpečnostními záležitostmi se zabývá Generální tajemník pro národní obranu (The Secretary-general for National Defense – SGDN), který je přímo podřízen francouzskému premiérovi. Ve Francii jsou klíčovými organizacemi zodpovědnými za ochranu KI:

- Central Directorate for Information Systems Security (DCSSI) – Ústřední ředitelství pro bezpečnostní informační systémy – bylo ustanoveno v roce 2001 pod autoritou SGDN. Hlavními cíli jsou zajištění bezpečnosti informačních systémů Francie zahrnujících mimo jiné KI v době krize a vytvoření důvěryhodného prostředí pro informační společnost.
- Inter-Ministerial Commission for the Security of Information Systems (CISSI) – Meziministerská komise pro bezpečnost informačních systémů.
- Advisory Office – poradní orgán.

V roce 2000 vznikl Strategic Advisory Board on Information Technologies (CSTI) - Strategický poradní výbor pro informační technologie, který je řízen francouzským ministerským předsedou. Výbor se skládá z obchodních a průmyslových řídících pracovníků a z předních představitelů výzkumné a vývojové sféry a jeho úkolem je poskytovat francouzské vládě doporučení v oblasti ochrany kritické infrastruktury.

2.1.3 Itálie

Od dob, kdy v řadě kritických sektorů začaly hrát důležitou roli informační a komunikační technologie, se stala ochrana kritické informační infrastruktury rozhodující. V Itálii byla vydána řada strategií, v nichž jsou definovány kritické sektory. Ty jsou považované za kritické, i přestože zde neexistuje žádný oficiální seznam. Jde o tyto sektory:

- bankovnictví a finance,
- veřejná bezpečnost a pořádek,
- telekomunikace,
- pohotovostní služby,
- výroba energie, doprava a distribuce,

- veřejná správa,
- systém zdravotní péče,
- doprava a logistika (letecká, železniční, námořní, pozemní),
- voda (pitná a odpadní),
- informační služby a media,
- zásobování potravinami.

Hlavními ministerstvy zabývajícími se ochranou kritické infrastruktury jsou Ministerstvo vnitra a Ministerstvo pro inovace a technologie. Rovněž Ministerstvo pro komunikaci zahrnuje různé aktivity pro zlepšení ochrany informačních a komunikačních sítí.

Pro zlepšení ochrany KI na všech úrovních spolupracují úzce veřejné organizace se soukromým sektorem. Nejdůležitější PPP organizací v oblasti ochrany KI je Společnost italských expertů pro kritickou infrastrukturu (Association of Italian Experts for Critical Infrastructures - AIIC).

2.1.4 Maďarsko

Maďarsko se zapojilo do Evropského programu na ochranu kritické infrastruktury v roce 2005. Definice ochrany KI v Maďarsku koresponduje s definicí vydanou EU, tak jak je formulována v Zelené knize. Kritická infrastruktura je zde označována jako vzájemně propojená, interaktivní a závislá infrastruktura prvků, podniků, služeb a systémů, které jsou důležité pro výkon národní ekonomiky a pro poskytování veřejných služeb za účelem získání přijatelné úrovně ochrany pro národ, jednotlivce a majetek. Sektory ochrany KI zahrnují:
- informační a telekomunikační systémy,
- energetiku,
- zásobování vodou,
- dopravu,
- veřejné zdraví,
- zásobování potravinovými produkty,
- bankovnictví a finanční sektor,
- průmysl,
- vládní instituce,
- veřejnou bezpečnosti a obranu státu.

Po parlamentních volbách konaných na přelomu dubna a května roku 2006 došlo ke změně vlády a její struktury. S ohledem na ochranu KI a vývoj informační společnosti byla nejpodstatnější změnou integrace Ministerstva informatiky a komunikace do Ministerstva pro ekonomiku a dopravu a Úřadu předsedy vlády. V současné době je hlavním úkolem přidělit ochranu KI jednotlivým ministerstvům.

- Ministerstvo pro ekonomiku a dopravu. Jako ministerstvo je zodpovědné za podporu a vývoj struktur zahrnujících informační infrastrukturu.
- Úřad předsedy vlády. S pomocí Elektronického vládního centra koordinuje Úřad předsedy vlády portál E-vláda.
- Ministerstvo obrany. Toto ministerstvo je zodpovědné za národní obranu zahrnující rovněž bezpečnosti informací. Zvláště je zodpovědné za ochranu státních tajemství a veřejných dat.
- Ministerstvo spravedlnosti a vymáhání práva. Toto ministerstvo poskytuje služby a má zodpovědnost za předcházení vzniku kriminality a bezpečnost informací.

V roce 1992 byl v Maďarsku založen The Theodore Puskás Foundation – Fond Theodore Puskáse, který pracuje jako PPP organizace a je spolufinancován vládou a několika dalšími institucemi a podniky. Hlavním cílem je rozšiřování progresivních technologií v Maďarsku a jeho hlavní aktivity spadají do oblasti výzkumu, poskytování konzultací a informací v oblasti informačních technologií.

2.1.5 Německo

V Německu je kladen důraz na skutečnost, že jak vláda, tak i celá společnost jsou závislé na bezpečné infrastruktuře. Jako kritické jsou zde definovány ty organizace a zařízení, které by v případě selhání nebo poškození způsobily významné narušení veřejného pořádku nebo jiné nepříznivé následky pro velkou část populace[71].

Podle německé ústavy je úkolem státu garantovat veřejnou bezpečnost a pořádek a zajistit, aby populace byla zabezpečena základními potřebami. Jako kritické jsou označovány organizace a zařízení důležitého významu pro stát, při jejichž výpadku nebo narušení může nastat:

[71] GORDON, Kathryn, DION Maeve. Protection of Critical Iinfrastructure and the Role of Investment Policies relating to National Security. Paris : OECD, 2008. 11 p.

a) trvalé narušení zásobování,

b) vážné narušení veřejné bezpečnosti,

c) nebo vzniknou jiné dramatické následky[72].

V Německu jsou definovány tyto sektory jako kritické:[73]

- energetika,
- zásobováni (zahrnující zásobování vodou, potravinami, zdravotní péče, nouzové a záchranné služby),
- telekomunikační a informační technologie,
- doprava a obchod,
- nebezpečné materiály,
- bankovnictví a finance,
- vládní agentury, státní správa a soudnictví,
- media, výzkumné instituce a kulturní hodnoty.

Celková zodpovědnost za aktivity v oblasti ochrany kritické infrastruktury leží na Spolkovém ministerstvu vnitra, které je společně s několika dalšími státními úřady zodpovědné za zajištění vnitřní bezpečnosti Německa. Spolupracujícími úřady jsou zejména:

- Spolkový úřad pro informační bezpečnost (Federal Office for Information Security – BSI),
- Spolkový úřad pro civilní ochranu a asistenci v případě pohrom (Federal Office of Civil Protection and Disaster Assistance – BBK),
- Spolková agentura kriminální policie (Federal Criminal Police Agency – BKA),
- Spolková policie (Federal Police – BPOL).

Pro koordinaci byla Spolkovým ministerstvem vnitra ustanovena v roce 2002 Meziministerská pracovní skupina pro kritickou infrastrukturu AG KRITIS. Strategický vývoj a implementace opatření jsou koordinovány za pomoci dalších spolkových ministerstev, zejména pak Spolkového ministerstva pro ekonomiku a technologie, Spolkového

---

[72] KOCH, Monika. Náročni strategie ochrany kritických infrastruktur. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukturen,* konference 2.-3.10.2006.[CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[73] Bundesministerium des Innern. *Schutz Kritischerr Infratrukturen – Risiko- und Krisenmanagement*. Berlin : Koelblin Fortuna, 2007.

velvyslanectví, Spolkového ministerstva spravedlnosti, Spolkového ministerstva zahraničních věcí, Spolkového ministerstva obrany a ve spolupráci s příslušnými agenturami.

V Německu existuje několik aktivit týkající se spolupráce mezi veřejným a soukromým sektorem v oblasti kritické infrastruktury. Největší platformou je iniciativa D 21 zahrnující průmyslové podniky, asociace, politické instituce a další organizace.

2.1.6 Nizozemí

Použitím tzv. metody Quick Scan[74] a konzultací s průmyslovými subjekty a vládou bylo v roce 2004 stanoveno, že kritická infrastruktura v Nizozemí zahrnuje 12 sektorů a 33 produktů a služeb. Infrastruktura je zde považována za kritickou tehdy, jestliže vytváří základní a nezbytné služby pro společnost a jestliže by její narušení mohlo přivodit stav nouze nebo by mohlo mít nepříznivé účinky na společnost v delším časovém období. V Nizozemí jsou mezi kritické zahrnovány tyto sektory:

- zásobování pitnou vodou,
- energie (elektrika, zemní plyn a ropa),
- finanční sektor (finanční služby a finanční infrastruktura, jak státní, tak soukromá)
- potraviny (zásobování potravinami a potravinová bezpečnost),
- zdraví (naléhavá zdravotní péče/nemocnice, očkování, nukleární medicína),
- právní řád (výkon spravedlnosti a vězenství, vymáhání práva),
- veřejný pořádek a bezpečnost (udržování veřejného pořádku a bezpečí),
- zadržování a hospodaření s povrchovou vodou (zajišťování kvality a množství vody),
- telekomunikace (pevná telekomunikační správa sítě, mobilní telekomunikační služby, rádiové spojení a navigace, satelitní spojení, rozhlasové vysílání, internetový přístup, poštovní a kurýrní služby),
- veřejná správa (diplomacie, zajišťování informací pro vládu, ozbrojené síly a obrana, rozhodování státní správy),
- doprava,
- chemický a jaderný průmysl (doprava, skladování a produkce).

[74] Quick Scan je postup, který hrubými odhady administrativních nákladů v jedné oblasti právního řádu umožnil identifikaci původců nákladů – původně za účelem ex-ante posuzování návrhů zákonů. K tomu se využívají data z dostupných databank, které obsahují data jiných průzkumů a měření.

Zodpovědnost za ochranu KI leží na různých činitelích a zahrnuje veřejný i soukromý sektor. Do ochrany je zapojena řada ministerstev (Ministerstvo vnitra, Ministerstvo pro ekonomické záležitosti, Ministerstvo dopravy, veřejných prací a vodohospodářství, Ministerstvo zdravotnictví, sociální péče a sportu) a za ochranu informační bezpečnosti je v Nizozemí odpovědna Generální zpravodajská a bezpečností služba.

V roce 2001 byl vytvořen Národní plán pro zajištění telekomunikace pro případ vzniku nepředvídaných situací v telekomunikačním sektoru, který byl v roce 2006 následně nahrazen Národním trvalou konzultační platformou (National Continuity Consultatiton Platform – NCO-T). V roce 2006 byl rovněž vytvořen Strategický panel pro ochranu kritické infrastruktury (The Strategic Board for CIP – SOVI) tvořený ze zástupců všech kritických sektorů, kteří se scházejí dva a třikrát ročně.

2.1.7 Norsko

V roce 2006 Komise pro ochranu kritické infrastruktury stanovila kritické sektory, rozlišující mezi kritickou infrastrukturou a zajištěním kritických služeb. Kritické služby jsou takové, které zajišťují základní společenské potřeby. Kritičnost infrastruktury je posuzována na základě těchto tří kritérií: závislost (vysoký stupeň závislosti na jiných infrastrukturách naznačuje kritičnost), alternativa (několik málo nebo žádné alternativy znamenají kritičnost) a pevné spojení (vysoký stupeň spojení s jinou infrastrukturou představuje kritičnost). Za použití těchto kritérií byly komisí stanoveny následující kritické infrastruktury:

- elektrická energie,
- elektronická komunikace,
- zásobování vodou a odpadní voda,
- doprava,
- ropa a plyn,
- satelitní infrastruktura.

Tyto kritické infrastruktury představují základ pro následující společensky kritické funkce:

- bankovnictví a finance,
- zásobování potravinami,
- zdravotní služby, sociální služby a bezpečnost,
- policie,
- záchranné služby.

- krizový management,
- parlament a vláda,
- soudnictví,
- obrana,
- environmentální dozor,
- zpracování odpadu.

V Norsku má ministerstvo, které zodpovídá za území v době míru a klidu, zodpovědnost také v době krize a války. Koordinační pravomoc za civilní oblast má Ministerstvo spravedlnosti a policie. Celkovou zodpovědnost za oblast zajištění bezpečnosti ochrany KI má Ministerstvo vládní administrativy a reformy, které přebírá tento úkol od Ministerstva průmyslu a obchodu, zatímco Ministerstvo obrany je zodpovědné za vojenskou oblast. Ministerstvo dopravy a spojů je odpovědné za oblast komunikace, včetně všech záležitostí týkajících se bezpečnosti.

Pro oblast zajištění PPP byla založena Koordinační rada pro zajištění národních informací v oblasti bezpečnosti. V této oblasti byl pro zvýšení kapacity včasného varování zřízen Norský počítačový tým rychlé odezvy (The Norwegian Computer Emergency Response Team - NorCERT) a Norské centrum pro bezpečnost informací (Norwegian Center for Information Security - NorSIS).

2.1.8 Polsko

Polsko považuje za kritickou infrastrukturu takové hmotné a kybernetické systémy, které jsou podstatné pro zajištěné nutného minima operací v ekonomice a vládě. Pro KI je v Polsku přijata tato definice. Jedná se o „systémy a s nimi spojené funkční objekty, objekty stavební, zařízení, instalace, klíčové služby pro bezpečnost státu a občanů sloužící k zajištění fungování orgánů státní správy, institucí a podnikatelů“. V Polsku neexistuje žádný formálně stanovený orgán pro ochranu KI. V návrhu krizového zákona je již problematika KI začleněna a navrženy jsou tyto oblasti KI v rámci jednotlivých odvětví:[75]

- komunikační a počítačové systémy,

[75] LIZAK, Slavomir. Critical Infrastructure in Poland. In *Ochrana obyvatelstva 2007 – ochrana kritické infrastruktury ,* s. 192-198. Ostrava : Sdružení požárního a bezpečnostní inženýrství; VŠB – TU Ostrava, 2007. ISBN 80-86634-51-5.

- bankovní a finanční sektor,
- zdravotnický sektor,
- doprava,
- záchranné služby – nouzové služby,
- zajištění funkční veřejné správy,
- zásobování vodou a potravinami,
- dodávky energie a paliv,
- zajištění systémů souvisejících s produkcí,
- skladování chemických a radioaktivních látek,
- produktovody nebezpečných látek.

V příslušných dokumentech jsou informační a komunikační systémy detailněji definovány stejně tak jako klíčová aktiva v oblasti kritické infrastruktury. Dále se doporučuje zvýšení kontrolních systémů a prioritu dnes tvoří plány pro zajištění kyber-bezpečnosti.

V Polsku mají za oblasti KI zodpovědnost dvě ministerstva, jsou to Ministerstvo pro vědu a vyšší vzdělání a Ministerstvo vnitra. V oblasti PPP vypomáhá polské konkurenční centrum pro E-vládu a E-vzdělávání společně s veřejným sektorem a IT společnostmi.

