

**Univerzita Pardubice**  
**Fakulta ekonomicko-správní**

**Ochrana kritické infrastruktury v ČR a zahraničí**

**David Myslikovjan**

**Bakalářská práce**

**2009**

Univerzita Pardubice  
Fakulta ekonomicko-správní  
Ústav systémového inženýrství a informatiky  
Akademický rok: 2008/2009

## **ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **David MYSLIKOVJAN**  
Studijní program: **B6209 Systémové inženýrství a informatika**  
Studijní obor: **Informatika ve veřejné správě**

Název tématu: **Kritická infrastruktura v ČR a v zahraničí**

### **Z á s a d y p r o v y p r a c o v á n í :**

- 1) Základní pojmy
- 2) Legislativa
- 3) Kritická infrastruktura v ČR
- 4) Kritická infrastruktura v zahraničí
- 5) Zhodnocení

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

[1] KARDA, L., KUDLÁK, A. Analýza, metody a nástroje řešení krizových situací. České Budějovice, 2007.

[2] LINHART, P. Některé otázky ochrany společnosti. Praha: MV-GŘ HZS ČR, 2005. ISBN 80-86640-43-4.

[3] PROCHÁZKOVÁ, D., ŘÍHA, J. Krizové řízení. Praha: MV-GŘ HZS ČR, 2004. ISBN 80-86640-30-2.

Vedoucí bakalářské práce:



Ing. Tomáš Kořínek

Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce:

6. října 2008

Termín odevzdání bakalářské práce:

1. května 2009



doc. Ing. Renáta Myšková, Ph.D.

děkanka

L.S.



doc. Ing. Jiří Krupka, Ph.D.

vedoucí ústavu

V Pardubicích dne 6. října 2008

**Prohlašuji:**

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

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice..

V Pardubicích dne 15.8. 2009

David Myslikovjan

# ANOTACE

Tato práce se zabývá ochranou kritické infrastruktury v zemích Evropy. Především se zaměřuje na Českou republiku a Evropskou unii, ale popisuje i situaci ochrany kritické infrastruktury v dalších zemích Evropy.

Nejdříve jsou vysvětleny základní pojmy, které se týkají problematiky kritické infrastruktury, a pak je popisována její ochrana v rámci Evropské unie. Další text je věnován ochraně kritických infrastruktur ve vybraných zemích Evropy. Jako poslední je uvedeno srovnání různých oblastí KI ve sledovaných zemích.

# KLÍČOVÁ SLOVA

Evropská unie, Kritická infrastruktura, EPCIP, Krizové řízení, Ochrana kritické infrastruktury, Oblasti kritické infrastruktury, Zelená kniha.

# TITLE

Critical infrastructure protection in Czech republic and abroad.

# ANOTATION

This work is concerned with Critical infrastructure protection. It is focus on Czech republic and European Union, but describes critical infrastructure in other european countries.

In first chapter are explaining of the fundamental terms which concern the critical infrastructure protection and then is described its protection within the European Union. Next the text is devoted to the protection of critical infrastructures in selected countries in Europe. As a last comparison is given to different areas of KI in the countries.

# KEYWORDS

European Union, Critical Infrastructure, EPCIP, Crisis Management, Critical Infrastructure Protection, Sectors of critical infrastructure, Green Paper

# Obsah

|          |                                                                                                        |           |
|----------|--------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>ZÁKLADNÍ POJMY</b>                                                                                  | <b>9</b>  |
| 1.1      | Kritická infrastruktura                                                                                | 9         |
| 1.1.1    | Počátky KI                                                                                             | 9         |
| 1.2      | Hrozba a riziko                                                                                        | 10        |
| 1.2.1    | Hrozba                                                                                                 | 10        |
| 1.2.2    | Riziko                                                                                                 | 12        |
| 1.3      | Krizový plán                                                                                           | 12        |
| 1.4      | Subjekty kritické infrastruktury                                                                       | 12        |
| 1.5      | Objekty kritické infrastruktury                                                                        | 12        |
| <b>2</b> | <b>OCHRANA KRITICKÉ INFRASTRUKTURY V EVROPSKÉ UNII</b>                                                 | <b>13</b> |
| 2.1      | Vznik a historie Evropské unie                                                                         | 13        |
| 2.2      | Orgány Evropské unie                                                                                   | 14        |
| 2.2.1    | Rada Evropské unie                                                                                     | 14        |
| 2.2.2    | Evropská rada                                                                                          | 15        |
| 2.2.3    | Evropský parlament                                                                                     | 15        |
| 2.2.4    | Evropská komise                                                                                        | 15        |
| 2.2.5    | Další evropské významné instituce                                                                      | 16        |
| 2.3      | Důležitost ochrany kritické infrastruktury na Evropské úrovni                                          | 16        |
| 2.4      | Jednotlivé oblasti kritické infrastruktury EU                                                          | 17        |
| 2.5      | Hlavní dokumenty EU týkající se kritické infrastruktury vydané Evropskou unií                          | 18        |
| 2.5.1    | Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“ | 18        |
| 2.5.2    | Zelená kniha „O evropském programu na ochranu kritické infrastruktury“                                 | 18        |
| 2.5.3    | Sdělení Komise „O Evropském programu na ochranu kritické infrastruktury“                               | 19        |
| 2.6      | Evropský program na ochranu kritické infrastruktury (EPCIP)                                            | 19        |
| 2.6.1    | Cíle EPCIP                                                                                             | 19        |
| 2.6.2    | Základní principy spolupráce v EPCIP                                                                   | 20        |
| 2.6.3    | Společný rámec EPCIP                                                                                   | 21        |
| 2.7      | Úrovně kritické infrastruktury                                                                         | 22        |
| 2.7.1    | Kritická infrastruktura na úrovni evropské unie (ECI)                                                  | 22        |
| 2.7.2    | Národní kritická infrastruktura (NCI)                                                                  | 22        |
| 2.7.3    | Výstražná informační síť kritické infrastruktury (CIWIN)                                               | 23        |
| 2.8      | Hrozby, které nejvíce ohrožují kritickou infrastrukturu Evropy.                                        | 23        |
| 2.8.1    | Terorismus                                                                                             | 24        |
| 2.8.2    | Šíření zbraní hromadného ničení                                                                        | 24        |
| 2.8.3    | Regionální konflikty                                                                                   | 24        |
| 2.8.4    | Zhroucení státní moci                                                                                  | 24        |
| 2.8.5    | Organizovaný zločin                                                                                    | 25        |
| 2.9      | Zhodnocení                                                                                             | 25        |

|            |                                                                               |           |
|------------|-------------------------------------------------------------------------------|-----------|
| <b>3</b>   | <b>KI VE VYBRANÝCH ZEMÍCH EVROPSKÉ UNIE</b>                                   | <b>26</b> |
| <b>3.1</b> | <b>Česká republika</b>                                                        | <b>26</b> |
| 3.1.1      | Ochrana KI                                                                    | 27        |
| 3.1.2      | Historie KI v ČR                                                              | 28        |
| 3.1.3      | Jednotlivé oblasti kritické infrastruktury České republiky                    | 30        |
| 3.1.4      | Zákony, předpisy a nařízení, týkající se ochrana KI v ČR                      | 31        |
| 3.1.5      | Největší rizika, která mohou vést k narušení infrastruktury v České republice | 31        |
| 3.1.6      | Financování kritické infrastruktury                                           | 33        |
| 3.1.7      | Krizové řízení                                                                | 33        |
| 3.1.8      | Orgány krizového řízení                                                       | 34        |
| 3.1.9      | Ochrana obyvatelstva v ČR                                                     | 35        |
| 3.1.10     | Zhodnocení                                                                    | 35        |
| <b>3.2</b> | <b>Německo</b>                                                                | <b>37</b> |
| 3.2.1      | Vývoj Ochrany kritické infrastruktury v Německu                               | 38        |
| 3.2.2      | Řešení ochrany kritické infrastruktury                                        | 40        |
| 3.2.3      | Jednotlivé oblasti kritické infrastruktury Německa                            | 40        |
| 3.2.4      | Nebezpečí, která mohou vést k narušení infrastruktury v Německu               | 41        |
| 3.2.5      | Orgány zabývající se ochranou kritické infrastruktury v SRN.                  | 42        |
| 3.2.6      | Národní plán na ochranu kritické infrastruktury v Německu                     | 44        |
| 3.2.7      | Zhodnocení                                                                    | 45        |
| <b>3.3</b> | <b>Švýcarsko</b>                                                              | <b>46</b> |
| 3.3.1      | Základní informace o kritické infrastruktuře                                  | 47        |
| 3.3.2      | Jednotlivé oblasti kritické infrastruktury Švýcarska                          | 48        |
| 3.3.3      | Orgány zabývající se ochranou kritické infrastruktury ve Švýcarsku            | 49        |
| 3.3.4      | Nebezpečí, která mohou vést k narušení infrastruktury ve Švýcarsku            | 50        |
| 3.3.5      | Zapojení kantonů a soukromého sektoru.                                        | 50        |
| 3.3.6      | Současné projekty Švýcarska                                                   | 51        |
| 3.3.7      | Zhodnocení                                                                    | 51        |
| <b>3.4</b> | <b>Porovnání zemí ve vybraných oblastech</b>                                  | <b>52</b> |
| 3.4.1      | Oblasti začleněné do kritické infrastruktury                                  | 52        |
|            | Odpovědné subjekty                                                            | 54        |
| 3.4.2      | Uvažovaná rizika a hrozby                                                     | 55        |

## Úvod

Žijeme v Evropě na začátku 21. století. Snad v celé historii našeho kontinentu, ale i celého světa, by se nenašla doba, která by byla více bezpečná než je ta dnešní. Nacházíme se v období, kdy naše životy nejsou ohroženy žádnou válkou, nebezpečnými epidemiemi moru, cholery, tyfu a jiných nemocí. Každý máme svůj domov se zavedeným plynem a elektřinou, což dělá náš život kvalitnější a pohodlnější. Můžeme mezi sebou komunikovat pomocí internetu, telefonicky atd. Využíváme služeb finančních ústavů, nemocničních zařízení, potravinových řetězců. Naše mobilita je zajištěna vynikající dopravní infrastrukturou a službami, které nám poskytují dopravní společnosti. Takto by se dalo pokračovat až do nekonečna.

Všechny tyto vyjmenované aspekty - a je jich pochopitelně mnohem víc - tvoří takzvanou kritickou infrastrukturu. Moderní společnost je na této infrastruktuře a pochopitelně na její plné funkčnosti naprosto závislá a její selhání by pak mělo naprosto katastrofální důsledky na kvalitu lidského života. Tento fakt si ovšem málokdo z nás uvědomuje. Většinou fungování kritické infrastruktury považujeme za samozřejmé a ani si neuvědomíme její křehkost a fakt, že je třeba ji chránit.

Jak již bylo řečeno, skládá se systém kritické infrastruktury z mnoha částí. A proto připomíná řetěz, kde platí, že pevnost tohoto řetězu rovná se pevnosti jeho nejslabší části. Pro kritickou infrastrukturu platí to samé, a to je důležité si při její ochraně uvědomit.

A právě kritickou infrastrukturou se zabývá i tato bakalářská práce. Jejím cílem je ukázat, jak vypadá její ochrana v České republice, Evropské unii a ve vybraných státech Evropy. Nejdříve jsou v ní objasněny základní pojmy, které s touto problematikou souvisí. Dále je pak popsáno, jak vypadá její ochrana v Evropské unii. Následně je tato ochrana popsána ve vybraných státech. Jsou zde dokumenty, které jsou významné pro ochranu kritické infrastruktury, její vznik a vývoj, důležité orgány, které ji řídí, jednotlivé oblasti i rizika, které jednotlivé státy považují za nejvíce nebezpečné.



Pro porovnání byly zvoleny tři země Evropy, a sice Česká republika, Německo a Švýcarsko. Volbu České republiky ukládá téma. Cílem je vybrat si k porovnání státy, ležící zhruba ve stejném regionu jako Česká republika, tedy státy v oblasti střední Evropy. Jako první padla volba na Německo. Je to jedna z největších zemí Evropy s velmi dobrou ekonomikou a velkým vlivem. Jedná se o našeho významného partnera.

Třetí porovnávanou zemí je Švýcarsko. Tento stát je zajímavý především tím, že .je dáván České republice za vzor dokonalé země, která navzdory své velikosti, málo příznivým geografickým podmínkám, nedostatku nerostných surovin a jiných nevýhod, dosáhla nejen celoevropského, ale i světového významu.

# 1 Základní pojmy

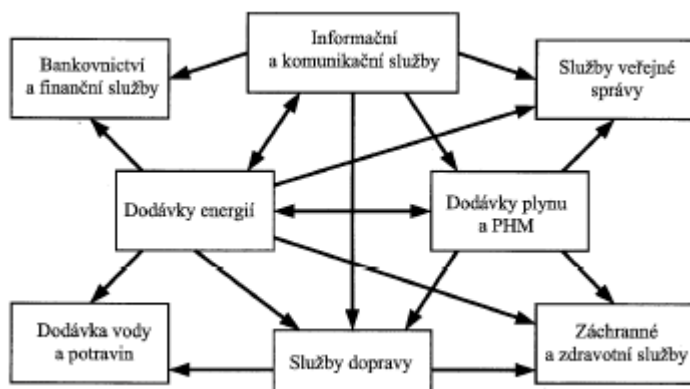
## 1.1 Kritická infrastruktura

Kritickou infrastrukturou rozumíme takovou infrastrukturu, která má rozhodující význam pro fungování společnosti. Úkolem společnosti je tuto infrastrukturu chránit. [12]

Existuje celá řada definic kritické infrastruktury. Jedna z nich říká, že „Kritické infrastruktury se skládají z takových fyzických a informačních technologií, sítí, služeb a majetku, které by v případě jejich zničení nebo narušení měly vážný dopad na zdraví, bezpečnost, ekonomický blahobyt občanů, či efektivní fungování“ [5]

Při její ochraně je dobré si uvědomit, že pokud máme chránit jednotlivé části kritické infrastruktury, musíme chránit kritickou infrastrukturu jako celek.

Na obrázku 1 vidíme příklad takové infrastruktury, na které je vidět, že narušení jedné oblasti by vedlo k narušení její funkčnosti až k jejímu úplnému zhroucení..



Obrázek 1 - Příklad sítě kritické infrastruktury [18]

### 1.1.1 Počátky KI

Problematika její ochrany se stále vyvíjí a mění. Postupně se mění i důvody k její ochraně, a to podle toho, jaké nebezpečí jejího narušení hrozí. Lidstvo se odjakživa obávalo různých katastrof. Největšími hrozbami byly války. V minulém století znamenaly 1. a 2. světová válka obrovskou katastrofu pro celý svět. Především v období studené války to byla hrozba jaderného napadení, později pak nebezpečí, plynoucí z následků živelných katastrof a terorismu.

Kvůli těmto hrozbám různých katastrof začaly vznikat projekty na ochranu KI. Vychází se z toho, že každé nebezpečí může omezit nebo dokonce vyřadit nějaký životně důležitý prvek společnosti (např. dodávky energií či potravin, právo na lékařskou péči atd.), a proto všechny prvky, které jsou takto ohroženy, jsou včleněny do systému KI. [13]

V každé zemi se tyto prvky mohou lišit v závislosti na přírodních i jiných podmínkách (např. Česká republika se nemusí obávat katastrofy tsunami), ale ty základní jsou vždy stejné. Stát má být vždy připraven těmto mimořádným situacím čelit.

Prvními státy, které se začaly o problém ochrany KI zajímat, byly USA a Austrálie. Právě americký prezident Bill Clinton vydal v roce 1998 dokument s názvem **White Paper** (Bílá kniha). Tato směrnice se stala prvním uceleným materiálem, který se zabýval problémy ochrany kritické infrastruktury.

Hlavním cílem Bílé knihy byla opatření, která by zamezila „hmotným a kybernetickým útokům na kritickou infrastrukturu“. Její podstatnou součástí pak byl požadavek na rozšíření povinností a pravomocí na OKI ke všem participujícím subjektům, jak z veřejného tak i soukromého sektoru. [13]

Dalším milníkem při OKI se staly teroristické útoky v září 2001. Tím se stala hrozba terorismu hlavním bodem kritické infrastruktury.