2.1.9 Slovensko

Na Slovensku je jako kritická infrastruktura označována ta část národní infrastruktury (vybrané organizace a instituce, objekty, soustavy, zařízení, služby a systémy), jejichž zničení nebo nefunkčnost v důsledku působení rizikového faktoru způsobí ohrožení nebo narušení politického a hospodářského chodu státu nebo ohrožení života a zdraví obyvatelstva[76].

Toto zničení nebo nefunkčnost může nastat z důvodu velké přírodní nebo technologické katastrofy, teroristického útoku, extrémních vlivů počasí nebo z dalších důvodů. Zničení nebo nefunkčnost KI by znamenalo obrovské ztráty na životech a majetku, morální škody nebo by vedlo k dezorganizaci společnosti. Byly by rovněž ohrožené bezpečnostní zájmy státu.

[76] Ministerstvo vnitra SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2006. 19 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk/?ochrana-kritickej-infrastruktury>.

Problematika KI není v současné době v žádných právních normách Slovenské republiky (SR) kodifikována, přesto dle doporučení EU jsou jako sektory KI na Slovensku vymezeny:[77]

- voda,
- potraviny,
- zdraví,
- energetika,
- informační a komunikační technologie,
- doprava,
- veřejný pořádek a vnitřní bezpečnost,
- průmysl,
- finanční sektor.

Kritická infrastruktura zahrnuje zejména objekty osobní důležitosti, další důležité objekty, vybrané informační a komunikační prostředky, zařízení na výrobu a zásobování vodou, elektrickou energií, ropou a zemním plynem. Dále pak jednotlivé části majetku státu, majetek podnikatelských právnických a fyzických osob určených vládou SR nebo jiným kompetentním orgánem státní správy, který je nevyhnutelný na zvládnutí krizových situací, na ochranu obyvatelstva a majetku, na zajištění minimálního chodu ekonomiky a správy státu, jakož i na zajištění vnitřní a vnější bezpečnosti státu a který je proto nutné speciálně chránit. Jsou to zařízení, služby a informační systémy životně důležité pro obyvatelstvo, řízení státu, jejichž nefunkčnost nebo zničení může ohrozit bezpečnostní zájmy státu[78].

Za koordinaci KI jsou zodpovědné zejména Ministerstvo hospodářství, Ministerstvo obrany a Ministerstvo vnitra, dále pak Ministerstvo dopravy a Ministerstvo životního prostředí. Značná část KI je v rukách soukromého sektoru, neboť ti nejlépe znají svůj bezpečnostní systém a zodpovědnost je proto na nich.

Problematika ochrany kritické infrastruktury Slovenska je dále podrobněji řešena v kapitole 4.3 Kritická infrastruktura na Slovensku.

---

[77] Ministerstvo vnitra SR. *Návrh Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2006. 24 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691>.

[78] KRÁLIK, Daniel. Ochrana kritickej infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukture,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

2.1.10 Španělsko

Ve Španělsku nebyly kritické sektory dlouhou dobu definovány. V roce 2007 však Úřad pro bezpečnost státu vydal Národní plán pro ochranu kritické infrastruktury, který definuje KI jako „sítě, služby, hmotné zařízení a informační technologie, jejichž přerušení nebo zničení by mělo negativní dopad na zdraví, bezpečnosti a ekonomiku obyvatel státu nebo na účinnost fungování státních institucí a veřejné administrativy“. Národní plán mimo jiné také obsahuje seznam 12 strategických kritických sektorů, a to:

- chemický průmysl,
- jaderný průmysl,
- výzkumná zařízení,
- vesmír,
- energetický sektor,
- telekomunikace,
- doprava,
- zásobování vodou,
- stravování,
- finanční sektor,
- veřejné zdraví.

Na plenárním zasedání v červnu 2007 rozhodl Kongres, aby vláda do půl roku zhotovila seznam národních kritických infrastruktur. Tento seznam byl vypracován a v současné době obsahuje na 3500 kritických zařízení vyskytujících se na území celého Španělska. Navíc, tento seznam se stal základem pro vypracování EPCIP a bude pravidelně aktualizován. Různé aspekty politiky ochrany kritické infrastruktury Španělska podléhají dozoru Ministerstva průmyslu, turistiky a obchodu, Ministerstva pro státní správu a Ministerstva vnitra.

V oblasti PPP byla vytvořena Informační společnost a analytické centrum pro telekomunikace (The Information Society and Telecommunications Analysis Center - ENTER) zajišťující poskytování informací a zpracování analýz. V této oblasti působí také Elektronická, informačně-technologická a telekomunikační průmyslová asociace Španělska (The Spanish Electronics, Information Technology and Telecommunications Industries Association - AETIC), která je neziskovou organizací spolupracující se státní správou, např. s Kanceláří prezidenta, Ministerstvem průmyslu, turistiky a obchodu a Ministerstvem pro státní správu.

2.1.11 Švédsko

Ve Švédsku neexistuje doposud žádná oficiální definice pro kritickou infrastrukturu. Nicméně ochranou KI se zde rozumí ochrana základních elektronických informačních služeb, jako jsou informační technologie, komunikační radiové a televizní služby. Ochrana KI v sobě zahrnujete nejenom technický aspekt, ale také aspekt lidský. Jako kritické jsou stanoveny tyto infrastruktury:

- vzdušné řídicí systémy,
- systémy kontrolního dohledu a sběru dat v oblasti zásobování vodou, dopravy a průmyslu,
- finanční systémy,
- státní povelové systémy,
- telekomunikační systémy,
- internet.

Nejrůznější agentury a organizace, které se zabývají ochranou KI, jsou v podřízenosti ministerstev, jimiž jsou zejména Ministerstvo obrany, Ministerstvo průmyslu, zaměstnanosti a komunikací a Ministerstvo spravedlnosti.

V lednu 2002 byla zřízena Švédská agentura krizového managementu (Swedish Emergency Management Agency – SEMA), která implementuje a spravuje národní strategii pro bezpečnost informací. SEMA je zodpovědná za koordinaci národní ochrany informací na politické úrovni. To zahrnuje zejména analýzu vývoje společnosti a nezávislost společenských kritických funkcí. Dále agentura zajišťuje spolupráci mezi veřejným a soukromým sektorem, koordinuje a iniciuje vědecký výzkum a rozvoj v oblasti krizového řízení. Má také celkovou zodpovědnost za ochranu informací ve Švédsku. V nejbližší době bude SEMA a další agentury přetvořeny do jedné, jejíž název bude Agentura pro civilní nepředvídané skutečnosti ve Švédsku (Swedish Civil Contingencies Agency – SCCA), jež bude podávat zprávy Ministerstvu obrany.

SEMA napomáhá v současné době také aktivitám PPP, tedy vzájemné součinnosti mezi státním a soukromým sektorem. Mimo to agentura zajišťuje, aby odborné znalosti nevládních organizací, jako je např. Komise pro bezpečnost průmyslu (Industry Security Delegation – NSD), byly brány v potaz při krizovém řízení. NSD je orgán uvnitř Konfederace švédských podnikatelů, jehož cílem je zvýšit spolupráci mezi podniky, organizacemi a úřady

a prosazovat komplexní pohled v oblasti zranitelnosti a bezpečnosti. Cílem tohoto síťového systému je zvýšit bezpečnostní a rizikové povědomí široké veřejnosti a podnikatelského sektoru. V oblasti PPP působí Švédská společnost pro zpracování informací (Swedish Information Processing Society - DFS), což je nezávislá organizace pro pracovníky z oblastí informačních technologií zahrnující 32 tisíc členů.

2.1.12 Velká Británie

Ve Velké Británii zahrnuje národní kritická infrastruktura takové klíčové prvky národní infrastruktury, které jsou rozhodující pro nepřetržité zajištění základních služeb. Bez těchto klíčových prvků by nemohly být základní služby zajišťovány, a pro Anglii by to znamenalo vážné následky zahrnující závažné ekonomické škody, hluboké sociální důsledky nebo dokonce rozsáhlé ztráty na životech. Mnoho kritických služeb, které jsou zásadní pro fungování Anglie, závisí na informačních technologiích a jsou zajišťovány jak státním, tak také soukromým sektorem. Uvedených devět sektorů je považováno za rozhodující:

- komunikace (datové komunikace, pevná zvuková komunikace, pošta, veřejné informace, bezdrátová komunikace),
- záchranné služby (ambulance, hasiči a záchranná služba, námořní záchranná služba, policie),
- energie (elektřina, zemní plyn, ropa),
- finance (management aktiv, finanční zařízení, investiční bankovnictví, trhy, maloobchodní bankovnictví),
- potraviny (výroba, dovoz, zpracování, distribuce, prodej),
- vláda a veřejné služby (ústřední vláda, regionální a místní vláda, parlament a legislativa, soudnictví, národní bezpečnost),
- veřejná bezpečnost (chemický, biologický, radiologický a jaderný terorismus, společenské události),
- zdraví (zdravotní péče, veřejné zdraví),
- doprava (vzdušná, námořní, železniční, silniční),
- voda (vodovodní síť, kanalizace).

Ve Velké Británii spadá zodpovědnost za ochranu kritické infrastruktury na Ministerstvo vnitra. Nicméně, řada dalších úřadů hraje důležitou roli při ochraně národní kritické infrastruktury. Do roku 2006 byly za ochranu kritické národní infrastruktury proti elektronickému útoku odpovědné Bezpečnostní koordinační centrum národní infrastruktury

(National Infrastructure Security Co-ordination Centre – NISCC) a Rada národních bezpečnostního centra (National Security Advice Centre – NSAC). Tyto úřady jsou od roku 2007 nahrazeny Centrem pro ochranu národní kritické infrastruktury (Centre for Protection of National Infrastructure – CPNI). Zodpovědnost za zajištění fyzické národní kritické infrastruktury je rozdělena mezi CPNI, bezpečnostní služby a policii.

V oblasti ochrany KI je široce rozvinuta spolupráce mezi veřejným a soukromým sektorem. Vláda úzce spolupracuje se řadou soukromých subjektů a CPNI sdílí informace s vlastníky národních kritických infrastruktur. Cílem je vytvořit mechanismus, s jehož pomocí by se řada společnosti mohla poučit ze zkušeností, chyb a úspěchů jiných. Mezi nejvýznamnější soukromé organizace patří např. British Computer Society – Britská počítačová společnost, Internet Security Forum – Fórum pro bezpečný internet a National Computing Centre – Národní počítačové centrum.

Shrnutí

V tabulce 4 je uveden přehled základních sektorů kritické infrastruktury ve vybraných státech EU. Srovnáváno bylo 12 zemí, konkrétně Finsko, Německo, Francie, Maďarsko, Itálie, Nizozemí, Norsko, Polsko, Slovensko, Španělsko, Švédsko a Velká Británie.

Je patrné, že do KI nelze zahrnout všechny systémy, ale pouze prioritní. Metody pro výběr priorit jsou velmi nákladné. V praxi se často používá metoda vícekriteriálního hodnocení, kdy se posuzuje zranitelnosti jednotlivých částí systému, nebo některé expertní metody, např. v USA a dalších zemích je často uplatňuje delfská metoda[79].

[79] PROCHÁZKOVÁ, Dana. Podklady pro ochranu kritické infrastruktury. In *Sborník 2. Mezinárodní konference Krizový management*. Brno, 2004. 298-306 s. ISBN 80-85960-71-0.

Tabulka 4: Sektory kritické infrastruktury u vybraných států EU

Sektor/Stát	Finsko	Německo	Francie	Maďarsko	Itálie	Nizozemí	Norsko	Polsko	Slovensko	Španělsko	Švédsko	Velká Británie
Informační a komunikační technologie	X	X	X	X	X	X	X	X	X	X	X	X
Energetika	X	X	X	X	X	X	X	X	X	X		X
Bankovnictví a finance	X	X	X	X	X	X	X	X	X	X	X	X
Potraviny – zemědělství	X	X	X	X	X	X	X	X	X			X
Státní správa – veřejná správa – veřejné služby	X	X	X	X	X	X	X	X			X	X
Zdravotnictví	X	X	X	X	X	X	X	X	X	X		X
Nouzové služby (policie, hasiči, zdravotní a záchranná služba)	X	X			X		X	X				X
Veřejný pořádek a bezpečnost			X	X	X	X	X		X			X
Civilní obrana			X	X		X	X					
Obranný průmysl (prům. výr. a jad. energ.)						X				X		X
Nebezpečné látky – průmysl		X	X	X		X		X	X	X	X	
Doprava – logistika	X	X	X	X	X	X	X	X	X	X	X	X
Zásobování vodou	X	X	X	X	X	X	X	X	X	X	X	X
Sociální zabezpečení	X						X					
Media – rozhlasové vysílání	X	X	X		X	X						
Zásob. ropou a plynem						X	X	X				
Právní řád – justice			X			X	X					X
Letecké řídicí systémy											X	
Vesmír a výzkum		X	X							X		
Environment							X	X				
Krizový management							X					
POČET OBLASTÍ	**11**	**12**	**15**	**11**	**9**	**15**	**11**	**12**	**9**	**9**	**7**	**12**

Pramen: autorka

Výše uvedená tabulka srovnává vybrané země EU v sektorech, jež si státy vymezily jako kritické. Je možné vypozorovat, že vybrané země shodně považuji určité oblasti za kritické. Všechny státy si stanovily za kritický sektor informačních a komunikačních technologií, sektor bankovnictví a financí, sektor dopravy-logistiky a sektor zásobování vodou. Jde o oblasti, které jsou nejzranitelnější, neboť např. ztrátu klíčových informací nelze žádným způsobem nahradit. Informační technologie mohou být velmi snadno zneužity pro kriminální a teroristické účely. Ve většině zemí došlo k neúměrně vysokému technologickému vývoji a četnost instalování počítačů v KI překročila možnosti tvorby bezpečnostních softwaru a standardů pro zajištění počítačové bezpečnosti. Také zaškolování pracovníků v této oblasti není jednoduchou záležitostí a vyžaduje určitý čas.

Dalšími významnými sektory jsou zejména energetika, státní správa, zdravotnictví a potraviny. Tyto sektory považuje za kritické převážná část vybraných zemí EU. Energetické systémy jsou uváděny za kritické zejména z toho důvodu, že energie je potřebná nejen pro zajištění odezvy na vzniklou krizovou situaci, ale také pro obnovu a nastartování dalšího rozvoje území a společnosti. Za sektor kritické infrastruktury označuje polovina vybraných zemí EU sektor nouzových služeb, veřejného pořádku a bezpečnosti a nebezpečné látky.

Z analýzy dostupných materiálů a z provedené komparace je možné vymezit tři typy zařízení kritické infrastruktury:[80]

a) veřejná, privátní a vládní klíčová zařízení infrastruktury, např. jaderné elektrárny, a přehrady, a závislé kybernetické a hmotné systémy,
b) významné postupy a místa řízení pomocí kritické infrastruktury,
c) cíle mající kulturní a politický význam a rovněž tzv. „měkké cíle“, kde se konají hromadné události, např. sport, oddych a kultura.