Pokud jde o Evropskou unii, ta začala svojí aktivitu v oblasti OKI roce 2004 dokumentem s názvem - **Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“**

V České republice se problém OKI objevuje v dokumentech z roku 2002 **Rozsah základních funkcí státu a Informace o národní kritické infrastruktuře a návrh zásad na její zabezpečení**. [9]

## **1.2 Hrozba a riziko**

### **1.2.1 Hrozba**

„Jakýkoli fenomén, který má potenciální schopnost poškodit chráněné zájmy objektu. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.“ [10]

Po skončení studené války se začaly objevovat nové hrozby a rizika. Stálou hrozbu přinášejí státy a nevládní organizace, pro které je typické, že nerespektují mezinárodní právo a k prosazování svých vlastních zájmů využívají metody války, násilí a porušování základních lidských práv. Způsob, kdy určité skupiny prosazují své zájmy, se nazývá terorismus a extremismus. Další hrozby pak představuje použití zbraní hromadného ničení, regionální konflikty atd. V poslední době se objevují hrozby spojené s pronikáním do elektronických a informačních systémů.

Zvláštním skupinou je pak narušení životního prostředí v důsledku lidské činnosti. To má za následek živelné pohromy, klimatické změny, epidemie a jiné.

**Většina evropských států se soustředí především na tato rizika[2]**

- Přírodní katastrofy
- Technogenní katastrofy
- Narušení životního prostředí v důsledku antropogenní činnosti
- Poruchy v zásobování
- Epidemie
- Masová migrace
- Organizovaná kriminalita
- Terorismus a extremismus
- Obchod s drogami
- Nekontrolovatelné šíření zbraní hromadného ničení

### **1.2.2 Riziko**

„Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vycházejí i z posouzení naší připravenosti hrozbám čelit.“ [10]

**Rizika dělíme podle původce na[1] :**

- Antropogenní – způsobené činností člověkem (provozní havárie...)
- Přírodní – způsobené činností přírody (živelné pohromy...)

### **1.3 Krizový plán**

Při OKI hraje velmi důležitou roli. Jde o plánovací dokument, ve němž orgány k tomu zákonem určené, plánují opatření a postupy, které pak uplatní při vzniku krizových situací. [1]

V České republice je definován jako „soubor dokumentů, obsahující popis a analýzu hrozeb a souhrn krizových opatření a postupů, které ministerstva, jiné správní úřady a orgány územní samosprávy zpracovávají k zajištění připravenosti na řešení krizových situací v dané působnosti dle zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů.“ [10]

### **1.4 Subjekty kritické infrastruktury**

Jsou to vlastníci a provozovatelé, kteří provozují vybraná zařízení a objekty, poskytují služby a vyvábí produkty v jednotlivých oblastech KI. [1]

### **1.5 Objekty kritické infrastruktury**

Objekty kritické infrastruktury jsou stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické infrastruktury[1]

## 2 Ochrana kritické infrastruktury v Evropské unii

Evropská unie má v současné době 27 členských států a téměř půl miliardy obyvatel. Již od svého založení se snaží zajistit svým občanům prosperitu a stabilitu. Ať si to uvědomujeme, či ne, její politika a činnost se nás všech přímo či nepřímo dotýká.

Evropská unie se snaží o to, aby byla spravedlivou společností, která pečuje o své občany. Snaží se podporovat hospodářskou prosperitu a vytvářet nová pracovní místa. [19]

### Základní údaje o Evropské unii

|                               |                              |
|-------------------------------|------------------------------|
| Počet členských států:        | 27                           |
| Počet obyvatel(mil):          | 499, 673                     |
| Rozloha (km <sup>2</sup> ):   | 4 325 675                    |
| HDP na obyvatele v USD (PPS): | 33 400                       |
| Hlavní sídla:                 | Brusel, Štrasburg, Lucemburk |

### 2.1 Vznik a historie Evropské unie

Hlavním důvodem vzniku Evropské unie bylo ukončit časté a krvavé války mezi jednotlivými státy Evropy, jež dosáhly vrcholu během druhé světové války. Jako začátek historie vzniku tohoto společenství by se dal označit rok 1950, kdy začíná hospodářské a politické sjednocování zemí Evropy do Evropského společenství uhlí a oceli, jehož cílem je dosáhnout trvalého míru. V roce 1957 vzniká Římská smlouva, kterou se zakládá Evropské hospodářské společenství (EHS) – jedná se o úmluvu o společném trhu.

V 60. letech 20.stol. se začíná hospodářství zemí, která jsou členy EHS, rozvíjet. Velkou zásluhu na tom má i to, že tyto země při zahraničním obchodu neuplatňují cla. Členské země také používají společnou kontrolu produkce potravin za účelem garance dostatku potravin pro všechny. K zemím EHS (Belgie, Francie, Itálie, Lucembursko, Nizozemsko a Německo) přibývají k 1.lednu 1973 další tři země – Dánsko, Irsko a Spojené království. Během 70. let postupně narůstal vliv Evropského parlamentu a jeho poslance už mohli občané v roce 1979 volit přímo.

Roku 1981 přistupuje i Řecko a v r. 1986 Španělsko a Portugalsko. V tomto roce je podepsán i Jednotný evropský akt. V této smlouvě je představen šestiletý program nařešení problémů volného obchodu mezi státy EU – jde tedy o jednotný trh. Když v roce 1989 padla Berlínská zeď, mohlo být do EU přibrána i bývalá NDR – tím že se připojila k SRN. Dalšími významnými daty při dotváření evropské unie jsou rok 1993, kdy vstupuje v platnost „Maastrichtská“ smlouva o Evropské unii. Od roku 1999 pak platí Amsterodamská smlouva. Mezitím roku 1995 vstupují do EU Finsko, Rakousko a Švédsko. Postupně, díky Schengenské dohodě lze cestovat přes hranice EU bez pasových kontrol.

Velmi významným dnem pro Evropskou unii je i 11.září 2001 – den kdy byl spáchán teroristický útok na New York a Washington. Od tohoto dne začíná válka EU proti terorismu. Členské země utužují spolupráci boje proti trestné činnosti. Roku 2004 vstupuje do EU 10 zemí (jsou to především státy bývalého východního bloku), mezi nimi i Česká republika. V současné době jsou na programu dne snahy o to, aby Evropská unie měla svoji ústavu. Zatím jsou tyto pokusy neúspěšné. [19]

## **2.2 *Orgány Evropské unie***

Evropská unie není pouze konfederací států nebo federální stát. Jedná se o nový typ právní kategorie, který se vyvíjí již více než 50 let.

Důležitost orgánů Evropské unie spočívá v tom, že přebírá ty pravomoci, které byly dříve v kompetenci orgánů a institucí jednotlivých členských států. Nejdůležitější trojúhelník institucí, které vytvářejí předpisy a politiky EU, je tvořen Radou(zastupuje vlády členských států), Evropskou komisí a Evropským parlamentem (zastupuje občany) [19]

### **2.2.1 Rada Evropské unie**

Je známá též jako „Rada ministrů“ nebo jen „Rada“. Jedná se o hlavní rozhodovací orgán EU. Členské státy unie se střídají každého půl roku v předsednictví této instituce. V první polovině roku 2009 předsedala Česká republika. Na každém zasedání Rady se účastní jeden ministr z každého členského státu. Výběr ministra je závislý na projednávané agendě – může být projednáváno zemědělství, průmysl atd.

Rada sdílí s Evropským parlamentem legislativní pravomoc a spolu s ním také schvaluje rozpočet EU. Další její funkcí je uzavírání dohod vyjednané Komisí

Počet hlasů každého státu v radě se odvíjí podle počtu obyvatel. [19]

### **2.2.2 Evropská rada**

Tento orgán se setkává čtyřikrát za rok. V čele stojí prezident nebo předseda vlády země, která v daném období předsedá radě unie.

Podle Maastrichtské smlouvy je Evropská rada ustanovena za iniciátora hlavních politik Unie a řeší naléhavé mezinárodní problémy v rámci společné zahraniční a bezpečnostní politiky. [19]

### **2.2.3 Evropský parlament**

Poslanci evropského parlamentu jsou od roku 1979 voleni lidem zemí Evropské unie. Jeho úkolem je politický dohled nad činností EU a podílí se na legislativních záležitostech. Volby se konají za 5 let.

Plenární zasedání Evropského parlamentu se konají ve Štrasburku. Jinak Evropský parlament zasedá v Bruselu.

Účast na legislativě je trojí úrovně:

- Postup „spolupráce“ - parlament se vyslovuje k návrhům směrnic a nařízení připravených evropskou komisí
- Postup „souhlas“ - parlament musí schválit mezinárodní dohody vyjednané Komisí a také jí navrhované rozšíření Evropské unie.
- Postup „spolurozhodování“ – umožňuje Parlamentu užívat stejné pravomoci jako Radě při přijímání legislativy, která se týká celé řady významných otázek jako je např. volný pohyb pracovních sil, vzdělávání, výzkum, životní prostředí atd.

Spolu s radou nese odpovědnost za rozpočet EU, a může, jak již několikrát udělal, rozpočet zamítnout. Vykonává kontrolu nad unií. Může rozpustit komisi a kladě Komisi a Radě písemné dotazy, které slouží jako kontrola ke každodennímu řízení politik EU[19]

### **2.2.4 Evropská komise**

Je posledním orgánem ze tří nejvýznamnějších, které řídí a spravují Evropskou unii. Členové Komise jsou jmenováni na 5 let. Tato instituce je odpovědná parlamentu a pokud jí Parlament vyjádří nedůvěru musí rezignovat.



Komise je při vykonávání svých pravomocí do značné míry nezávislá. Zajišťuje provádění nařízení směrnic přijatých Radou a Parlamentem v členských státech. V případě jejich neuplatňování může podat na zemi, neplnící své povinnosti žalobu)

Dále provádí rozhodnutí Rady. Má širokou pravomoc při řízení společných politik EU. Sídlí v Bruselu a Lucemburku. [19]

### **2.2.5 Další evropské významné instituce**

Níže uvedeny jsou některé z dalších významných evropských institucí [19]

- Soudní dvůr
- Účetní dvůr
- Evropský hospodářský a sociální výbor
- Výbor regionů
- Evropská investiční banka
- Evropská centrální banka

## **2.3 *Důležitost ochrany kritické infrastruktury na Evropské úrovni***

Ačkoliv je ochrana obyvatelstva a s ním související KI vymezena hlavně legislativními předpisy každého konkrétního členského státu, ukazuje se rostoucí potřeba co největší standardizace. Přírodní i technogenní katastrofy, tak i ozbrojené konflikty, se dost často neomezují jen hranicemi určitého státu, ale velmi často působí i za jeho hranicemi. Tato potřeba zesílila především po zářijových událostech roku 2001. [2]

Na základě principu subsidiarity, který je zakotven v čl. 5 smlouvy o založení Evropského společenství (dále jen „Společenství“), je ochrana obyvatelstva věcí členských států Evropské unie. Zároveň ale existuje v oblasti ochrany obyvatelstva při závažných přírodních a antropogenních katastrofách řada aktivit na úrovni Unie. Počátek evropské spolupráce v této oblasti se datuje rokem 1985, kdy byla předložena tzv. Zelená kniha Evropské komise s názvem „Péče o naše životní prostředí – akce pro evropské životní prostředí“. [1]

## 2.4 *Jednotlivé oblasti kritické infrastruktury EU* [4]

- **Energetika** (produkce ropy a plynu, rafinování, zpracování, skladování a distribuce potrubím, výroba a rozvod elektřiny)
- **Jaderný průmysl** (produkce, skladování a zpracování jaderných látek)
- **Informační a komunikační technologie** (ochrana informačních systémů a sítí, automatizace přístrojů a kontrolních systémů, internet, poskytování pevných telekomunikačních sítí, radiová komunikace a navigace, satelitní komunikace, vysílání)
- **Voda** (zásobování pitnou vodou, kontrola kvality vody, těsnění a kontrola množství vody)
- **Potraviny** (zásobování potravinami a zajištění bezpečnosti potravin)
- **Ochrana zdraví** (lékařská a nemocniční péče, léky, séra, očkovací látky a léčiva, biologičtí činitelé)
- **Finančnictví** (infrastruktury a systémy zúčtování a vypořádání obchodů s cennými papíry, regulované trhy)
- **Doprava** (Silniční, železniční, letecká, vnitrozemská vodní, zámořská a příbřežní námořní doprava)
- **Chemický průmysl** (produkce a skladování/zpracování chemických látek, potrubí pro přepravu nebezpečných látek)
- **Vemír**
- **Výzkumná zařízení**

## ***2.5 Hlavní dokumenty EU týkající se kritické infrastruktury vydané Evropskou unií***

### **2.5.1 Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“**

Po 11. září 2001 se začaly množit debaty o bezpečnosti západního světa a především jeho připravenosti na obranu před hrozbou terorismu. Proto v červnu 2004 požádala Evropská rada Komisi, aby posoudila schopnost členských států předcházet a čelit teroristickým útokům a aby připravila celkovou strategii na ochranu kritické infrastruktury. Odpověď na tuto žádost přišla 20.10.2004, kdy bylo vydán dokument Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“. [5]

Toto sdělení se stalo prvním uceleným dokumentem týkajícím se ochrany kritické infrastruktury Evropské unie. Dokument obsahuje souhrn opatření za účelem posílení stávajících nástrojů a splnění úkolů uložených Evropskou radou.

Směrnice obsahuje mimo jiné rozebírání termínu KI, definování jednotlivých prvků KI, či výčet možných hrozeb. Uvádí se zde, že každý členský stát si má stanovit infrastrukturu, která je pro něj kritická, v souladu s postupem EU, a také organizace nebo osoby odpovědné za jeho bezpečnost.

Komise také navrhuje zřídit Evropský program na ochranu kritické infrastruktury (EPCIP) a Výstražnou informační síť kritické infrastruktury (CIWIN)

### **2.5.2 Zelená kniha „ O evropském programu na ochranu kritické infrastruktury“**

Hlavním cílem Zelené knihy je do EPCIP zainteresovat velké množství subjektů a získat tak od nich konkrétní informace o politikách, které by se pro tento program hodily nejlépe. Zelená kniha ve své 2. kapitole říká že: „Účinná ochrana kritické infrastruktury vyžaduje komunikaci, koordinaci a spolupráci jak na národní, tak na evropské úrovni, a to mezi všemi zainteresovanými subjekty – vlastníky a provozovateli infrastruktur, regulačními orgány, profesními organizacemi a odvětvovými sdruženími, stejně jako všech úrovní státní a veřejné správy a také veřejnosti.“ [4]

Tento dokument navrhuje možnosti, které si Komise může zvolit, aby uspokojila požadavky Rady na zřízení EPCIP a CIWIN, a začíná tak druhou fázi konzultací, které mají za cíl zavést Evropský program na ochranu kritické infrastruktury.

Z tohoto sdělení se také dozvídáme hlavní cíl EPCIP. Tento program má zajistit, aby v celé Evropské unii „existovala přiměřená a rovnoměrná úroveň bezpečnostní ochrany kritické infrastruktury, co nejméně možností selhání a rychlá, vyzkoušená nápravná opatření.“ Úroveň ochrany by podle Zelené knihy neměla být stejná pro všechny KI, ale měla by se odvíjet od dopadů, jež by mohlo způsobit jich možné selhání.

Dalšími důležitými body této směrnice je návrh základních principů EPCIP, definování kritické infrastruktury na národní i na evropské úrovni, včetně vymezení rolí vlastníků, uživatelů a provozovatelů KI. V poslední části nazvané „Podpůrná opatření pro EPCIP“ je blíže vysvětlená Výstražná informační síť KI (CIWIN) a také objasněny otázky související s financováním tohoto programu. [4]

### **2.5.3 Sdělení Komise „O Evropském programu na ochranu kritické infrastruktury**

Tento dokument z prosince 2006 „obsahuje zásady, postupy a nástroje, navrhované s cílem zavést systém EPCIP. Zavádění systému EPCIP bude případně doprovázeno sděleními pro jednotlivá odvětví, která stanoví přístup Komise, týkající se určitých odvětví kritické infrastruktury.“ [6]

## **2.6 *Evropský program na ochranu kritické infrastruktury (EPCIP)***

Základní myšlenka Evropské unie o společném rámci ochrany kritické infrastruktury, který bude platný ve všech členských zemích, byla realizována díky EPCIP.