Dílčí závěr

V kapitole byla soustředěna pozornost na vybrané státy EU. U těchto zemí byla provedena deskripce oblastí, které jsou považovány za kritické. Po provedené komparaci je možné konstatovat, že kritická infrastruktura se v jednotlivých státech liší, což souvisí zejména

[80] BOŽEK, František, URBAN, Rudolf, BOŽEK, Miloš. Ochrana kritické infrastruktury. In *Sborník 9. odborné konference s mezinárodní účastí „Současnost a budoucnost krizového řízení“*. Praha : T-SOFT s.r.o. , 2006, 8 s. ISBN 80-239-7296-2.

s podmínkami, které daný stát má. Do určité míry je to dáno geografickými odlišnostmi jednotlivých zemí, např. v Nizozemí je kladen důraz na problematiku záplav, zatímco ve Švédsku na řízení letového provozu a v Itálii na civilní obranu[81]. Při vymezování sektorů kritické infrastruktury se však v určitých oblastech vybrané státy EU shodují, což umožňuje definovat nejzranitelnější a nejdůležitější cíle. Těmto cílům je pak nutné věnovat náležitou pozornost a dále stanovit způsob jak chránit a kolik do jejich ochrany investovat finančních prostředků. Je totiž patrné, že z důvodu omezenosti zdrojů není možné chránit vše potřebné. Dále došlo ke zmapování orgánů, do jejichž kompetence ochrana KI v zemi náleží. V oblasti aktivit PPP byla u jednotlivých zemí uvedena součinnost mezi státním a soukromý sektorem, neboť jak již bylo dříve uvedeno, převážná většina aktivit leží v rukou soukromého sektoru.

2.2 Kritická infrastruktura vybraných států světa mimo Evropskou unii

V této kapitole jsou popsány způsoby ochrany kritické infrastruktury ve vybraných státech světa mimo Evropskou Unii. Zvoleny byly státy, které jsou v procesu ochrany kritické infrastruktury vyspělé, mají vybudován systém, jsou definovány sektory KI, odpovědné orgány státní správy a současně mají tyto státy rozvinutou veřejně-soukromou spolupráci. Konkrétně byly vybrány tyto státy: Austrálie, Kanada, Nový Zéland a USA. Jedná se o země, které vkládají do oblasti KI značné finanční částky, a vývoj z posledních let jen dokazuje, že tyto výdaje jsou opodstatněné. Mimoto, jak již bylo v kap. 1.1.1 uvedeno, USA a Austrálie byly prvními státy, které začaly nad problematiku ochrany kritické infrastruktury diskutovat a americká „Národní strategie fyzické ochrany KI a klíčových zařízení“ je dodnes považována za jeden z nejkomplexnějších materiálů řešící ochranu KI. Je možné konstatovat, že i vytvoření EPCIP bylo tímto dokumentem inspirováno.

2.2.1 Austrálie

Austrálie přijala tuto definici kritické infrastruktury: „kritickou infrastrukturou jsou zařízení, zásobovací řetězce, informační technologie a komunikačních sítě, jejichž zničení, znehodnocení nebo nedosažitelnosti pro delší doby by mělo významný dopad na sociální a ekonomický blahobyt země nebo by ovlivnilo národní obranu a zajištění národní bezpečnosti“. Národní informační infrastruktura je pak podmnožinou kritické infrastruktury. Kritická infrastruktura v Austrálii zahrnuje 9 sektorů, které jsou považované za kritické:

[81] MULLER, Jan. *Kritická infrastruktura státu a ICT technologie* [on-line].[cit. 2009-02-25] Dostupné na WWW: <http://www.isss.cz/archiv/2004/download/prezentace/icz_muller.ppt>.

- komunikace (telekomunikace – telefon, fax, internet, kabel, satelity, elektronické sdělovací prostředky),
- energie (plyn, ropná paliva, rafinérie, potrubí, výroba elektřiny a její přenos),
- bankovnictví a finance (bankovnictví, finance a devizové obchody),
- zásobování potravin (výroba, skladování a distribuce),
- pohotovostní služby,
- zdravotnictví (nemocnice, veřejné zdravotnictví, výzkumné a vývojové laboratoře),
- národní symboly (ikony a místa pro veřejné shromaždování),
- doprava (řízení letového provozu, pozemní komunikace, námořní a železniční doprava, nákladní distribuční centra),
- technické vybavení (voda, odpadní voda a odpadové hospodářství).

V Austrálii je program na ochranu KI zpracováván Oddělením hlavního právního zástupce státu (Attorney-General´s Department – AGD) v úzké spolupráci s vlastníky a odborníky z oblasti kritické infrastruktury. Program na ochranu KI je koordinován sdílením sítě důvěrných informací o ochraně KI, která zajišťuje rámec pro veřejně-soukromou spolupráci. AGD úzce spolupracuje s dalšími veřejnými agenturami. Nejdůležitější administrativní změnou v uplynulém období bylo ustanovení Vládního koordinačního výboru pro zajištění e-bezpečnosti (E-Security Policy and Coordination Committee – ESPaC). Dalšími úřady jsou:
- Ředitelství pro obranné informace (Defense Signals Directorate – DSD),
- Australská bezpečnostní informační služba (Australian Security Intelligence Organization - ASIO),
- Australská federální policie (Australian Federal Police – AFP).

2.2.2 Kanada

Kanadská kritická infrastruktura se skládá z fyzických a informačních technologií, sítí a prvků, které jsou zásadní pro zdraví, bezpečnost, ochranu a ekonomický blahobyt obyvatelů a pro účinné fungování vlády. NCI Kanady je rozdělena do deseti sektorů:
- energie a zařízení,
- komunikační a informační technologie,
- finance,
- zdravotní péče,
- potraviny,
- voda,

- doprava,
- bezpečnost,
- vláda,
- průmyslová výroba.

Kanadská vláda si uvědomila, že národní kritická infrastruktura by v případě narušení nebo ohrožení mohla vyvolat fyzické i kybernetické hrozby způsobené jak přírodními, tak také lidskými faktory. V roce 2003 bylo rozhodnuto spojit ochranu KI a nouzovou připravenost do jediné organizace, kterou se stala Veřejná bezpečnost Kanady (Public Safety Canada). Organizace byla integrována s cílem maximalizovat nouzovou připravenost a reakci na živelní pohromy a bezpečnostní nouzové situace. Integrovány byly tyto úřady:

- Oddělení generálních prokurátorů (Department of the Solicitor General),
- Centrum pro prevenci národní kriminality (National Crime Prevention Centre),
- Úřad pro ochranu kritické infrastruktury a nouzové připravenosti (Office of Infrastructure Protection and Emergency Preparedness – OCIPEP), který koordinuje rozvoj v rámci zlepšení spolupráce s významnými partnery a investory.

Předpokladem pro zajištění bezpečné kanadské kritické infrastruktury je přesné a včasné informování o vzniklé hrozbě. Integrované centrum pro posuzování hrozeb (Integrated Threat Assessment Centre – ITAC) napomáhá zajišťovat informace z nejrůznějších informačních zdrojů. Kromě toho bylo ustanoveno permanentní Fórum pro zajištění spolupráce mezi federální a místní vládou.

2.2.3 Nový Zéland

Nový Zéland pod ochranou kritické infrastruktury rozumí takovou infrastrukturu, která je nutná pro zajištění kritických služeb. Kritické služby jsou ty, jejichž narušení by mělo vážné nepříznivé dopady na zemi jako celek anebo na značné procento populace. Mezi kritické sektory jsou na Novém Zélandu zahrnuty systémy nezbytné pro zabezpečení:

- záchranných služeb,
- energie (zahrnující výrobu elektřiny a její distribuci, distribuci ropy a plynu),
- financí a bankovnictví,
- vlády (zahrnující právní řád, národní a ekonomickou bezpečnost),
- telekomunikace a internetu,
- dopravy (zahrnující vzdušnou, pozemní a vodní dopravu).

Jednotlivé kritické sektory jsou na sobě navzájem závislé. Většina systému předpokládá kontinuitu výkonu, telekomunikační infrastrukturu a značné použití sítových informačních technologií ve svých systémech řízení a kontroly. Mezi státní instituce v oblasti ochrany kritické infrastruktury patří:

- Vnitrostátní a externí bezpečnostní sekretariát (Domestic and External Security Group – DESG),
- Výbor pracovníků státní správy pro koordinaci vnitřní a vnější bezpečnosti (Officials Committee for Domestic and External Security Co-ordination - ODESC),
- Meziresortní výbor pro bezpečnost (Interdepartmental Committee on Security – ICS),
- Centrum pro ochranu kritické infrastruktury (Centre for Critical Infrastructure Protection – CCIP),
- Vládní úřad pro bezpečnost komunikací (Government Communications Security Bureau – GCSB) a
- Program E-vláda.

V oblasti PPP působí Novozélandská bezpečnostní asociace (New Zeeland Security Association – NZSA), která zajišťuje zastupování obou sektorů. Jejími členy jsou osoby poskytující služby vládě, státním podnikům, firmám a soukromým uživatelům.

2.2.4 Spojené státy americké

Ve Spojených státech amerických je kritická infrastruktura definována jako „systémy a zařízení jak hmotné tak virtuální, které jsou životně důležité pro USA, jejichž zneschopnění nebo zničení by mělo dopad na bezpečnost, národní ekonomickou bezpečnost, národní veřejné zdraví a bezpečí nebo na jakoukoliv jinou jejich kombinaci“. Na základě této definice bylo v prosinci 2003 identifikováno 17 kritických infrastruktur a klíčových aktiv a vymezila se role a zodpovědnost za ochranu těchto sektorů. Plán ochrany národní kritické infrastruktury a Národní strategie vnitřní bezpečnosti (vydaná v roce 2007) znovu potvrdily seznam 17 kritických sektorů a příslušné vymezení zodpovědnosti. V současné době jsou definovány tyto kritické infrastruktury a klíčové aktivity:

- informační technologie,
- telekomunikace,
- chemické látky
- komerční zařízení,
- přehrady,

- jaderné reaktory, materiály a odpad,
- vládní zařízení,
- dopravní systémy (zahrnující hromadnou dopravu, letectví, námořní, pozemní, železniční dopravu a potrubní systémy),
- nouzové služby,
- poštovní a doručovací služby,
- zemědělství a potraviny,
- veřejné zdravotnictví a zdravotní péče,
- pitná voda a systémy úpravy odpadních vod,
- energie (zahrnující produkci, čištění, skladování a distribuci ropy a plynu, elektrické energie s výjimkou komerčních jaderných zařízení),
- bankovnictví a finance,
- národní symboly a ikony,
- základy obranného průmyslu,
- kritická výroba.

Útoky z 11. září 2001 daly podnět ke změně celkového organizačního rámce ochrany kritické infrastruktury USA. V březnu 2003 bylo vytvořeno Ministerstvo pro vnitřní bezpečnost (Department of Homeland Security – DHS), které koordinuje práci federálních, státních a místní vlád. Vznikl Úřad pro ochranu infrastruktur (Office of Infrastructure Protection – OIP), který usměrňuje snahy chránit kritické infrastruktury a klíčová zařízení a Úřad pro kyber-bezpečnost a komunikaci (Office for Cyber-security and Communications – CSαC), který spolupracuje se soukromým sektorem v oblasti identifikace hrozeb, řízení rizika a zlepšení připravenosti.

Shrnutí

Z provedené komparace (tabulka 5) sektorů kritických infrastruktur vybraných států světa vyplývá, že tyto země považují za nejzranitelnější sektor informačních a komunikačních technologií, energetiky, dopravy a sektor bankovnictví a financí. Tyto sektory byly považovány za nejvíce kritické také vybranými zeměmi Evropské Unie. Na druhou stranu se zde vyskytovaly zcela nové prvky, konkrétně v USA byly za kritické označeny také sektor životní prostředí a sektor národní symboly. Austrálie považuje za jeden z kritických sektorů

sektor krizového managementu. V ostatních zemích spadá tato oblast do sektoru zajišťování nouzových služeb.

Tabulka 5: Sektory kritické infrastruktury ve vybraných státech světa

Sektor/Stát	Austrálie	Kanada	Nový Zéland	USA
Informační a komunikační technologie	X	X	X	X
Energetika	X	X	X	X
Bankovnictví a finance	X	X	X	X
Potraviny – zemědělství	X	X		X
Státní správa – veřejná správa – veřejné služby		X	X	X
Zdravotnictví - veřejné zdraví	X	X		X
Nouzové služby (policie, hasiči, zdravotní a záchranná služba)	X			X
Veřejný pořádek a bezpečnost		X	X	
Obranný průmysl (prům. výroba a jad. energ.)				X
Nebezpečné látky – průmysl		X		X
Doprava – logistika	X	X	X	X
Zásobování vodou	X	X		X
Zásobování ropou a plynem	X		X	X
Právní řád – justice			X	
Životní prostředí				X
Krizový management	X			
Národní symboly	X			X
POČET OBLASTÍ	**11**	**10**	**8**	**14**

Pramen: autorka

Dílčí závěr

V kapitole byly popsány kritické infrastruktury vybraných států světa mimo Evropskou unii a ze srovnání je možné vypozorovat, že státy při vymezování sektorů kritické infrastruktury používají podobný přístup. Stejně jako vybrané země EU také tyto země shodně považují za nejzranitelnější sektor informačních a komunikačních technologií, sektor energetiky, sektor dopravy a v neposlední řadě bankovnictví a finance. Mimo to, státy dospěly k závěru, že izolovaný pohled nestačí, je potřeba dosáhnout určitého konsensu. Dnešní společnost není izolovaná, ale naopak stále více vzájemně propojená a při zajištění ochrany nejde jen o životy a bezpečnost státu, ale také o zachování fungování celé společnosti.

3 KRITICKÁ INFRASTRUKTURA V ČESKÉ REPUBLICE A JEJÍ SROVNÁNÍ S EVROPSKOU UNIÍ

V České republice je v současné době vymezeno 9 oblastí a 37 produktů a služeb, které jsou považovány za prioritní z hlediska fungování společnosti. Každá oblast KI spadá do gesce příslušného ministerstva nebo jiného orgánů státní správy. Hlavní míra odpovědnosti za vlastní KI spočívá na členských státech, kdy na základě principu subsidiarity odpovídá každá země za ochranu vlastní KI, a proto národní řešení problematiky KI je vysoce aktuální záležitostí. Přehled oblastí, produktů a služeb kritické infrastruktury České republiky a příslušný gestor je uveden v tabulce 6. V tabulce 7 je pak provedeno srovnání oblastí KI v České republice a Evropské unie.