Tento program je poprvé zmiňován ve sdělení z října 2004 „Ochrana kritické infrastruktury v boji proti terorismu“, a blíže specifikovaný v dokumentech „Zelená kniha“ a Sdělení Komise „O Evropském programu na ochranu kritické infrastruktury“ [4]

### **2.6.1 Cíle EPCIP**

Program si klade za cíl, aby byla v Evropské unii zajištěna přiměřená a rovnoměrná úroveň bezpečnosti ochrany kritické infrastruktury, aby se objevovalo co nejméně možností selhání a nápravná opatření byla rychlá a vyzkoušená. V úvahu je bráno i to, že úroveň ochrany nebude stejná pro všechny kritické infrastruktury, ale bude se odvíjet od dopadů, které by byly způsobeno jejím možným selháním[4]

Dalším úkolem EPCIP bude snižovat negativní dopady, které zvýšené investice na ochranu mohou působit konkurenceschopnosti daného odvětví. [4]

## 2.6.2 Základní principy spolupráce v EPCIP

### ➤ Subsidiarita

Tento princip vyjadřuje fakt, že ochrana infrastruktury na národní úrovni je především v kompetenci jednotlivých států. Hlavní odpovědnost za její ochranu tedy především spadá pod členskou zemi EU. Komise se má zaměřit jen na případy spojené s ochranou kritických infrastruktur, které přesahují hranice těchto zemí.

### ➤ Doplnkovost

Jedná se o to, aby bylo zabráněno, že evropské úsilí na ochranu kritické infrastruktury bude uplatňováno tam, kde již s úspěchem působí ochrana na vnitrostátní či regionální úrovni. EPCIP jen bude navazovat na již existující opatření a doplňovat je.

Informace o ochraně kritické infrastruktury budou utajovány jak na evropské úrovni, tak na úrovni jednotlivých členských států. Přístup k těmto informacím bude možný jen v případě potřeby.

### ➤ Spolupráce zainteresovaných subjektů

Všechny subjekty kritické infrastruktury se zapojí do rozvoje a provádění EPCIP

### ➤ Proporcionalita

Opatření se budou provádět jen tam, kde byla na základě nějakého předchozího rozboru současných nedostatků bezpečnosti zjištěna jejich potřeba. Současně se počítá s tím, že prováděná opatření budou úměrná stupni a druhu ohrožení.

### ➤ Odvětvový přístup

Vychází se z předpokladu, že různé odvětví mají různé zkušenosti, odborné znalosti a požadavky na ochranu kritické infrastruktury. Proto bude EPCIP rozvíjen podle odvětví a aplikován podle předem stanoveného seznamu odvětví ochrany kritické infrastruktury. [6]

### 2.6.3 Společný rámec EPCIP

EPCIP byl zaveden z důvodu, že selhání kritické infrastruktury může negativně působit na ostatní státy a na evropskou ekonomiku. Takováto selhání mohou být čím dál častější v závislosti na rozvoji nových technologií, či liberalizace trhu. Aby ochrana byla maximálně efektivní, vzniká potřeba komunikace, koordinace a spolupráce na národním a evropském stupni mezi všemi dotčenými zeměmi.

Počítá se s tím, že bude na úrovni Evropské unie zaveden společný rámec na ochranu kritické infrastruktury, kde bude zajištěno, že každá členská země bude poskytovat přiměřenou nebo stejnou úroveň související s vlastní kritickou infrastrukturou.

Pro posílení kritické infrastruktury EU bude dosaženo zavedením společného rámce EPCIP (společné cíle, metody...), díky němuž lze dosáhnout výměny nejlepších postupů a kontrolních mechanismů. [4]

#### Společné principy EPCIP

- Společně dohodnuté kódy/standardy
- Obecné definice, na základě kterých mohou být tvořeny odvětvově specifické definice
- Společný seznam odvětví s kritickou infrastrukturou
- Prioritní oblasti CIP
- Popis odpovědnosti zúčastněných subjektů
- Dohodnuté referenční ukazatele
- Metody pro srovnávání a stanovení prioritních infrastruktur u jednotlivých odvětví

Rámec EPCIP může být v závislosti na jednotlivých tématech buď dobrovolný, nebo povinný (případně mix obojího). Zde záleží na jednotlivých problémech bezpečnosti, ovšem ve všech případech platí, že by se měla doplňovat opatření na úrovni EU a úrovni členských států. [4]

## **2.7 Úrovně kritické infrastruktury**

Úrovně kritické infrastruktury se objevují v Zelené knize. Evropská unie určuje, kdy bude ochrana infrastruktury v kompetenci unie a kdy v kompetenci členských států.

### **2.7.1 Kritická infrastruktura na úrovni evropské unie (ECI)**

Evropská kritická infrastruktura se bude týkat pouze těch událostí, které způsobí vážné důsledky i mimo členskou zemi, kde se nachází daná infrastruktura. Je třeba dbát na to, aby ECI obsahovala ty „materiální zdroje, služby, zařízení informačních technologií, sítě a majetek, které mají v případě narušení nebo zničení vážný dopad na zdraví, bezpečnost, zabezpečení, hospodářský nebo sociální blahobyt.“ [4]

### **2.7.2 Národní kritická infrastruktura (NCI)**

S respektováním pravomocí unie mají odpovědnost za ochranu vnitrostátních kritických infrastruktur jejich vlastníci (provozovatelé) a členské země.

Aby bylo dosaženo zlepšení ochrany kritických infrastruktur na národní úrovni, je třeba, aby všechny země evropského společenství vytvořily vnitrostátní program na ochranu kritických infrastruktur. Cílem těchto programů bude definovat přístup každého členu EU k ochraně vnitrostátních kritických infrastruktur umístěných na jeho území. Takové programy budou řešit tyto aspekty:

- Definování a vytvoření vnitrostátních kritických infrastruktur státem EU podle předem stanovených vnitrostátních požadavků. Tyto požadavky by si měla každá členská země vytvořit sama s přihlédnutím k následujícím množstevním i jakostním dopadům narušení, či destrukci kritické infrastruktury:
- Zahájení dialogu s vlastníky.
- Určení vzájemných zeměpisných a odvětvových závislostí.
- Vytváření případných krizových plánů souvisejících s vnitrostátními kritickými infrastrukturami.

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

Realizováním těchto bodů, týkajících se ochrany kritických infrastruktur v jednotlivých členských státech EU lze dosáhnout toho, že subjekty, které se podílejí na kritické infrastruktuře v celé Evropě, budou mít prospěch z toho, že nespádají pod odlišné rámce KI, vedoucí k dalším nákladům a že není narušen vnitřní trh. [4]

### **2.7.3 Výstražná informační síť kritické infrastruktury (CIWIN)**

Výstražná síť CIWIN, která je součástí EPCIP, je zřízena k tomu, aby jednotlivé země měly možnost vyměňovat informace (např. osvědčené postupy) při ochraně kritických infrastruktur. Bude doplňovat již existující síť s tím, že bude velká pozornost věnována tomu, aby nedocházelo ke zdvojování.

#### **Cíle**

- Poskytnou členským státům EU, které chtějí spolupracovat pomocný nástroj IT.
- Nabídnout účinnou a rychlou alternativu k časově náročným způsobům vyhledávání informací.
- Zajistit, aby sdílené informace byly bezpečné.
- Dát členským státům možnost přímé komunikace a poskytování informací, které považují za důležité.

### **2.8 *Hrozby, které nejvíce ohrožují kritickou infrastrukturu Evropy.***

Masivní útok proti některým z členských států je v současné době nepravděpodobný. Namísto toho ovšem Evropa čelí novým hrozbám, které jsou různorodější, méně nápadné a hůře předvídatelné.



### **2.8.1 Terorismus**

Strach z tohoto fenoménu zesílil především po 11. září 2001. Terorismus ohrožuje lidské životy, zvyšuje náklady na bezpečnost, snaží se zasít strach a pochybnosti o vlastní bezpečnosti a stává se stále větší hrozbou pro celou Evropu. Teroristická hnutí po celém světě jsou stále lépe financována, využívají nejmodernější informační technologie k vzájemné komunikaci a neštítí se jakéhokoliv násilí. [7]

Teroristé již proti evropským zemím a městům nejednou zaútočili. Dokonce v několika evropských státech jako je Velká Británie, Itálie, Belgie, Německo či Španělsko byly odhaleny logistické základny buněk Al-Kájdý.

### **2.8.2 Šíření zbraní hromadného ničení**

Jde o potenciálně největší hrozbu současnosti. V poslední době se ji podařilo díky mezinárodním úmluvám a vývozním kontrolám šíření zbraní hromadného ničení zpomalit. Nyní ale může nastat období, kdy problémové země Blízkého i Dálného východu (Irán, Severní Korea, Pákistán, Indie atd.) budou kvůli řešení vzájemných sporů zvyšovat svůj jaderný arsenál. Nejhorší scénář obsahuje variantu, při níž se teroristické organizace těchto zbraní hromadného ničení zmocní. [7]

### **2.8.3 Regionální konflikty**

Problémy takového druhu, jaké se objevují v např. Kašmíru, v oblasti velkých afrických jezer nebo na Korejském poloostrově, mají na evropské zájmy přímý i nepřímý vliv stejně jako konflikty odehrávající se blíže evropskému území, například na Blízkém východě. Přetrvávající konflikty totiž ohrožují lidské životy a regionální stabilitu, jsou hrozbou pro menšiny a pro základní lidské svobody a práva. Můžou vést k extremismu a terorismu. [7]

### **2.8.4 Zhroucení státní moci**

Zhroucení státní moci může nastat důsledkem občanských konfliktů nebo špatného vládnutí (korupce, zneužití státní moci, slabých institucí, či absenci standardních mechanismů odpovědnosti). Jako příklady zemí, v nichž ke zhroucení státní moci v poslední době došlo, můžeme jmenovat Somálsko, Libérii či Afghánistán. [7]

### **2.8.5 Organizovaný zločin**

Evropa bohužel patří k oblastem, na něž se organizovaný zločin zaměřuje nejčastěji. Velkou část činnosti zločineckých gangů představuje pašování drog, žen, ilegálních přistěhovalců a zbraní.

Příjmy z obchodu s drahými kameny, střelnými zbraněmi či drogami podporují konflikty na jiných místech světa. Takovéto aktivity podřívají základy právní státu a společenský řád. V extrémních případech dochází i k tomu, že organizovaný zločin ovládne státní strukturu. [7]

## **2.9 Zhodnocení**

Evropská unie udělala k Ochráně kritické infrastruktury již řadu kroků. Vydala během let 2004, 2005 a 2006 důležité dokumenty, upravující tuto problematiku, především Zelenou knihu. Vymezila částečně pravomoci jak své, tak i jednotlivých členských států. Spustila programy EPCIP, CIWIN a také systém včasného varování ARGUS. Do této problematiky jistě spadají i její snahy v boji proti terorismu. Za slabou stránku lze považovat to, že Evropská unie zcela nemá dopracovanou legislativu k ochraně kritické infrastruktury. To způsobuje, že státy postupují při její ochraně samostatně a nesystematicky.

### **3 KI ve vybraných zemích Evropské unie**

V této kapitole bude popsáno řešení ochrany kritické infrastruktury v jednotlivých státech.

Každá kapitola se věnuje počátkům ochrany kritické infrastruktury dané země a obsahuje oblasti její kritické infrastruktury, orgány, které se na ochraně podílí, důležité dokumenty s kritickou infrastrukturou související. Popsány jsou rizika, považované za klíčové a je provedeno shrnutí ochrany infrastruktury dané země.

#### **3.1 Česká republika**

Česká republika má z geografického hlediska vynikající polohu uprostřed Evropy, na styku či v dosahu všech jejích velkých oblastí (západní, východní Evropa, Balkán, Skandinávie). Její nejdelší hranice je hranice s největší hospodářskou mocností kontinentu – Německem.

Větší část území zaujímá Česká vysočina, tvořená pahorkatinami a vrchovinami. Nížina a roviny představuje Česká tabule. Celou oblast obklopují nevysoká hraniční pohoří. Územím státu probíhá hlavní evropské rozvodí. Klima je mírné a podléhá oceánským i kontinentálním vlivům.

Prvními obyvateli dnešní České republiky byli keltští Bójové. Odtud název země Bohemia. V 6. století se na území usazují Slované a v 7. století je založen kmenový svaz zvaný Sámova říše. V roce 830 vznikl první státní útvar v českých zemích Velkomoravská říše. Z ní se na přelomu 9. a 10. století odtrhly Čechy a vznikl tak počátek českého státu. Vládnoucím rodem se stali Přemyslovci, po jejichž vymření roku 1306 nastoupili na český trůn Lucemburkové. Po nich přišli Jagelonci a roku 1526 přešla česká koruna na Ferdinanda Habsburského. Tento rod vládl až do roku 1918 (s výjimkou krátkého období Fridricha Falckého).

Porážka v bitvě na Bílé hoře roku 1620 přinesla velký hospodářský úpadek a konec samostatnosti českého státu. Následovalo období poněmčování, náboženského a sociálního útlačku. Až s nástupem kapitalismu na přelomu 18. a 19. století docházelo k obrození českého jazyka, kultury a k celkovému formování českého národa. K obnovení samostatné české státnosti došlo ovšem až roku 1918 po skončení první světové války. V té době vznikla Československá republika a prvním prezidentem se stal Tomáš Garrigue Masaryk.

Samostatnost netrvala dlouho, neboť roku 1939 obsadila stát německá vojska. Po německé okupaci získali roku 1948 moc komunisté. Až v listopadu 1989 došlo k pádu komunistického režimu. K 1.1. 1993 došlo k rozdělení republiky na Česko a Slovensko.

Obyvatelstvo je národnostně homogenní. Nejvýznamnější je slovenská menšina. Hospodářství země, které za období vlády komunistů dosti upadalo, procházelo velmi složitým obdobím přechodu k volnému trhu.

Země je ve výrobě potravin prakticky soběstačná. Polovina orné půdy, která zabírá asi 40% plochy území, je tvořena obilovinami. Mezi hlavní pěstované plodiny patří pšenice, ječmen, cukrovka a brambory. Světově významná je produkce chmele.

Nerostné zdroje jsou omezené. Nejvýznamnější je těžba černého a hnědého uhlí. Nejdůležitější odvětví průmyslu představuje hutnictví a strojírenství. Významný je také cestovní ruch v čele s hlavním městem Prahou.

Země má poměrně zastaralou komunikační a technickou infrastrukturu. Je zde velmi hustá, avšak málo efektivní, železniční síť. [8], [15]

Větší část území zaujímá

|                             |                       |
|-----------------------------|-----------------------|
| Hlavní Město:               | Praha                 |
| Počet obyvatel(mil):        | 10,22                 |
| Státní zřízení:             | Federativní republika |
| Rozloha (km <sup>2</sup> ): | 78 864                |
| Úřední jazyk:               | Čeština               |
| Rok vstupu do Eu:           | 2004                  |

### 3.1.1 Ochrana KI

Na způsob přístupu k ochraně kritické infrastruktury v ČR existuje několik názorů. Jeden názor hovoří o tom, že je třeba vyčkat na vyřešení celé problematiky v rámci ***Evropského projektu ochrany kritické infrastruktury*** (EPCIP) a pak vše převzít. Naproti tomu existuje mínění, že u nás máme dostatek odborných kapacit na to, abychom otázky KI vyřešili sami. A navíc máme určitá specifika, která v jiných zemích nejsou. [12]

Existuje i takový názor, který říká, že bychom měli převzít zahraniční zkušenosti a upravit je do našich podmínek, protože postupná globalizace ekonomiky všechny rozdíly mezi zeměmi v zásadě smaže. "

### **Problematiku kritické infrastruktury v ČR lze rozdělit na 3 části:**

- Mapování kritické infrastruktury v ČR.
- Inventura přístupu subjektů řešících problematiku kritické infrastruktury v jejich jednotlivých oblastech
- Rozbor situace v jednotlivých odvětvích ČR s vazbou na postupy mezinárodních organizací a institucí (EU, NATO aj.)

### **3.1.2 Historie KI v ČR**

Prvním projektem, který se stal základem pro komplexní řešení problematiky KI v České republice, byl materiál ***Definice a rozsah základních funkcí státu***, který byl projednán Výborem pro civilní nouzové plánování (dále jen „VCNP“) dne 24. června 2001, usnesení č. 105 a následně Bezpečnostní radou státu (dále jen „BRS“) dne 24. července 2001.

Byl to materiál, který se věnoval základním funkcím státu v případě mimořádných nebo krizových situací a jeho základem byly tragické následky povodní v Česku v letech 1997 a 1998.