Tabulka 6: Přehled oblastí kritické infrastruktury České republiky s odpovídajícím gestorem

Oblasti KI	Produkt nebo služba	Gesce
1. Energetika	1.1 Elektřina 1.2 Plyn 1.3 Tepelná energie 1.4 Ropa a ropné produkty	MPO MPO MPO SSHR/MPO
2. Vodní hospodářství	2.1 Zásobování pitnou a užitkovou vodou 2.2 Zabezpečení a správa povrchových vod a podzemních zdrojů vody 2.3 Systém odpadních vod	MZe MZe/MŽP MZe
3. Potravinářství a zemědělství	3.1 Produkce potravin 3.2 Péče o potraviny 3.3 Zemědělská výroba	MZe
4. Zdravotní 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	MZ
5. Doprava	5.1 Silniční 5.2 Železniční 5.3 Letecká 5.4 Vnitrozemská vodní	MD
6. Komunikační a IS	6.1 Služby pevných telekomunikačních sítí 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	MPO/ČTÚ MV

7. Bankovní a finanční sektor	7.1 Správa veřejných financí 7.2 Bankovnictví 7.3 Pojišťovnictví 7.4 Kapitálový trh	MF ČNB
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 monitorovaní vč. Podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření 8.5 Předpovědní, varovná a hlásná služba	MV MV MO SÚJB MŽP
9. Veřejná správa	9.1 Státní správa a samospráva 9.2 Sociální ochrana a zaměstnanost (sociální zabezpečení, stát. soc. podpora, soc. pomoc) 9.3 Výkon justice a vězeňství	MV MPSV MS

Pramen: Usnesení Bezpečnostní rady státu č. 3 z roku 2007

Tabulka 7: Oblasti kritické infrastruktury v České republice a Evropské unii

Oblast KI ČR - produkt nebo služba	Oblasti KI EU - pododvětví
1 Energetika 1.1 Elektřina 1.2 Plyn 1.3 Tepelná energie 1.4 Ropa a ropné produkty	1 Energetika 1.1Produkce ropy a plynu, rafinování, zpracování, skladování a distribuce potrubím 1.2 Výroba a rozvod elektřiny
2 Vodní hospodářství 2.1 Zásobování pitnou a užitkovou vodou 2.2 Zabezpečení a správa povrchových vod a podzemních zdrojů vody 2.3 Systém odpadních vod	2 Voda 2.1 Zásobování pitnou vodou 2.2 Kontrola kvality vody 2.3 Těsnění a kontrola množství vody
3 Potravinářství a zemědělství 3.1 Produkce potravin 3.2 Péče o potraviny 3.3 Zemědělská výroba	3 Potraviny 3.1Zásobování potravinami a zajištění bezpečnosti potravin
4 Zdravotní péče 4.1 Přednemocniční neodkladná péče 4.2 Nemocniční péče 4.3 Ochrana veřejného zdraví 4.4Výroba, skladování a distribuce léčiv a zdravotnických prostředků	4 Ochrana zdraví 4.1 Lékařská a nemocniční péče 4.2 Léky, séra, očkovací látky a léčiva 4.3 Biologické laboratoře a biologičtí činitelé
5 Doprava 5.1 Silniční 5.2 Železniční 5.3 Letecká 5.4 Vnitrozemská vodní	5 Doprava 5.1 Silniční doprava 5.2 Železniční doprava 5.3 Letecká doprava 5.4 Vnitrozemská vodní doprava 5.5 Zámořská příbřežní námořní doprava

6 Komunikační a informační systémy 6.1 Služby pevných telekomunikačních sítí 6.2Služby 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	6 Informační a komunikační technologie 6.1 Ochrana informačních systémů a sítí 6.2Automatizace přístrojů a kontrolních systémů 6.3 Internet 6.4 Poskytování pevných telekomunik. sítí 6.5 poskytování mobilních telekomunik. sítí 6.6 Radiová komunikace a navigace 6.7 Vysílání (televizní a rozhlasové)
7 Bankovní a finanční sektor 7.1 Správa veřejných financí 7.2 Bankovnictví 7.3 Pojišťovnictví 7.4 Kapitálový trh	7 Finanční sektor 7.1Infrastruktury a systémy zúčtování a vypořádání obchodů s cennými papíry 7.2 Regulované trhy
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 monitorovaní vč. Podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření 8.5 Předpovědní, varovná a hlásná služba	Není řešeno
9 Veřejná správa 9.1 Státní správa a samospráva 9.2Sociální ochrana a zaměstnanost (sociální zabezpečení, stát. soc. podpora, soc. pomoc) 9.3 Výkon justice a vězeňství	Není řešeno
Není řešeno	10 Jaderný průmysl 10.1Produkce a skladování/zpracování jaderných látek
Není řešeno	11 Chemický průmysl 11.1Produkce a skladování/zpracování chemických látek 11.2 Potrubí pro přepravu nebezpečných látek (chemických látek)
Není řešeno	12 Vesmír 12.1 Vesmír
Není řešeno	13 Výzkumná zařízení 13.1 Výzkumná zařízení

Pramen: autorka dle Usnesení BRS č. 30, Praha, 2007 a Zelené knihy o Evropském programu na ochranu kritické infrastruktury, Brusel, 2005

Při srovnání oblastí kritické infrastruktury České republiky s oblastmi stanovenými v Evropské unii je možné zjistit, že jsou v základních rysech totožné. Seznam kritické infrastruktury ČR obsahuje devět oblastí, zatímco seznam kritické infrastruktury EU jedenáct. Seznamy jsou téměř identické v sedmi základních bodech. Orgány EU se zaměřují zejména na tu KI, která má význam pro EU jako celek a jejíž vyřazení v jednom členském státu by negativně ovlivnilo situaci i v dalším členském státě.

Třebaže je definování produktů a služeb v ČR a pododvětví v EU na první pohled odlišné, jejich obsah je v mnoha aspektech stejný. Odlišnosti jsou následující:

- Energetika – ČR má jako jeden produkt nebo službu vymezenou tepelnou energii, zatímco EU toto pododvětví chybí.
- Vodní hospodářství – ČR má oproti EU zaveden produkt nebo službu zásobování užitkovou vodou a zaveden systém odpadních vod.
- Potravinářství – zde má kritická infrastruktura ČR a EU v upravené stejné oblasti.
- Zdravotní péče – také v této oblasti nejsou výrazné rozdíly v přístupu ČR a EU.
- Doprava – v EU je jako pododvětví uvedena zámořská a příbřežní doprava, která v ČR není z důvodu vnitrozemského státu opodstatněná.
- Komunikační a informační systémy – v EU je jako jedno z pododvětví uvedena ochrana informačních systémů a síti, a ČR není tato oblast do produktů a služeb kritické infrastruktury zařazena. Na druhou stranu EU nemá mezi pododvětvími zařazenou poštovní službu.
- Bankovní a finanční sektor – V ČR je mezi produkty a služby zařazeno navíc pojišťovnictví.
- Nouzové služby – tato oblast je zařazena pouze do kritické infrastruktury ČR, EU s ní jako s pododvětvím nepočítá.
- Veřejná správa – také toto pododvětví není v EU vymezeno v rámci kritické infrastruktury.
- Jaderný a chemický průmysl – ČR nemá vymezen jako produkt nebo službu. Nezařazení těchto sektoru v ČR je poněkud zarážející, neboť v ČR jsou tato průmyslová odvětví hojně zastoupena.
- Vesmír a výzkum není rovněž v ČR vymezen, v našich podmínkách je tato irelevance pochopitelná.

Lze předpokládat, že oba seznamy kritické infrastruktury se budou dále vyvíjet a přizpůsobovat aktuálním potřebám. Cílem bude zajistit vyšší spolehlivost a odolnost kritické

infrastruktury. Pozornost se zaměří zejména na klíčové prvky, protože disponibilní materiální a finanční zdroje jsou omezené a není možné je v potřebné výši zajistit pro celou zájmovou oblast.

Dílčí závěr

V této kapitole byly srovnány oblasti kritické infrastruktury ČR a oblasti, které jsou označeny jako evropská kritická infrastruktura. Seznam kritické infrastruktury ČR a EU se shoduje v sedmi bodech, ale v několika dalších částech jsou seznamy odlišné. Na jednu stranu je irelevance některých sektorů v podmínkách ČR pochopitelná (vesmír), ale na druhou stranu na seznamu odvětví KI ČR nefigurují významné sektory, jejichž zahrnutí by bylo opodstatněné (chemický a jaderný průmysl). Jako klíčové je možné označit ty součásti KI, jejichž vyřazení může ovlivnit nejen funkčnost a spolehlivost KI jako celku, ale jejichž nahrazení či uvedení do původního stavu je spojeno s potížemi a komplikacemi.

4 SROVNÁNÍ KRITICKÉ INFRASTRUKTURY V ČESKÉ REPUBLICE A NA SLOVENSKU

Pro porovnání kritické infrastruktury byla zvolena jako srovnávací země Slovenská republika, neboť má přibližně stejné podmínky. Postavení obou států je v EU i v mezinárodních společenstvích velmi podobné, stejně tak přírodní podmínky a počet obyvatel je přibližně stejný. Pro názornost jsou uvedeny základní společné rysy obou států:

a) ČR a Slovensko (tehdy ještě ČSR) se v roce 1990 odklánějí od komunismu,

b) ČR (1999) a Slovensko (2004) se stávají spolu s dalšími státy členem NATO,

c) ČR a Slovensko vstupují v roce 2004 spolu s dalšími státy do EU.

4.1 Metoda Check listu a její aplikace na vybrané státy

Pro srovnání přístupu obou zemí byla využita metoda kontrolního seznamu, tzv. check listu[82]. Kontrolní seznam je postup založený na kontrole plnění stanovených podmínek a opatření. Obecně jsou seznamy kontrolních otázek generovány na základě seznamu charakteristik sledovaného systému a jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář. Analýza kontrolním seznamem může být aplikována ve kterémkoliv stadiu procesu a zajišťuje základ pro posouzení hodnoceného procesu.

V diplomové práci je vytvořen seznam kontrolních otázek týkající se oblastí kritické infrastruktury pro ČR a Slovensko (příloha C). Tento seznam byl vytvořen za účelem jednoduchého srovnání postavení dvou vybraných států v oblasti ochrany kritické infrastruktury. Je zřejmé, že pro podrobnější srovnání by bylo nezbytné vytvořit rozsáhlejší seznam otázek. Tím by se dospělo k provedení detailnější komparace. Kontrolní seznam je rozdělen do třech dílčích částí, které je možné považovat za klíčové. První oblast je pojmenována řídící mechanismy a obsahuje otázky zaměřené na řízení celého procesu ochrany KI. Druhou část tvoří řídící dokumenty, zde jsou otázky směřovány na existenci a implementaci strategických dokumentů. Třetí oblast je pak zaměřena na definice, základní pojmy a legislativu v oblasti KI.

---

[82] ŠENOVSKÝ, M., ADAMEC, V, ŠENOVSKÝ P. *Ochrana kritické infrastruktury*. Ostrava : PBI, Spektrum. 2007. ISBN 978-80-7383-025-0.

Vyplněný kontrolní seznam obsahuje odpovědi na zvolené otázky. Odpovědi jsou typu *ano* (výroková hodnota 1), ne (výroková hodnota 0). Pro vyhodnocení kontrolního seznamu se následně sečtou kladné odpovědi a vyjádří se v procentech. Tabulka 8 popisuje hodnocení sledovaného kritéria dle kladných odpovědí.

Tabulka 8: Vyjádření hodnocení sledovaného kritéria

Kladné odpovědi [v %]	Hodnocení sledovaného kritéria
95 a více	výborný
70 – 94	velmi dobrý
50 – 69	dobrý
20 – 49	špatný
do 20	velmi špatný/kritický

Pramen: ŠENOVSKÝ, M., ADAMEC, V, ŠENOVSKÝ P. Ochrana kritické infrastruktury. Ostrava : PBI, Spektrum. 2007. ISBN 978-80-7383-025-0.

Podle výše uvedené metody je hodnocena Česká republika a Slovensko v oblasti ochrany kritické infrastruktury. Čím vyšší procento kladných odpovědí stát obdrží, tím má v procesu ochrany kritické infrastruktury lepší postavení. Pro verbální interpretaci tohoto ukazatele se použije stupnice dle tabulky 8.

4.2 Kritická infrastruktura v České republice

Situace v oblasti ochrany kritické infrastruktury v ČR je detailně popsána v kap. 1.1.3. Kromě historického vývoje zajištění ochrany jsou v této kapitole uvedeny nejdůležitější orgány, dokumenty a popsán současný stav. Proto se následující část bude zaměřovat zejména na hledání odpovědi do vytvořeného kontrolního seznamu.

Pro první oblast – řídící mechanismy, je významná skutečnost, že odpovědnost za oblast KI má Ministerstvo vnitra ČR. MV však úkoly přeneslo na Generální ředitelství hasičského záchranného sboru (GŘ HZS). Žádný další orgán, kterému by byla veškerá oblast ochrany KI přidělena, není zřízen ani stanoven. Pravděpodobně je tento fakt ovlivněn tím, že neexistuje žádný zákon o ochraně KI, a proto se veškerá koordinace řídí krizovým zákonem a nařízením vlády č. 462/2000 Sb. Dalším důležitým ministerstvem, které se mimo jiné podílí na úkolech v oblasti KI, je Ministerstvo průmyslu a obchodu. V rámci MPO je ustanoven Odbor krizového plánování, meziresortním orgánem je Výbor pro civilní nouzové plánování a dalšími subjekty jsou Bezpečnostní rada státu, Ústřední krizový štáb a krizové štáby ministerstev, krajů a obcí.

Druhá oblast – řídící dokumenty, se týká strategických dokumentů pro oblast ochrany KI. Zde je podstatné, že již byla v roce 2008 schválena „Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020“ zahrnující mimo jiné oblast KI. Do konce roku 2009 se předpokládá zpracování „Komplexní strategie ČR k řešení problematiky ochrany KI“. Ta by měla představovat konsensuální rámec pro zpracování dalších koncepčních materiálů, které by ji rozvrhly do konkrétních kroků a následných opatření. „Národní program ochrany KI“ doposud není zpracován, ale předpokládá se předložení jeho návrhu do 31. 12. 2009.

Co se týká vzdělávání, tak pro oblast ochrany obyvatelstva bude i nadále výzkum a vývoj řešen prostřednictvím centrálního pracoviště, které je v působnosti MV-GŘ HZS ČR, v současné době je to Institut ochrany obyvatelstva Lázně Bohdaneč. GŘ HZS ČR připravuje vybudování Národního centra pro krizovou připravenost a výcvik složek IZS. Toto centrum by mělo vzniknout do roku 2013 v Hradci Králové a do jeho areálu by se měl přestěhovat i výše uvedený Institut ochrany obyvatelstva Lázně Bohdaneč. Vybudováním centra dojde k vytvoření infrastruktury nezbytné pro dosažení potřebné úrovně odborné přípravy v oblasti krizového řízení a havarijního plánování ve státní a místní správě, zefektivnění řízení a koordinaci IZS, zvýšení účinnosti prevence přírodních, technologických a bezpečnostních rizik, zdokonalení koordinace reakce na krizové situace a mimořádné události. Celkově je možné říct, že dojde k užšímu propojení vědeckých a výzkumných programů a jejich ověřování v záchranářské praxi[83].

Priority výzkumně-vývojové podpory procesů ochrany obyvatelstva budou uplatněny v rámci přípravy a realizace komplexně řešených výzkumných programů, projektů a záměrů Bezpečnostního výzkumu ČR. Z prostředků NATO budou podporovány výzkumné projekty zejména z oblasti environmentální bezpečnosti a boje proti terorismu. Přestože doposud nebyl vytvořen program na financování opatření pro oblasti ochrany KI, práce v oblasti výzkumu již probíhají. Je podporována řada projektů řešící nějakou speciální oblast KI, např. v MMR podpořilo projekt „ Zásady pro sestavování plánů obnovy majetku v územích postižených živelnou nebo jinou pohromou, které zohledňují zajištění kontinuity kritické infrastruktury“. Také Grantová agentura ČR financuje projekty z této oblasti, např. projekt „Odolnost

[83] *V Hradci Králové bude vybudováno Národní centrum pro složky integrovaného záchranného systému*. [on-lin]. [cit. 2009-01-07]. Dostupné z WWW: <http://www.rozhlas.cz/hradec/zpravy/_zprava/532571>.

umělých staveb proti rozrušení dopravní infrastruktury území náhodnými či záměrnými činy“[84].