Pokračováním tohoto materiálu byly další projekty, týkající se ochrany kritické infrastruktury České republiky, a to dokumenty z roku 2002 ***Rozsah základních funkcí státu a Informace o národní kritické infrastruktuře a návrh zásad na její zabezpečení***. [9]

V další etapě byly tyto dokumenty upraveny a doplněny údaji o oblastech KI v ČR. Tím vznikl nový dokument z roku 2003 pod názvem ***Projekt analýzy zabezpečení základních funkcí státu a prvků kritické infrastruktury v ČR za krizových situací***. Jedná se o otevřený dokument, který je stále aktualizován.

Tento dokument je rozdělen do tří fází:

- Informace o jednotlivých oblastech (včetně právních předpisů pro krizové situace).

- Přehled subjektů kritické infrastruktury.
- Zjištění vzájemných vazeb a souvislostí.

Od poloviny roku 2004, kdy Evropská unie vytvořila **Evropský program na ochranu kritické infrastruktury** (EPCIP) a **Varovnou informační síť kritické infrastruktury** (CIWIN), se pozornost zaměřuje na aktivity související s ochranou kritické infrastruktury v rámci EU. [9]

V červnu 2007 projednal Výbor pro Civilní a nouzové plánování materiál **Zpráva o řešení problematiky kritické infrastruktury v České republice**. Následně byl tento materiál projednán rovněž Bezpečnostní radou státu, která vyzvala ministra vnitra k předložení materiálu, jenž bude obsahovat **Harmonogram dalšího postupu zpracování dokumentu Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národní program kritické infrastruktury**. Tento dokument vláda schválila dne 25.února 2008 [11]

**Zpráva o řešení problematiky kritické infrastruktury** obsahovala podrobnou analytickou část, která se zabývala situací v jednotlivých oblastech kritické infrastruktury České republiky a řešila i obecné řešení této problematiky.

#### **Závěry z uvedené analýzy byly tyto**

- Požadavek legislativně upravit pojem kritická infrastruktura, její ochranu, objekty a subjekty kritické infrastruktury a stanovit kompetence a povinnosti státní správy a vlastníků/provozovatelů kritické infrastruktury, včetně zásad financování/.
- Zapojit do řešení problematiky ochrany kritické infrastruktury krajské, popř. obecní orgány.
- Zpracovat analýzy dopadů narušení objektů kritické infrastruktury, stanovit vzájemné vazby mezi oblastmi nebo objekty kritické infrastruktury.
- Stanovit prioritní oblasti nebo objekty, jejichž narušení ovlivní jiné oblasti kritické infrastruktury a zásady zabezpečení jejich ochrany.

- Upřesnit ostatní oblasti nebo objekty kritické infrastruktury a zásady zabezpečení jejich ochrany (nahraditelnost organizačními nebo nouzovými opatřeními).
- Využít finančních prostředků EU pro oblast kritické infrastruktury zpracováním vhodných projektů.
- Určit a stanovit oblasti, subjekty a zařízení kritické infrastruktury, které by odpovídaly zařazení pod pojem ECI (Evropská kritická infrastruktura) v souladu se Směrnicemi Rady o ECI, včetně požadavků na určené subjekty, vyplývající z tohoto dokumentu.

Zatím poslední aktualizace Harmonogramu dalšího postupu zpracování dokumentů Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národního programu ochrany kritické infrastruktury obsahuje program do roku 2012.

### 3.1.3 Jednotlivé oblasti kritické infrastruktury České republiky

- **Energetika** (elektrina, plyn, tepelná energie, ropa a ropné produkty).
- **Vodní hospodářství** (zásobování pitnou a užitkovou vodou, zabezpečení a správa objemu povrchových vod s podzemních zdrojů vody, systém odpadních vod).
- **Potravinářství a zemědělství** (produkce potravin, péče o potraviny, zemědělská výroba).
- **Zdravotní péče** (přednemocniční neodkladná péče, nemocniční péče, ochrana veřejného zdraví, distribuce léčiv).
- **Doprava** (silniční, železniční, letecká, vnitrozemská vodní).
- **Komunikační a informační systémy** (služby pevných a mobilních komunikačních sítí, rádiová a satelitní komunikace, televizní a rádiové vysílání, přístup k internetu a datovým službám, poštovní a kurýrní služby).
- **Bankovní a finanční sektor** (správa veřejných financí, bankovníctví, pojišťovnictví, kapitálový trh).

- **Nouzové služby** (Hasičský záchranný sbor ČR, Policie, Armáda ČR, Radiační monitorování vč. Doporučení ochranných opatření, předpovědní, varovná a hlásná služba).
- **Výroba nebezpečných látek, skladování, přeprava** (výroba a skladování nebezpečných látek, doprava a přeprava nebezpečného zboží, biologické materiály, radioaktivní materiály). [20]

### **3.1.4 Zákony, předpisy a nařízení, týkající se ochrana KI v ČR**

- 238/2008 Sb., o Hasičském záchranném sboru
- 240/2000 Sb., o Krizovém řízení
- 241/2000sb., o Hospodářských opatřeních pro krizové stavy
- 110/1998 Sb.
- 239/2008 Sb.
- 222/1999 Sb.

### **3.1.5 Největší rizika, která mohou vést k narušení infrastruktury v České republice**

a) vnitřní problémy na objektech a v systémech kritické infrastruktury, přičemž příčiny narušení funkcí nemusí být přímo ovlivněny příslušným subjektem či subjekty.

- Technologické havárie.
- Technické poruchy, nedostatek náhradních dílů.
- Výpadky dodávek energií (elektřina, plyn, teplo, PHM).
- Výpadky dodávek vody.
- Výpadky dodávek surovin (součástí) pro výrobu nebo poskytování služeb.
- Kolaps počítačových sítí.

■



**b) vnitřní problémy** na objektech a v systémech kritické infrastruktury, přičemž příčiny narušení funkcí **jsou přímo či nepřímo ovlivněny** příslušným subjektem nebo subjekty,

- Dočasná změna orientace (priorit) poskytování výrobků a služeb z důvodu řešení mimořádných událostí (krizových situací nevojenských i vojenských).
- Dlouhodobá nebo trvalá změna orientace (priorit) poskytování výrobků a služeb z důvodu rozhodnutí managementu subjektu kritické infrastruktury (může být ovlivněno i prorůstáním organizovaného zločinu do firem).
- „Krach“ firmy z ekonomických nebo jiných důvodů.
- Stávka.

**c) vnější důvody,**

- Narušení objektu kritické infrastruktury z důvodu živelní pohromy nebo průmyslové havárie v „sousedním objektu“.
- Narušení objektu kritické infrastruktury způsobené člověkem (teroristický útok, kriminální čin, důsledky války).
- Nedostatek (úbytek) pracovních sil, včetně zvýšené nemocnosti (pandemie, infekční onemocnění), odmítnutí pracovat např. při řešení vlastních problémů souvisejících se vznikem mimořádných událostí.

**Silné stránky ekonomiky ČR z hlediska ochrany kritické infrastruktury:**

- Stabilizace finančního sektoru (bankovníctví, pojišťovnictví).
- Tradice v některých odvětvích průmyslu, zejména zpracovatelského.
- Vysoký podíl uspokojení energetických potřeb z vlastních zdrojů.
- Soběstačnost a spolehlivost v oblasti výroby elektrické energie.
- Vysoká hustota železniční a silniční sítě.
- Výrazně dynamický rozvoj komunikačních sítí.

## Slabé stránky

- Nedostatečná (nevybudovaná, zastaralá nebo špatně udržovaná) vodohospodářská a energetická infrastruktura (inženýrské sítě, čistírny odpadních vod) ve většině regionů.
- Chybějící úseky dálnic a rychlostních silnic, absence silničních obchvatů obcí.
- Nedostatečná údržba a nevyhovující stav dopravních cest.
- Nedostatečné využití možností elektrické trakce v dopravě.
- Nedostatečné využití kombinované dopravy.
- Významné ekonomické rozdíly mezi regiony. [11]

### 3.1.6 Financování kritické infrastruktury

Co největší zabezpečení ochrany kritické infrastruktury je velmi důležité pro bezpečnost lidí a normální chod státu. Je ovšem třeba si uvědomit, že nic není zadarmo. Zejména se to týká „zvyšování odolnosti objektů proti působení rizik a zálohování prioritních částí koické infrastruktury, včetně využití různých principů zálohování a rozmístění záloh v území“

Financování ochrany KI v České republice lze provést podobně jako financování krizových opatření obsažených v krizovém zákoně. Důležitá je i možnost využití zdrojů EU. Od roku 2007 do roku 2013 má být ochrana naší KI financována prostřednictvím rámcového programu s názvem **Bezpečnost a ochrana Svobod**. Evropská komise počítá s tím, že na ochranu kritické infrastruktury vyčlení 137,4 milionů EUR.