Pro třetí oblast – definice, pojmy a legislativa, jsou nezbytné tyto uvedené skutečnosti. Pojem kritická infrastruktura není v naší legislativě vůbec definován a v současné době je existence tohoto pojmu pouze na bázi navrhovaných dokumentů a zpráv. V blízké budoucnosti by měl být tento stav změněn, neboť se předpokládá novelizace krizového zákona[85] a zákona o IZS[86]. V ČR nebyl zatím vytvořen finální seznam odvětví KI, ale je snahou tento seznam sjednotit tak, aby odpovídal požadavkům a vymezením EU i NATO.

[84] BENEŠ, Ivan. Zkušenosti s ochranou kritické infrastruktury v ČR. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukturen*, konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.
[85] Ministerstvo vnitra ČR. Zákon č. 240 ze dne 28. června 200 o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. Praha, 2000.
[86] Ministerstvo vnitra ČR. Zákon č. 239 ze dne 28. června 2000 o integrovaném záchranném systému, ve znění pozdějších předpisů. In Sbírka zákonů České republiky. Praha, 2000.

Tabulka 9: Chect list s kontrolními otázkami pro Českou republiku

1. oblast - řídící mechanismy	**Ano**	**Ne**
Je stanoven odpovědný gestor?	1	0
Je ustanoven orgán pro ochranu KI legislativně?	0	1
Je zajištěna koordinace ochrany KI?	1	0
Je stanoven odborný subjekt/subjekty pro oblast KI?	1	0
Je zaveden vhodný vzdělávací a výcvikový program pro osoby pracující v oblasti KI?	1	0
Je vytvořen program na finanční zabezpečení plnění opatření pro ochranu KI?	0	1
2. oblast - řídící dokumentace		
Je přijata koncepce zahrnující oblast KI?	1	0
Je schválena koncepce KI?	0	1
Je zpracována Komplexní strategie ČR k řešení problematiky ochrany KI?	0	1
Je zpracován Národní program ochrany kritické infrastruktury?	0	1
Je do koncepčních materiálů týkajících se KI zahrnuta také oblast vzdělávání.	1	0
Je do priorit a cílu výzkumně-vývojové podpory zahrnuta oblast ochrany KI?	1	0
3. oblast - definice, pojmy a legislativa v oblasti KI		
Je vymezena definice KI?	1	0
Jsou definice základních pojmů vymezené legislativou?	0	1
Je stanoven přehled základních oblastí KI?	1	0
Jsou vymezeny sektory KI?	1	0
Jsou vymezeny prvky KI?	0	1
Je vytvořen seznam nejdůležitějších objektů KI?	1	0
Je seznam odvětví KI sjednocený s požadavky EU a NATO?	0	1
Je zajištěn soulad základních pojmů (např. definice KI) s řešením Evropské kritické infrastruktury?	0	1

Pramen: autorka

V případě ČR bylo v rámci tří vymezených oblastí zodpovězeno 20 otázek, z toho kladných odpovědí bylo 11, což představuje 55 % a záporných odpovědí 9, což představuje 45 %. Procento kladných odpovědí leží v rozmezí 50-69 % a dle tabulky 8 je výsledek hodnocení „dobrý“.

4.3 Kritická infrastruktura na Slovensku

Problematika ochrany KI na Slovensku byla již popsána v kap. 2.1.9, jejíž součásti je zejména vymezení oblastí ochrany KI, nejdůležitějších orgánů a institucí a dále pak popis spolupráce v mezi veřejným a soukromým sektorem. Dále budou uvedeny informace týkající se oblasti

ochrany KI na Slovensku. V roce 2007 byla vydána Koncepce kritické infrastruktury ve Slovenské republice a způsob její ochrany a obrany[87] (dále jen Koncepce), která mimo jiné specifikuje, kdy je vhodné prvek národní infrastruktury zařadit jako prvek KI. Podle této Koncepce je v tom případě, když prvek národní infrastruktury splňuje alespoň jedno z kritérií uvedených v tabulce 10.

Tabulka 10: Podmínky pro posuzování kritické infrastruktury na Slovensku

Číslo kritéria	Vymezení kritéria	Popis kritéria
1.	Pravděpodobnost, že prvek může být cílem teroristického útoku, resp. může být ohrožen jinými rizikovými faktory	Toto kritérium se uplatňuje na základě poznání nebo intuice (pravděpodobnosti), že podobný prvek byl v minulosti cílem teroristického útoku, nebo je možné předpokládat, že se stane cílem teroristického útoku, např. z hlediska důležitosti pro politický dopad, pohybu velkého množství lidí, snadné přístupnosti apod., případně může být ohrožen jinými rizikovými faktory.
2.	Neakceptovatelné riziko	Toto kritérium je splněno, když následky útoku nebo působení jiného rizikového faktoru na prvek způsobí ohrožení nebo narušení politického chodu státu nebo jeho obranyschopnosti. Ve vztahu k narušení obranyschopnosti to splňují objekty obranné infrastruktury.
3.	Jedinečnost prvku	Kritérium je splněno za předpokladu, že prvek se vyskytuje jako jediný svého druhu a v případě jeho narušení či zničení jej nelze nahradit ani obnovit.
4.	Generalizace	Kritérium se uplatňuje v případě existence skupiny prvků se stejnou funkcí. Vyřazení nebo zničení určité části prvků této skupiny může způsobit ohrožení nebo narušení některé oblasti bezpečnosti státu, ale předem nelze určit, které konkrétní prvky by to mohly být. Z tohoto důvodu je třeba všechny prvky této skupiny zařadit do KI.
5.	Exkluzivita – doplňkové kritérium	Kritérium se uplatňuje v situaci, kdy prvek není zahrnut do žádného.

Pramen: Ministerstvo vnitra SR. Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany [on-line]. 2006. 19 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.

V příloze D je uveden seznam sektorů národní infrastruktury. Seznam je přílohou č. 2 uvedené Koncepce a podle něho jsou vymezeny pro jednotlivá ministerstva a další státní instituce sektory a prvky, jež jsou považované za kritické.

[87] Ministerstvo vnitra SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2006. 19 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.

V Koncepci je rovněž definován pojem kritická infrastruktura. Tou se rozumí „ta část národní infrastruktury (vybrané organizace a instituce, objekty, soustavy, zařízení, služby a systémy), jejichž zničení nebo zneškodnění v důsledku působení rizikového faktoru způsobí ohrožení nebo narušení politického a hospodářského chodu státu nebo ohrožení života a zdraví obyvatelstva“. Současnou KI jsou také objekty obranné infrastruktury. Za sektory KI jsou vymezeny: voda, potraviny, zdraví, energetika, informační a komunikační technologie, doprava, veřejný pořádek a vnitřní bezpečnost, průmysl, finanční sektor. Sektory KI tvoří podskupinu národní infrastruktury, a proto lze pro lepší přehlednost jsou v příloze D tyto sektory a prvky KI zvýrazněny tučným písmem.

Dále již je provedeno hodnocení Slovenska v oblasti ochrany KI dle nadefinovaného kontrolního seznamu. Hodnocení je opět rozděleno do třech dílčích oblastí. V rámci první oblasti – řídící mechanismy, je rozhodující fakt, že v současné době není problematika KI kodifikována v žádných právních normách a nejsou zákonem ustanovené pravomoci a odpovědnost žádnému ústřednímu orgánu státní správy ani žádnému poradnímu orgánu vlády Slovenské republiky. V současné době není stanovený národní gestor pro oblast ochrany a obrany KI, ale navržen jako gestor byl Úřad civilní ochrany MV SR. Národní gestor by měl mimo jiné plnit úlohu kontaktního místa SR pro spolupráci s národními gestory v rámci EU a NATO a bude ustanoven v zákoně o kritické infrastruktuře. Doposud se problematikou ochrany KI zabývalo Ministerstvo hospodářství SR, ale pro další období se o jeho působnosti v této oblasti neuvažuje. Koordinaci doposud zajišťovalo Ministerstvo hospodářství společně s Ministerstvem vnitra a s Ministerstvem obrany, a to zejména z důvodu plnění úkolů zajištění národní bezpečnosti. Pod MV byla zřízena sekce krizového managementu a civilní ochrany a v rámci ní existuje odbor civilní ochrany obyvatelstva, který zabezpečuje mimo jiné úkoly v oblasti ochrany kritické infrastruktury. Tato sekce se podílí na plnění úkolů v oblasti ochrany KI s orgány EU, NATO, ministerstvy, ostatními ústředními orgány státní správy a orgány místní státní správy, dále pak vypracovává podklady a podněty pro tvorbu státní politiky související s vykonáváním opatření v oblasti ochrany KI[88]. V současné době probíhají diskuse týkající se vytvoření Národní strategie o ochraně KI a počítá se také se založením národního koordinačního orgánu o ochraně KI.

[88] PETROVIC, Petr. Aktuální otázky ochrany KI v SR. In Sborník *Ochrana obyvatel 2007 – Ochrana kritické infrastruktury*. Ostrava : VŠB TU Ostrava, 2007. 267-268 s. ISBN 80-86634-51-5.

Pro druhou oblast – řídící dokumentace, je podstatné, že byla vytvořena a schválena Koncepce kritické infrastruktury[89], která tvoří první stupeň zvýšení připravenosti země čelit hrozbám. V roce 2007 byl pak dále vytvořen „Národní program pro ochranu a obranu kritické infrastruktury ve Slovenské republice“[90] (dále Národní program). Cílem vypracování Národního programu je zhodnocení současného stavu na Slovensku a identifikace nejdůležitějších kritických infrastruktur spolu se stanovením programových kroků pro zkvalitnění ochrany a obrany.

Pro třetí oblast – definice, pojmy a legislativa, je významná skutečnost, že v Návrhu koncepce v příloze č. 1 se uvádí terminologie pro oblast kritické infrastruktury, v rámci které jsou definovány jednotlivé pojmy např. národní infrastruktura[91]. Obsahem přílohy č. 2 je seznam sektorů národní infrastruktury uvedený v tabulce 11. Obsah seznamu není považován za pevný, je možné ho flexibilně měnit, a to na základě objektivních změn, nových poznatků a vývoje. V Národním programu byl vznesen požadavek vytvořit mezirezortní program na finanční zabezpečení plnění opatření pro ochranu a obranu KI ve SR. Tím dojde ke zpřehlednění finančních toků vynakládaných ze státního rozpočtu na plnění úkolů ochrany a obrany KI ve SR.

[89] Vláda SR. Usnesení č. 120 ze dne 14. února 2007 k návrhu Koncepce kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany. 2006.
[90] Ministerstvo vnitra SR. *Národní program pro ochranu a obranu kritické infrastruktury ve Slovenské republice* [on-line]. Bratislava, 2007. 24 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.
[91] Tou se rozumí organizace a instituce, objekty, soustavy, zařízení, služby, systémy, jejichž funkce je nevyhnutelná na zabezpečení politického a hospodářského chodu státu.

Tabulka 11: Chect list s kontrolními otázkami pro Slovensko

1. oblast - řídící mechanismy	**Ano**	**Ne**
Je stanoven odpovědný gestor?	0	1
Je ustanoven orgán pro ochranu KI legislativě?	0	1
Je zajištěna koordinace ochrany KI?	1	1
Je stanoven odborný subjekt/subjekty pro oblast KI?	1	0
Je zaveden vhodný vzdělávací a výcvikový program pro osoby pracující v oblasti KI?	1	0
Je vytvořen program na finanční zabezpečení plnění opatření pro ochranu KI?	0	1
2. oblast - řídící dokumentace		
Je přijata koncepce zahrnující oblast KI?	1	0
Je schválena koncepce KI?	1	0
Je zpracována Komplexní strategie ochrany SR pro oblast KI?	0	1
Je zpracován Národní program na ochranu KI?	1	0
Je do koncepčních materiálů týkajících se KI zahrnuta také oblast vzdělávání.	1	0
Je do priorit a cílu výzkumně-vývojové podpory zahrnuta oblast ochrany KI?	1	0
3. oblast - definice, pojmy a legislativa v oblasti KI		
Je vymezena definice KI?	1	0
Jsou definice základních pojmů vymezené legislativou?	0	1
Je stanoven přehled základních oblastí KI?	1	0
Jsou vymezeny sektory KI?	1	0
Jsou vymezeny prvky KI?	1	0
Je vytvořen seznam nejdůležitějších objektů KI?	1	0
Je seznam odvětví KI sjednocený s požadavky EU a NATO?	0	1
Je zajištěn soulad základních pojmů (např. definice KI) s řešením Evropské kritické infrastruktury?	0	1

Pramen: autorka

V případě SR bylo v rámci tří vymezených oblastí zodpovězeno 20 otázek, z toho kladných odpovědí bylo 13, což představuje 65 % a záporných odpovědí 7, což představuje 35 %. Procento kladných odpovědí leží v rozmezí 50-69 % a dle tabulky 8 je výsledek hodnocení „dobrý“.

Výhodou této metody je kromě její jednoduchosti také to, že umožňuje dobře popsat aktuální stav. Mezi nevýhody je pak nutno uvést subjektivitu a zejména špatnou predikci budoucího vývoje. Výstupem metody je vytvoření doporučení, jak by se mělo dále pokračovat.

Dílčí závěr

Při srovnání pozice ČR a Slovenska je možné konstatovat, že v oblasti ochrany KI má lepší postavení Slovensko; dle kontrolního seznamu dosáhlo Slovensko lepšího hodnocení v počtu kladných odpovědí. Přestože obě země jsou hodnoceny výsledkem „dobrý“, je Slovensko o krok napřed, a to zejména díky zpracovaným dokumentům „Koncepce kritické infrastruktury ve Slovenské republice a způsob její ochrany a obrany“ a “ Národnímu programu pro ochranu a obranu kritické infrastruktury ve Slovenské republice“. Současný právní řád ani jedné ze zemí nemá upravenou legislativu pro oblast ochrany KI, nezná definici KI a objektů KI. V legislativní oblasti je nutné vydefinovat rozsah KI a určit způsob její ochrany, proto je potřeba provést novelizaci příslušné legislativy. Po analýze dostupných materiálu je možné konstatovat, že zákon vztahující se k ochraně KI bude pravděpodobně dříve přijatý na Slovensku, a to v časovém horizontu jednoho roku.

Dále je z provedené analýzy patrné, že ani v jedné zemi není pojmosloví zcela totožné s návrhy EU, což může být problémem. Přestože některé dokumenty EU nejsou předpisy, ale pouze doporučení, bylo by vhodné mít pojmosloví kompatibilní s EU. Tato skutečnost je důležitá zejména pro účely mezinárodního srovnání. Pokud některé sektory nejsou v dané zemi významné, nemusel by je stát dále podrobně rozpracovávat. Celý systém ochrany KI by měl být systematicky sledován a ve vhodných případech by bylo vhodné přejímat zahraniční zkušenosti ze zahraničí.

Pro srovnání obou vybraných zemí byla zvolena metoda tzv. check listu, resp. kontrolního seznamu. Jedná se o jednoduchou metodu založenou na seznamu kontrolních otázek. Pro detailnější analýzu by bylo nezbytné vytvořit rozsáhlejší seznam otázek a do jeho tvorby i následného hodnocení zapojit více odborníků, čímž by se metoda více objektivizovala a došlo by tím ke snížení subjektivity. Složitější formou hodnocení by pak bylo i přirazení různých bodových hodnot jednotlivým otázkám. Cílem této kapitoly však bylo provést analýzu a jednoduše srovnat tyto země a poukázat na možné rozdíly s cílem upozornit na možnost dalšího rozvíjení problematiky.

ZÁVĚR

Česká republika, stejně jako další vyspělé státy světa, vymezila pro zajištění základních životně důležitých potřeb kritickou neboli životně důležitou infrastrukturu. První materiály z této oblasti začaly být vydávány již v roce 2001, a jelikož jde o interdisciplinární fenomén, procházejíc napříč mnohými oblastmi lidské společnosti, vyžaduje si jejich tvorba širokou spolupráci odborníků z mnohých odvětví. Je nezbytné poznamenat, že kritická infrastruktura je součástí struktury bezpečnostního prostoru státu a v případě selhání jejích funkcí nebo při jejím částečném či úplnému zničení, může dojít ke vzniku kritických dopadů na bezpečnost, ekonomickou prosperitu státu, životní prostředí, životy zdraví a bezpečnost obyvatel.

Diplomová práce je rozdělena do čtyř stěžejních kapitol. První kapitola seznamuje s vývojem kritické infrastruktury v USA, Evropě, České republice a na úrovni Severoatlantické aliance. Zdůvodňuje potřebu zabývat se ochranou životně důležitých infrastruktur a v chronologickém pořadí uvádí výčet nejvýznamnějších dokumentů a materiálů, jež byly v jednotlivých státech pro oblast KI přijaty. V první kapitole je dále uvedena explikace základních pojmů, zejména pojem infrastruktura a její základní členění. Protože oblast kritické infrastruktury není v České republice zakotvena v legislativě, je úkolem orgánů státní správy ji připravit. V současné době se v ČR k ochraně KI využívá systému krizového řízení vycházejícího z krizového zákona, podle něhož složky integrovaného záchranného systému postupují. Je zde zdůrazněno, že kritická infrastruktura je na jednotlivých úrovních pojímána odlišně. Pro potřeby EU byla vymezena evropská kritická infrastruktura, avšak každý členský stát EU si musí v rámci své působnosti určit, která infrastruktura je pro něj kritická. V první kapitole jsou rovněž specifikovány subjekty, které jsou do procesu tvorby strategií ochrany KI na jednotlivých úrovních zapojovány a dále jsou zde uvedena kritéria, podle kterých je možné subjekty KI rozdělovat do odpovídajících kategorií.

V druhé části diplomové práci byl popsán systém ochrany kritické infrastruktury ve vybraných zemích Evropské Unie i vyspělých státech mimo EU. Byl vytvořen přehled organizačního zabezpečení ochrany KI s uvedením nejdůležitějších orgánů státní správy zabývající se problematikou ochrany KI, dále byla uvedena forma spolupráce státního sektoru se soukromým a vymezeny sektory, které jsou v jednotlivých státech považovány za kritické. Tyto tři aspekty jsou pro oblasti ochrany KI považovány za klíčové a na jejich základě je

možné vypozorovat diference v národním přístupu každé země k ochraně KI. Komparací kritických sektorů jednotlivých států byly stanoveny nejzranitelnější sektory a uvedeny důvody pro zajištění jejich ochrany. Nutno poznamenat, že vybrané státy se ve vymezení kritických sektorů v základních oblastech shodují. Obsahem druhé kapitoly je dále popis systému ochrany KI ve vybraných státech světa mimo Evropskou unii, konkrétně v Austrálii, Kanadě, Novém Zélandu a USA. Vybrány byly zejména takové země, které vkládají do procesu ochrany KI značné finanční částky, a vývoj z posledních let jen dokazuje, že jsou tyto výdaje opodstatněné.

Obsahem třetí kapitoly diplomové práce je provedení komparace kritické infrastruktury České republiky a Evropské unie. Z výsledků srovnání vyplývá, že česká kritická infrastruktura je s evropskou kritickou infrastrukturou totožná jen ve stěžejních bodech. Irelevance některých sektorů v podmínkách ČR je pochopitelná, např. vesmír, ale na druhou stranu na seznamu odvětví KI ČR nefigurují některé významné sektory, jejichž zahrnutí by bylo žádoucí, např. chemický a jaderný průmysl. Orgány EU se při vymezování kritických části zaměřily na takovou infrastrukturu, která má význam pro EU jako celek, a jejíž vyřazení v jednom členském státě by mohlo negativně ovlivnit situaci v dalším členském státě.

V poslední kapitole diplomové práce bylo provedeno srovnání kritické infrastruktury ČR a Slovenska. Jako srovnávací země byla záměrně vybrána Slovenská republika, neboť má přibližně stejné výchozí podmínky pro zajištění bezpečnosti země a rovněž postavení obou zemí v mezinárodních společenstvích je velmi podobné (v 90. letech se odklánějí od komunismu, postupně vstupují co Severoatlantické aliance a v roce 2004 se stávají členy Evropské unie). Po provedeném srovnání, kdy bylo metodou tzv. check listu neboli kontrolního seznamu hodnocena pozice ČR a Slovenska, a je možné konstatovat, že v oblasti ochrany KI má lepší postavení Slovensko. Slovensko je v tomto směru o krok napřed zejména díky zpracovaným dokumentům „Koncepce kritické infrastruktury ve Slovenské republice a způsob její ochrany a obrany“ a “ Národnímu programu pro ochranu a obranu kritické infrastruktury ve Slovenské republice“. Avšak současný právní řád ani jedné země nemá zákonem upravenou oblasti ochrany KI a bude proto nezbytné provést novelizaci příslušné legislativy.

V České republice bude nezbytné vypracovat nosný koncept, minimálně v podobě koncepce kritické infrastruktury, která by mimo jiné obsahovala zejména analýzu dosavadní situace v oblasti KI, navrhovala by možná řešení splňující kritérium efektivnosti celého systému, dále pak kritérium informační kvality, kvalitní spolupráce všech dotčených subjektů a odolnosti systému vůči vnějším vlivům. Klíčové bude rovněž zakotvit v legislativě národního gestora pro oblast ochrany kritické infrastruktury, který zabezpečí koordinaci všech aktivit orgánů krizového řízení v oblasti ochrany KI. Bylo by vhodné, aby tento národní gestor zároveň plnil úlohu kontaktního místa pro spolupráci s národními gestory v rámci EU a NATO. Žádoucí je také stanovit seznam definic a odvětví, kterých se ochrana týká a jasně vymezit kritéria pro zařazení objektů do jednotlivých úrovní KI (evropské, národní, regionální, místí). Příprava legislativy a její další rozpracování do konkrétních úloh s vyčísleným finančních dopadů na státní rozpočet bude náročný úkol. Je potřeba jasně definovat odpovědnost za zajištění ochrany, poskytnou potřebné zdroje pro vykonávání nezbytné ochrany a klást důraz na výzkum a vývoj v této oblasti. Vytvoření právního rámce zastřešujícího celou oblast kritické infrastruktury významně ovlivní bezpečnostní prostředí.

Na závěr je nutno dodat, že dosažení dostatečné ochrany bude dlouhodobým procesem. Kritická infrastruktura obsahuje subsystémy, jejichž počet není doposud ustálený a dokonce v rámci jedné země je možné vypozorovat změny ve složení i počtu těchto subsystému v čase[92]. Je však nezbytné klást důraz na to, aby kritická infrastruktura byla fungující, neboť stát nechrání pouze svůj zájem, ale hlavně chrání životy a zdraví obyvatel, majetek, životní prostředí a další zájmy.

[92] PROCHÁZKOVÁ, Dana. Problém ochrany kritické infrastruktury. In Internationaler *Erfahrungsaustausch Schutz Kritischer Infreastrukturen*, konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

SEZNAM POUŽITÝCH ZKRATEK

Použitá zkratka	Česky	Anglicky
AETIC	Španělska elektronická, informačně-technologické a telekomunikační průmyslová asociace	The Spanish Electronics, Information Technology and Telecommunications Industries Association
AFP	Australská federální policie	Australian Federal Police
AGD	Právní zástupce státu	Attorney-General´s Department
AIIC	Společnost italských expertů pro kritickou infrastrukturu	Association of Italian Experts for Critical infrastructures
ASIO	Australská bezpečnostní informační služba	Australian Security Intelligence Organization
A-SIT	Centrum bezpečnostních informačních technologií Rakouska	Center for Secure Information Technology Austria
BBK	Spolkový úřad pro civilní ochranu a asistenci v případě pohrom	Federal Office of Civil Protection and Disaster Assistance
BKA	Spolková agentura kriminální policie	Federal Criminal Police Agency
BPOL	Spolková policie	Federal Police
BRS	Bezpečnostní rada státu	National Security Council
BSI	Spolkový úřad pro informační bezpečnost	Federal Office for Information Security
CCIP	Centrum pro ochranu kritické infrastruktury	Centre for Critical Infrastructure Protection
CII	Kritická informační infrastruktura	Critical Information Infrastructure
CISSI	Meziministerská komise pro bezpečnost informačních systémů	Inter-Ministerial Commission for the Security of Information Systems
CIWIN	Výstražná informační síť kritické infrastruktury	Critical Infrastructure Warning Information Network
CO	Civilní ochrana	Civil Protection
CPNI	Centrum pro ochranu kritické infrastruktury	Centre for Protection of National Infrastructure
CSTI	Strategický poradní výbor pro informační technologie	Strategic Advisory Board on Information Technologies
CSαC	Úřad pro kyber-bezpečnost a komunikaci	Office for Cyber-security and Communications
ČNB	Česká národní banka	Czech National Bank
ČTÚ	Český telekomunikační úřad	Czech Telecommunication Office
DCSSI	Ústřední ředitelství pro bezpečnostní informační systémy	Central Directorate for Information Systems Security
DESG	Vnitrostátní a externí bezpečnostní sekretariát	Domestic and External Security Group
DFS	Švédská společnost pro zpracování informací	Swedish Information Processing Society
DHS	Ministerstvo pro vnitřní bezpečnost	Department of Homeland Security
DSD	Ředitelství pro obranné informace	Defense Signals Directorate

ECI	Evropská kritická infrastruktura	European Critical Infrastructure
ENTER	Informační společnosti a analytické centrum pro telekomunikace	The Information Society and Telecommunications Analysis Center
EPCIP	Evropský program pro ochranu kritické infrastruktury	European Programme for Critical Infrastructure Protection
ESPaC	Vládního koordinačního výboru pro zajištění e-bezpečnosti	E-Security Policy and Coordination Committee
EU	Evropská unie	European Union
GCSB	Vládní úřad pro bezpečnost komunikací	Government Communications Security Bureau
ICS	Meziresortní výbor pro bezpečnost	Interdepartmental Committee on Security
IS	Informační systém	Information System
ITAC	Integrované centrum pro posuzování hrozeb	Integrated Threat Assessment Centre
IZS	Integrovaný záchranný systém	Integrated Rescue System
KI	Kritická infrastruktura	Critical Infrastructure
MD	Ministerstvo dopravy	Transport Ministry
MF	Ministerstvo financí	Ministry of Finance
MPO	Ministerstvo průmyslu a obchodu	Ministry of Industry and Trade
MPSV	Ministerstvo práce a sociálních věcí	Ministry of Labour and Social Affairs
MS	Ministerstvo spravedlnosti	Ministry of Justice
MV	Ministerstvo vnitra	Ministry of the Interior
MZ	Ministerstvo zdravotnictví	Ministry of Health
MZe	Ministerstvo zemědělství	Ministry of Agriculture
MŽP	Ministerstvo životního prostředí	Ministry of the Environment
NATO	Severoatlantická aliance	Nord Atlantic Treaty Organization
NCI	Národní kritická infrastruktura	National Critical Infrastructure
NCO-T	Národním trvalou konzultační platformou	National Continuity Consultation Platform
NESA	Národní nouzová zabezpečovací agentura	National Emergency Supply Agency
NESA	Národní nouzová zabezpečovací agentura	National Emergency Supply Agency
NESC	Rada pro národní nouzové zásobování	National Emergency Supply Council
NISCC	Bezpečnostní koordinační centrum národní infrastruktury	National Infrastructure Security Co-ordination Centre
NorCERT	Norský počítačový tým rychlé odezvy	The Norwegian Computer Emergency Response Team
NorSIS	Norské centrum pro bezpečnost informací	Norwegian Center for Information Security
NSAC	Rada národních bezpečnostního centra	National Security Advice Centre
NSD	Komise pro bezpečnost průmyslu	The Industry Security Delegation
NZSA	Novozélandská bezpečnostní asociace	New Zeeland Security Association
OCIPEP	Úřad pro ochranu kritické infrastruktury a nouzové připravenosti	Office of Infrastructure Protection and Emergency Preparedness

ODESC	Výbor pracovníků státní správy pro vnitřní a vnější bezpečností koordinaci	Officials Committee for Domestic and External Security Co-ordination
OIP	Úřad pro ochranu infrastruktur	Office of Infrastructure Protection
OSN	Organizace spojených národů	United Nations agency
PAGSI	Vládní akční program pro informační společnost	Government Action Program for an Information Society
SCCA	Agentura pro civilní nepředvídané skutečnosti ve Švédsku	Swedish Civil Contingencies Agency
SEMA	Švédská agentura krizového managementu	Swedish Emergency Management Agency
SGDN	Generální tajemník pro národní obranu	Secretary-general for National Defense
SOVI	Strategický panel pro ochranu kritické infrastruktury	The Strategic Board for CIP
SSHR/ ASMR	Správa státních hmotných rezerv	Administration of State Material Reserves
SÚJB	Státní úřad pro jadernou bezpečnost	State Office for Nuclear Safety
USA	Spojené státy americké	United States of America
VCNP/ CCPC	Výbor pro civilní nouzové plánování	Civil Emergency Planning Committee

SEZNAM TABULEK

Tabulka 1: Oblasti kritické infrastruktury v České republice
Tabulka 2: Vymezení produktu a služeb pro oblast kritické infrastruktury Nouzové služby
Tabulka 3: Forma spolupráce ve vybraných státech EU z pohledu státu a z pohledu státu v kooperaci se soukromým sektorem
Tabulka 4: Sektory kritické infrastruktury u vybraných států EU
Tabulka 5: Sektory kritické infrastruktury ve vybraných státech světa
Tabulka 6: Přehled oblastí kritické infrastruktury České republiky s odpovídajícím gestorem
Tabulka 7: Oblasti kritické infrastruktury v České republice a Evropské unii
Tabulka 8: Vyjádření hodnocení sledovaného kritéria
Tabulka 9: Chect list s kontrolními otázkami pro Českou republiku
Tabulka 10: Podmínky pro posuzování kritické infrastruktury na Slovensku
Tabulka 11: Chect list s kontrolními otázkami pro Slovensko

SEZNAM PŘÍLOH

Příloha A: Sektory kritické infrastruktury podle „Národní strategie fyzické ochrany kritické infrastruktury“ v USA

Příloha B: Klíčová zařízení kritické infrastruktury podle „Národní strategie fyzické ochrany kritické infrastruktury“ v USA

Příloha C: Kontrolní seznam pro hodnocení státu v oblasti ochrany kritické infrastruktury

Příloha D: Seznam sektorů národní infrastruktury Slovenské republiky

SEZNAM OBRÁZKŮ

Obrázek 1: Základní členění infrastruktury státu

Obrázek 2: Kritéria určující rozdělení subjektů kritické infrastruktury do jednotlivých kategorií

Obrázek 3: Rozdělení objektů kritické infrastruktury

Obrázek 4: Kritická infrastruktura státu a její ochrana

SEZNAM POUŽITÉ LITERATURY A DALŠÍCH PRAMENŮ

PUBLIKACE

[1] Bundesministerium des Innern. Sc*hutz Kritischerr Infratrukturen – Risiko- und Krisenmanagement*. Berlin : Koelblin Fortuna, 2007.

[2] BRUNNER, Elgin; SUTER, Manuel. *International CIIP Handbook 2008/2009 – An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. Zurich : ETH Zurich - Center for Security Studies, 2008. 648 p. Dostupný z WWW: <http://se2.isn.ch/serviceengine/FileContent?serviceID=11&fileid=8EAC1DE9-B8D- DA5B-93D7-4FC32E2415B2&lng=en>.

[3] DRYMLOVÁ, Veronika. *Plán znovuobnovení kritické infrastruktury na místní úrovni* [Diplomová práce]. České Budějovice : JU, 2008. 324 s. [on-line]. Dostupné z WWW: <http://theses.cz/id/4stg5a/>.

[4] GORDON, Kathryn, DION Maeve. Protection *of Critical Iinfrastructure and the Role of Investment Policies relating to National Security*. Paris : OECD, 2008. 11 p.

[5] KOTÍK, David. *Ochrana kritické infrastruktury Evropské unie.* [Diplomová práce]. Zlín, 2008. 87 s. [on-line]. Univerzita Tomáše Bati ve Zlíně. Dostupné také z WWW: <http://theses.cz/id/9xl4cn/>.

[6] KARDA, Ladislav, KUDLÁK, Aleš. A*nalýza, metody a nástroje řešení krizových situací.* České Budějovice : Jihočeská univerzita v Českých Budějovicích, 2007.

[7] LAMMING, R., BESSANT, J. *Macmillanův slovník podnikání a managementu*. Praha : Management Press, 1995. 296 s. ISBN 80-85603-47-0.

[9] MALANÍK, Luboš. *Ochrana kritické infrastruktury České republiky.* [Diplomová práce]. Zlín, 2008. 115 s. [on-line]. Univerzita Tomáše Bati ve Zlíně. Dostupné z WWW: < http://theses.cz/id/qlhx9p/>.

[10] Ministerstvo vnitra-generální ředitelství Hasičského záchranného sboru České republiky. *Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020.* Praha, 2008.

[11] Ministerstvo vnitra ČR. *Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu*. Praha, 2004. Dostupné na WWW: <http://www.olomouc.eu/kmmo/ data/dokumenty/term.slovnik/terminsl.pdf>.

[12] MOTEFF, John and PARFOMAK, Paul. Critical *Infrastructure and Key Assets: Definition and Identification.* Congressional Research Service. 2004, 19 p.

[13] PERNICA, P. *Logistický management – teorie a podniková praxe*. Praha : Radix. 1998. ISBN 80-8603113-6.

[14] ŠENOVSKÝ, M., ADAMEC, V, ŠENOVSKÝ P. *Ochrana kritické infrastruktury*. Ostrava : PBI, Spektrum. 2007. ISBN 978-80-7383-025-0.

TIŠTĚNÉ ZDROJE

[1] ADAMEC, Vilém. Ochrana kritické infrastruktury v ČR. In *Sborník 4. Mezinárodní konference*. Brno : VIO UO, 2006, ISBN 80-7231-141-7.

[2] BOŽEK, František, URBAN, Rudolf, BOŽEK, Miloš. Ochrana kritické infrastruktury. In *Sborník 9. odborné konference s mezinárodní účastí „Současnost a budoucnost krizového řízení"*. Praha : T-SOFT s.r.o., 2006, 8 s. ISBN 80-239-7296-2.

[3] LIZAK, Slavomír. Critical Infrastructure in Poland. In *Ochrana obyvatelstva 2007 – ochrana kritické infrastruktury,* s. 192-198. Ostrava : Sdružení požárního a bezpečnostní inženýrství; VŠB-TU Ostrava, 2007. ISBN 80-86634-51-5.

[4]PETROVIC, Petr. Aktuální otázky ochrany KI v SR. In Sborník *Ochrana obyvatel 2007 – Ochrana kritické infrastruktury*. Ostrava : VŠB TU Ostrava, 2007. 267-268 s. ISBN 80-86634-51-5.

[5] PROCHÁZKOVÁ, Dana. Podklady pro ochranu kritické infrastruktury. In *Sborník 2. Mezinárodní konference Krizový management*. Brno, 2004. 298-306 s. ISBN 80-85960-71-0.

[6] URBÁNEK, Jiří. F. Nové hodnocení kritické infrastruktury z hlediska AČR. In *Sborník IV. Konference s mezinárodní účastí Instituce a zařízení regionu v systému ochrany obyvatelstva*. Brno, 2006. 212-217 s. ISBN 80-7231-175-1.

[7] VALÁŠEK, Jarmil. Ochrana kritické infrastruktury. In *Sborník referátů 4. energetického kongresu ČR.* Praha, 2004.

PRÁVNÍ PŘEDPISY

[1] The White House. Presidental Decision Directive 63 [on-line]. 1998 [cit. 2008-09-28]. Dostupný z WWW: <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

[2] Komise Evropských společenství. Sdělení Komise Radě a Evropskému parlamentu. *Ochrana kritické infrastruktury při boji proti terorismu*. Brusel, 2004. KOM/2004/0702.

[3] Komise Evropských společenství. *Zelená kniha o Evropském programu na ochranu kritické infrastruktury*. Brusel, 2005.

[4] Komise Evropských společenství. *Sdělení Komise o Evropském programu na ochranu kritické infrastruktury.* Brusel, 2006.

[5] Komise Evropských společenství. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* Brusel, 2009.

[6] Evropský parlament. *Usnesení Evropského parlamentu o určování a označování KI a o posouzení potřeby zvýšit její ochranu.* Brusel, 2007.

[7] Česká národní rada. Ústavní zákon č. 1 ze dne 16. prosince 1992, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. Praha, 1992.

[8] Ministerstvo vnitra ČR. Zákon č. 239 ze dne 28. června 2000 o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. Praha, 2000.

[9] Ministerstvo vnitra ČR. Zákon č. 240 ze dne 28. června 200 o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. In *Sbírka zákonů České republiky.* Praha, 2000.

[10] Ministerstvo vnitra ČR. Zákon č. 241 ze dne 29. června 2000 o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů. In *Sbírka zákonů České republiky*. Praha, 2000.

[11] Ministerstvo obrany ČR. *Směrnice k výběru objektu obranné infrastruktury a zpracování dokumentace.* Praha, 2007.

[12] Vláda ČR. Usnesení ze dne 5. října 2000 č. 123 Návrh strategie výstavby informačních systémů na podporu krizového plánování a řízení ve státní správě. Praha, 2000.

[13] Vláda ČR. Usnesení ze dne 24. června 2001 č. 105. Praha 2001.

[14] Vláda ČR. Usnesení ze dne 24. června, č. 173, Praha, 2003.

[15] Vláda ČR. Usnesení ze dne 23. září, č. 179, Praha, 2003.

[16] Vláda ČR. Usnesení ze dne 21. června, č. 222, Praha, 2006.

[17] Vláda ČR. Usnesení ze dne 21. března, č. 244, Praha, 2007.

[18] Vláda ČR. Usnesení ze dne 19. prosince, č. 1436, Praha, 2007.

[19] Vláda ČR. Usnesení ze dne 3. července, č. 30, Praha, 2007.

[20] Vláda ČR. Usnesení vlády České republiky ze dne 25. února 2008 č. 165 k Vyhodnocení stavu realizace Koncepce ochrany obyvatelstva do roku 2006 s výhledem do roku 2015 a o Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020. Praha, 2008.

[21] Vláda ČR. Usnesení ze dne 25. února č. 170 o Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury. Praha, 2008.

[22] Vláda SR. Usnesení č. 120 ze dne 14. února 2007 k návrhu Koncepce kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany. Bratislava, 2006.

[23] Ministerstvo vnitra SR. *Národní program pre ochranu a obranu kritickej infrastruktury v Slovenskej republike* [on-line]. Bratislava, 2007. 24 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.

[24] Ministerstvo vnitra SR. *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany* [on-line]. Bratislava, 2006. 19 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.

ZDROJE NA CD

[1] BENEŠ, Ivan. Zkušenosti s ochranou kritické infrastruktury v ČR. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukturen,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[2] FUCHS, Pavel. Metodika pro hodnocení kritické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infreastrukturen,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[3] KOCH, Monika. Nároční strategie ochrany kritických infrastruktur. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukturen,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[4] KLABAN, Vladimír. Kritická infrastruktura, možnosti jejího vymezení a stanovení potencionálních hrozeb. In *Problematika řešení mimořádných událostí a krizových situací v regionech*, konference 4. - 5. 9. 2008. [CD-ROM]. Univerzita Tomáše Bati ve Zlíně, 2008.

[5] KRÁLIK, Daniel. Ochrana kritickej infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukture,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[6] PROCHÁZKOVÁ, Dana. Problém ochrany kritické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infreastrukturen*, konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

[7] URBÁNEK, Jiří. F. KELLNER, Josef, NAVRÁTIL, Josef. Úloha Univerzity obrany při ochraně kybernetické infrastruktury. In *Internationaler Erfahrungsaustausch Schutz Kritischer Infrastrukture,* konference 2.-3.10.2006. [CD-ROM]. Lázně Bohdaneč: Institut ochrany obyvatelstva, 2006.

WWW ČLÁNKY

[1]COLLINS, Pamela. *Critical Infrastructure and Continuity of Operations in a post 9/11 World.* [on-line]. [cit. 2009-02-17]. Dostupné z WWW: <http://www.jsc.eku.edu/docs/ Finland-Infrastructure%20Protection%20%20Presentation.ppt>.

[2] KRULÍK, O. *Fyzická ochrana kritické infrastruktury a klíčových aktivit* [on-line]. [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/rs_atlantic/data/files/insp_usa _infra.pdf>.

[3] LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. *112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva*. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.

[4] MARTÍNEK, Bohumír. Východiska a principy zajištění ochrany kritické infrastruktury v České republice. *112 – odborný časopis požární ochrany, integrovaného záchranného systému a ochrany obyvatelstva.* 2008, č. 4, s. 22 [cit. 2008-09-28]. Dostupné na WWW: <http://web.mvcr.cz/archiv2008/casopisy/112/2008/ duben/strana_22.html>.

[5] PROCHÁZKOVÁ, Dana. Komplexní pohled na problematiku bezpečnosti. *Veřejná správa* [on-line]. 2004, č. 35 [cit. 2008-10-11]. Dostupný z WWW: <http://aplikace.mvcr.cz /archiv2008/2003/casopisy/vs/ 0435/konz_info.html>.

[6] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj* [on-line]. 2007, roč. 10, č. 4 [cit. 2008-09-28]. Dostupný z WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.

[7] MULLER, Jan. *Kritická infrastruktura státu a ICT technologie* [on-line].[cit. 2009-02-25] Dostupné na WWW: <http://www.isss.cz/archiv/2004/download/prezentace/icz_muller .ppt>.

[8] SCHNEIDER, Jan. *Zpravodajské služby a ochrana kritické infrastruktury* [on-line].[cit. 2008-10-10]. Dostupné na WWW:<http://www.bezpecnostnimanagement.cz/www/files/File/ anotace/2D/Terorismus,%20krizove%20 rizeni/ANOT_Jan_Schneider.pdf>.

WWW STRÁNKY

[1] *Informace o dokumentech z bezpečnostní oblasti projednávaných vládou a BRS* [on-line]. Praha, 2008 [cit. 2008-10-07]. Dostupné z WWW: <http://www.chmi.cz/katastrofy/ bezradst1607.pdf>.

[2] *The USA Patriot Act*. Public Law 107-56. 2001. [on-line]. Electronic Privacy Information Centre. [cit. 2008-10-07]. Dostupné z WWW: <http://www.epic.org/privacy/terrorism/ usapatriot>.

[3]*V Hradci Králové bude vybudováno Národní centrum pro složky integrovaného záchranného systému*. [on-lin]. [cit. 2009-01-07]. Dostupné z WWW:http://www.rozhlas.cz /hradec/zpravy/_zprava/ 532571>.

[4] *Energy infrastructure: Studies* [on-line]. [cit. 2009-04-20]. Dostupné na WWW: <http://ec.europa.eu/energy/infrastructure/critical_en.htm>.

Příloha A: Sektory kritické infrastruktury podle „Národní strategie fyzické ochrany kritické infrastruktury“ v USA

Poř.	Sektory kritické infrastruktury	Charakteristika
1.	Zemědělství a potraviny (Agriculture and Food)	Jedná se o potravinové řetězce, živočišné a rostlinné produkty, osiva, průmyslová hnojiva a zásobovací potravinové řetězce, spojené s procesem výroby, prodeje a distribuce do maloobchodů, stravovacích zařízení, restaurací a domácí spotřeby.
2.	Voda (Water)	Tento sektor se skládá ze dvou základních komponentů: zásobování pitnou vodou a nakládání s odpadními vodami. Hlavní úsilí je zaměřeno na ochranu 170 000 veřejných vodovodních systémů, které jsou závislé na zásobnících, přehradách, vodních pramenech, jakož i na čisticím zařízení, čerpadlových stanicích, vodovodech a vodovodních potrubích.
3.	Veřejné zdraví (Public Health)	Sektor veřejného zdraví zahrnuje státní a místní zdravotnická střediska, nemocnice, zdravotnické kliniky, zařízení pro mentálně postižené, zařízení pro zásobování krví, laboratoře, domácí ošetřování, márnice farmaceutické zásoby.
4.	Nouzové služby (Emergency Services)	Infrastruktura nouzových služeb se skládá z požárnických služeb, záchranářských služeb a zdravotnických záchranných služeb a dalších organizací, které jsou dle zákona najímány k záchraně životů a majetku při nehodách, přírodních pohromách nebo teroristických akcích.
5.	Nouzové služby (Emergency services)	Infrastruktura nouzových služeb se skládá z požárnických služeb, záchranářských služeb a zdravotnických záchranných služeb a dalších organizací, které jsou dle zákona najímány k záchraně životů a majetku při nehodách, přírodních pohromách nebo teroristických akcích.
6.	Telekomunikace (Telecomunication)	Jedná se o telekomunikační sektor, poskytující hlasové a datové služby veřejným a soukromým uživatelů.
7.	Energetika (Energy)	Sektor energetiky je v kontextu ochrany kritické infrastruktury rozdělen do dvou segmentů: elektřinu a ropu a zemní plyn.
8.	Doprava (Transportation)	Sektor dopravy se skládá z následujících klíčových větví: letectví námořní dopravy, železniční dopravy, sítí produktovodů, dálniční dopravy, kamionové a autobusové dopravy a veřejné dopravy. Ochrana je zaměřena na 5 000 veřejných letišť, 120 000 mil. hlavních železničních tahů, 590 000 dálničních mostních konstrukcí a staveb, 2 mil. mil

		produktovodů, 300 vnitrozemních a pobřežních přístavů a 500 hlavních provozovatelů městské veřejné dopravy.
9.	Bankovnictví a finance (Banking and Finance)	Bankovní a finanční sektor je složen z hmotných struktur, zejména budov a vybavení pro finanční operace, a také lidského kapitálu.
10.	Chemický průmysl a nebezpečné látky (Chemical Industry and Hazardous Materials)	Chemický průmysl vyrábí produkty, které jsou nezbytné pro ekonomiku USA a tvoří fundamentální základ pro jiné ekonomické sektory. Například produkty chemického průmyslu, v hodnotě 97 mld. Dolarů, jdou do oblasti zdravotnické péče. Současný chemický průmysl je největším americkým exportérem. Ochrana je zaměřena na 66 000 chemických závodů.
11.	Poštovní a zásilkové služby (Postal and Shipping)	Americká státní poštovní služba, soukromé poštovní a zásilkové služby dosahují každoroční příjem, přesahujících 200 mld. dolarů. Denně více než 300 000 poštovních vozů dopraví poštou na více než 137 mil. adres. Americká poštovní služba má přes 749 000 zaměstnanců na plný pracovní úvazek. Poštovní systém je velmi závislý na ostatních infrastrukturních systémech, zejména na dopravním systému.

Pramen: LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. 112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.

Příloha B: Klíčová zařízení kritické infrastruktury podle „Národní strategie fyzické ochrany kritické infrastruktury“ v USA

Poř.	Klíčová zařízení kritické infrastruktury	Charakteristika
1.	Národní kulturní památky (National Monuments and Icons)	Ochrana národních kulturních památek představuje zvláštní úkol, protože jejich ochrana je kombinací pravomocí, odpovědnosti a zdrojů federální, státní a místní jurisdikce a v některých případech má soukromý charakter. Ochrana je zaměřena na 5 800 historických budov.
2.	Jaderné elektrárny (Nuclear Power Plants)	Jaderná energetika se podílí 20 % na výrobě elektrické energie. V USA se nachází 104 jaderné reaktory ve 31 státech.
3.	Přehrady (Dams)	Přehrady, jako další prvek kritické infrastruktury, poskytují vodu a elektrickou energii pro větší část populace, městské aglomerace a zemědělský komplex. V USA se nachází přibližně 80 000 přehrad. Federální vláda je odpovědna přibližně za 10 % vodních děl, jejichž zničení či poškození by způsobilo významné hospodářské škody nebo by mělo důsledky na veřejné zdraví a bezpečnost.
4.	Vládní zařízení (Government Facilities)	Před 11. 9. 2001 hlavní a nejdůležitější způsob ohrožení vládních budov a zařízení spočíval v použití výbušnin. Přestože tento způsob ohrožení zůstává jako hlavní, tak po 11. září 2001 možnosti ohrožení dostávají nové dimenze. Ochrana je zaměřena na 3 000 vládních budov a zařízení, vlastněných nebo provozovaných státem.
5.	Komerční klíčová zařízení (Commercial Key Assets)	Ochrana významných komerčních center, kancelářských budov, sportovních stadionů, významných parků a dalších míst, kde se koncentruje větší počet osob, je považována za významný úkol. Každodenní ochrana takovýchto zařízení je v kompetenci vlastníků a provozovatelů v těsné spolupráci s místními bezpečnostními subjekty. Odpovědnost federální vlády za ochranu těchto zařízení je považována více méně jako nepřímá, spočívajících zejména ve včasné indikaci ohrožení, varování a ve spolupráci s vlastníky při koordinaci ochrany jejich zařízení. Ochrana je zaměřena na 460 mrakodrapů.

Pramen: LINHART, Petr; RICHTER, Rostislav. Ochrana kritické infrastruktury [on-line]. 112 – odborný časopis požární ochrany integrovaného záchranného systému a ochrany obyvatelstva. 2003, č. 3 [cit. 2008-09-28]. Dostupný z WWW: <http://www.mvcr.cz/ casopisyú112/3/_2003/linhart.pdf>.

Příloha C: Kontrolní seznam pro hodnocení státu v oblasti ochrany kritické infrastruktury

1. oblast - řídící mechanismy	**Ano**	**Ne**
Je stanoven odpovědný gestor?		
Je ustanoven orgán pro ochranu KI legislativě?		
Je zajištěna koordinace ochrany KI?		
Je stanoven odborný subjekt/subjekty pro oblast KI?		
Je zaveden vhodný vzdělávací a výcvikový program pro osoby pracující v oblasti KI?		
Je vytvořen program na finanční zabezpečení plnění opatření pro ochranu KI?		
2. oblast - řídící dokumentace		
Je přijata koncepce zahrnující oblast KI?		
Je schválena koncepce KI?		
Je zpracována Komplexní strategie ochrany ČR (SR) pro oblast KI?		
Je zpracován Národní program na ochranu KI?		
Je do koncepčních materiálů týkajících se KI zahrnuta také oblast vzdělávání.		
Je do priorit a cílu výzkumně-vývojové podpory zahrnuta oblast ochrany KI?		
3. oblast - definice, pojmy a legislativa v oblasti KI		
Je vymezena definice KI?		
Jsou definice základních pojmů vymezené legislativou?		
Je stanoven přehled základních oblastí KI?		
Jsou vymezeny sektory KI?		
Jsou vymezeny prvky KI?		
Je vytvořen seznam nejdůležitějších objektů KI?		
Je seznam odvětví KI sjednocený s požadavky EU a NATO?		
Je zajištěn soulad základních pojmů (např. definice KI) s řešením Evropské kritické infrastruktury?		

Pramen: autorka

Příloha D: Seznam sektorů národní infrastruktury Slovenské republiky[93]

Ministerstvo	Sektor	Prvky
Ministerstvo hospodářství	**Sektor průmyslu**	**průmysl s výjimkou potravinářství a stavebních výrobků**
	Energetika	**těžba, přeprava, skladovaní, zpracování a úprava ropy a distribuce produktů ze zpracování ropy**
		těžba, přeprava, skladování, zpracování, úprava a distribuce plynu
		výroba elektřiny včetně výroby v jaderných elektrárnách, hospodaření s jaderným palivem, vyhořelým jaderným palivem a radioaktivním odpadem, přenos a distribuce elektřiny
		teplárenství
	Obchod	vnitřní obchod, zahraniční obchod
	Cestovní ruch	cestovní ruch
	Báňská činnost	**těžba a úprava rudných a nerudných surovin a vyhledávání a průzkum radioaktivních surovin**
Ministerstvo financí	Státní pokladna	státní pokladna
	Finanční trh	**bankovnictví**
		pojišťovnictví
		kapitálový trh
		devizové hospodářství
		specifický sektor v oblasti poskytování služeb
Ministerstvo dopravy, pošt a telekomunikací	**Doprava**	**dráhy a doprava na drahách**
		silniční doprava
		kombinovaná doprava
		pozemní komunikace
		vnitrozemská plavba a přístavy, námořní plavba
		civilní letectví
	Pošta	pošta (doprava zásilek, peněž a správa)
	Informační a komunikační systémy a technologie	**telekomunikace v rámci komunikačních systémů a technologií**
		informatizace společnosti v rámci IS a technologií
	Ozbrojené sbory v dopravě	ozbrojené sbory v dopravě
Ministerstvo vnitra	**Veřejný pořádek a**	ochrana ústavního zřízení
		ochrana veřejného pořádku, bezpečnosti osob a majetku
		ochrana a správa státních hranic
		ochrana ústavních činitelů, ochrana diplomatických misí a dalších objektů určených vládou
		bezpečnost a plynulost silničního provozu

[93] Tučně zvýrazněné sektory a prvky národní infrastruktury tvoří součást kritické infrastruktury SR.

	vnitřní bezpečnost	zbraně a střelivo
		soukromé bezpečnostní služby
		boji proti terorizmu, organizovanému zločinu a kriminalitě
		migrace (boj proti nelegální migraci, vstupný režim na území SR a pobyt cizinců na území)
		integrovaný záchranný systém
		Hasičský a záchranný sbor (ochrana před požárem, likvidace průmyslových havárií, přírodních katastrof a dopravních nehod spojených s únikem nebezpečných látek, síly a prostředky)
		civilní ochrana (vyrozumívajíc a varovný systém, síly a prostředky)
		civilní nouzové plánování
		automatizovaný informační systém MV SR a PZ
		policejní sbor, síly a prostředky
	Všeobecná vnitřní správa	všeobecná vnitřní správa v rámci věci územního a správního uspořádání SR
		výkon státní správy uskutečňované obcemi, VÚC a orgány místní státní správy (KU, ObÚ, speciální státní správa)
		informační systém
Ministerstvo půdního hospodářství	Sektor půdního hospodářství	**výroba potravin a bezpečnost potravin**
		zemědělská výroba
		lesní hospodářství
Ministerstvo výstavby a regionálního rozvoje	Regionální rozvoj	regionální rozvoj
	Výstavba	stavební výroba a stavební výrobky
	Bytová politika	tvorba a uskutečňovaní bytové politiky
Obrana státu a ozbrojené síly		řízení a kontrola obrany SR a plnění závazků vyplývajících z kolektivní obrany
		výstavba, řízení a kontrola ozbrojených sil SR
		koordinace činnosti a kontrola orgánů veřejné správy a jiných právnických osob při přípravě na obranu SR
		budování, obrana a ochrana vojenské obranné infrastruktury a obrana nevojenské obranné infrastruktury
		koordinace vojenského letového provozu s civilním letovým provozem
		vojenské zpravodajství
Ministerstvo spravedlnosti	Spravedlnost	soudy
		vězenství
Ministerstvo zahraničních věcí	Zahraniční politika	zahraniční politika a vztahy SR k ostatním státům a mezinárodním organizacím
		ochrana práv a zájmů SR a jejich občanů v zahraničí
		řízení zastupitelských úřadů SR v zahraničí
		styky s orgány a představiteli cizích států v SR a v zahraničí
		hospodaření a nakládání s majetkem SR v zahraničí

		koordinace přípravy a vnitřního projednáváni, uzavírání a vykonávání mezinárodních smluv
Ministerstvo práce, sociální věcí a rodiny	Ochrana práce Ochrana práce	pracovněprávní vztahy, právní vztahy při výkonu práce ve veřejném zájmu a právní vztahy volených funkcionářů orgánů územní samosprávy
		bezpečnost a ochrana zdraví při práci
		inspekce práce
	Zaměstnanost	strategie zaměstnanosti, koordinace její tvorby a realizace a politika trhu práce
	Sociální věci a rodina	sociální pojištění, starobní důchodové spoření a doplňkové důchodové spoření
		státní sociální dávky, sociální pomoc a pomoc v hmotné nouzi
		sociálně-právní ochrana dětí a koordinace státní rodinné politiky
		antidiskriminační politika a rovné příležitosti
Ministerstvo životního prostředí	Ochrana přírody a krajiny	ochrana přírody
		ochrana a regulace obchodu s ohroženými druhy volně žijících živočichů a volně rostoucích rostlin
		biologická bezpečnost
		posuzovaní vlivů na životní prostředí
		ochrana krajiny
	Složky životního prostředí	prevence závažných průmyslových havárií
		ochrana ovzduší
		odpadové hospodářství
		vodní hospodářství
	Geologické výzkum a průzkum	výzkum a vývoj geologické stavby území státu
		geologický výzkum a průzkum neobnovitelných surovinových zdrojů, zdrojů geotermální energie, zdrojů a zásob podzemních vod
		inženýrská geologie, ověřování geologických činitelů životního prostředí, geologický průzkum na speciální účely, t j. návrh sanací havarijních sesuvů a návrh na ochranu zdrojů podzemních vod
Ministerstvo kultury	Kultura	státní jazyk
		ochrana památkového fondu, kulturní dědictví a knihovnictví
		umění
		autorské právo a práva související s autorským právem
		osvětová činnost a lidová umělecká výroba
		podpora kultury národnostních menšin
		podpora kultury Slováků žijících v zahraničí
		prezentace slovenské kultury v zahraničí
		vztahy s církvemi a náboženskými společnostmi
		média a audioprostředky
Ministerstvo školství	Školství	základní školy, střední školy, vysoké školy
		školská zařízení
		celoživotní vzdělávání
		státní péče o mládež a sport

		věda a technika
Ministerstvo zdravotnictví	**Zdravotnictví**	zdravotní péče
		ochrana zdraví
		veřejné zdravotní pojištění
		další vzdělávání zdravotnických pracovníků
		přírodní léčivé koupele, přírodní léčivé zdroje, přírodní minerální vody
		cenová politika v oblasti cen výrobků, služeb a výkonů v zdravotnictví a v oblasti cen nájmu nebytových prostor ve zdravotnických zařízeních
Úřad vlády	Úřad vlády	kontrola plnění úloh souvisejících s výkonem státní správy, kontrola plnění úloh z usečení vlády, jakož i kontrola peticí a stížností.
Antimonopolní úřad	Hospodářská soutěž	ochrana a podpora hospodářské soutěže
Statistický úřad	Statistika	státní statistika
Úřad geodezie, kartografie a katastru	Geodézie, kartografie a katastr	geodézie, kartografie a katastr nemovitostí
Úřad jaderného dozoru	Jaderný dozor	dozor nad bezpečností jaderných zařízení
		přeprava a nakládání s jaderným materiálem, radioaktivními odpady a vyhořelým jaderným palivem
		fyzická ochrana jaderných zařízení, jaderných materiálů, radioaktivních odpadů a vyhořelého jaderného paliva a fyzická ochrana při přepravě radioaktivních materiálů
		dozor nad havarijní připraveností jaderných zařízení
Úřad pro normalizaci, metrologii a zkušebnictví	Normalizace, metrologie a zkušebnictví	technická normalizace, metrologie, kvalita a posouzení shody
Úřad pro veřejné zakázky	Sektor veřejných zakázek	veřejné zakázky
Úřad průmyslového vlastnictví	Průmyslové vlastnictví	průmyslové vlastnictví (ochrana vynálezu, užitných vzoru, designu, topografie polovodičového výrobku, ochranné známky, označování původu výrobku a zeměpisného označování výrobků)
Správa státních hmotných rezerv	Správa rezerv	státní hmotné rezervy
		koordinace a metodické usměrňování opatření na řešení stavu ropné krize
Národní bezpečnostní úřad	Utajované skutečnosti	ochrana utajovaných skutečností, šifrovací služba a elektronických podpis
Průřezové sektory	**Informační systémy**	**ochrana informačních systémů je v kompetenci jednotlivých rezortů**

Pramen: Ministerstvo vnitra SR. Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany [on-line]. Bratislava, 2006. 19 s. [cit. 2008-10-12]. Dostupné z WWW: <http://www.minv.sk>.