Dále se počítá s využitím evropských prostředků na podporu prevence (připravenosti reakce na teroristické útoky), přičemž větší část bude věnována na přípravu Evropského programu ochrany kritické infrastruktury. [12]

### 3.1.7 Krizové řízení

Protože v České republice neexistuje zákon, který by upravoval ochranu kritické infrastruktury, odvíjí se celková ochrana od **Krizového zákona č. 240/2000 sb.** [1]

„Systém krizového řízení představuje komplex činností státní správy a samosprávy směřující k zamezení vzniku krizových situací, případně k zvládnutí krizových situací“

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů říká, že krizové řízení je: „Souhrn řídicích činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace.“ [1]

Základní dokument krizového řízení pro řešení krizových situací se nazývá **Krizový plán kraje**. Vypracovává ho **Hasičský záchranný sbor** kraje podle zákona č.240/2000 Sb. a nařízením vlády 462/2000 Sb. Tento dokument vymezuje působnost a odpovědnost orgánů veřejné správy a jiných orgánů, hodnotí možná rizika a jejich dopady na území. Krizový plán kraje je po projednání Bezpečnostní radou schválen hejtmanem. [1]

### 3.1.8 Orgány krizového řízení

Orgány krizového řízení jsou takové „orgány (Vláda ČR, ministerstva a ostatní správní úřady, Česká národní banka, orgány krajů, obcí a určené orgány s územní působností ), které ve prospěch svého zřizovatele zabezpečují analýzu a vyhodnocení možných ohrožení jeho bezpečnosti, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravnými opatřeními a řešením krizových situací.“ [1]

[1]

#### **Bezpečnostní rada**

Koordinačním orgánem pro přípravu krizové situace v ČR je Bezpečnostní rada (státu, kraje, či určené obce). Jejím předsedou na úrovni státu je předseda vlády, na úrovni kraje hejtman a na úrovni obce je to starosta obce. [1]

#### **Krizový štáb**

Krizový štáb je svoláván na výzvu jeho zřizovatele, kterým je předseda vlády, hejtman či starosta, a to podle toho zde je vyhlášen krizový stav pro celé území státu nebo pro jeho část, dle působnosti orgánů krizového řízení. Tento štáb je svoláván operativně, zejména k projednání klíčových otázek souvisejících s řešením krizové situace a přijetím krizových opatření spojených. [1]

### 3.1.9 Ochrana obyvatelstva v ČR

V České republice je působnost a pravomoc státních orgánů a orgánů územních a samosprávních celků a práva a povinnosti právnických a fyzických osob v této oblasti upravena hlavně zákonem o Integrovaném záchranném sboru (IZS). Dále pak dalšími právními předpisy pro oblast krizové legislativy. [9]

Hlavní orgán, který se zabývá ochranou kritické infrastruktury v ČR je Výbor pro civilní nouzové plánování (VCNP) Bezpečnostní rady státu. Tento orgán spadá pod MV GŘ HZS.

Hlavním dokumentem pro rozvíjení ochrany obyvatelstva v České republice je ***Koncepce ochrany obyvatelstva do roku 2006 s výhledem do roku 2015*** z roku 2002. (2005 novelizovaná)

Ochrana obyvatelstva je v tomto dokumentu charakterizovaná jako „soubor činností a postupů, včetně příslušných orgánů, dalších subjektů i jednotlivých občanů, směřujících k minimalizaci dopadů mimořádných událostí na životy a zdraví obyvatelstva, majetek a životní prostředí“. [2]

#### **Orgány v ochraně obyvatelstva**

Roli hlavního orgánu státní správy v ČR zastává Ministerstvo vnitra, prostřednictvím MV-GŘ HZS ČR. Realizace ochrany obyvatelstva se účastní ministerstva a ostatní ÚSÚ, jímž odpovědnost za ochranu života, zdraví a majetku určují příslušné zákony.

Velmi důležitou roli na krajské úrovni mají Hasičské záchranné sbory (HZS) krajů, které plní úkoly krajů a obecních úřadů s rozšířenou působností v organizaci přípravy na mimořádné události, provádění záchranných a likvidačních prací a ochrany obyvatelstva. Čím dál více se daří předávat odpovědnost za ochranu obyvatelstva na úroveň obcí.

### 3.1.10 Zhodnocení

V oblasti ochrany kritické infrastruktury učinila Česká republika řadu významných kroků. Jedná se o deklarování základních funkcí státu za krizových situací a možnosti zabezpečení nebo vytvoření přehledů subjektů kritické infrastruktury na úrovni národní, regionální či lokální.

V posledních letech se vyvíjely a dále vyvíjejí kroky ve výzkumu postupů k zachování funkčnosti jednotlivých oblastí kritické infrastruktury.

Část odborné veřejnosti se však domnívá, že je třeba vytvořit ucelenou národní koncepci ochrany kritické infrastruktury v České republice.[12]

### 3.2 Německo

Německo je po Rusku nejlidnatější země Evropy. Má nejsilnější ekonomiku na kontinentu a jeho hospodářský a politický vliv významně formuje integraci celé Evropy

Jeho geografická poloha je velmi výhodná a sousedí s devíti státy. Na severu je omýváno Severním a Baltským mořem. Pobřežní pásmo má 2390 km. Jeho územím prochází nejdůležitější komunikační osy, spojující různé části Evropy. Klima je mírné, na severu výrazně oceánské.

Původními obyvateli Německa byli v 1.tisíciletí př.n.l. Keltové, na severu pak Germáni. Kolem roku 0 se země stala součástí antického Říma. Za Karla Velikého bylo území ovládáno Franckou říší. Tato říše byla později rozdělena a na území Německa vznikla východofrancká říše. Počátkem 10.stol. se i tato říše rozpadla na několik vévodství. Roku 962 je korunován císařem Oto I. a stává se zakladatelem Svaté říše římské, která sjednocovala území Německa, Itálie a Burgundska. Tato říše zaniká až roku 1806. Ještě v tomto roce založilo několik německých států tzv. „Rýnský spolek“. Mezitím na území Německa rostla moc Pruska a roku 1871 po sjednocení Německa pruským kancléřem Otto von Bismarckem, bylo vyhlášeno Německé císařství. Německo se krátce na to stalo evropskou průmyslovou velmocí, postavilo obrovské loďstvo a získalo první zámořské kolonie.

Německo do značné míry ovlivnila 1.světová válka v letech (1914-1918). Válka skončila jeho porážkou, obsazením průmyslového Sárska a Porýní Francií, územními ztrátami na východě země a koncem císařství. Země byla vystavena velkým hospodářským problémům, povinností platit válečné reparace a okupaci Porúří. V roce 1934 se stal vůdcem Třetí říše Adolf Hitler, který v roce 1939 začal II.světovou válku a v roce 1945 ji prohrál. Důsledkem bylo rozdělení země do čtyřech okupačních zón. Roku 1949 byly 3 zóny(francouzská, britská a americká sloučeny a vznikla Spolková republika Německo. Ze čtvrté okupační zóny, kterou spravoval Sovětský svaz, se stala Německá demokratická republika. V roce 1952 byl utvořen podél celé hranice neprostupný kordón. SRN a NDR se spojily až v roce 1990 po prvních svobodných volbách a pádu socialismu v Evropě.

Německo je federativní republikou a má 15 členských zemí. Funkci zákonodárného orgánu zde plní dvoukomorový parlament, který se skládá ze Spolkového sněmu (662 poslanců volených na 4 roky) a Spolkové rady, jejíž 68 členů jsou zástupci z jednotlivých členských zemí. Spolkový sněm volí předsedu vlády (kancléře). Prezident je volen voličským sborem (zástupci Spolkového i zemských sněmů)

Obyvatelstvo tvoří převážně Němci. Nejvíce přistěhovalců tvoří Turci, obyvatelé bývalé Jugoslávie, Řekové a další.

Zemědělství je velmi intenzivní, vysoce mechanizované, ale zaměstnává jen 3% ekonomicky aktivních obyvatel. Hodně potravin je proto třeba dovážet, především z Francie.

Nerostné zdroje jsou poměrně omezené. Jedná se především o těžbu hnědého uhlí a produkci draselných solí. Více než 2/3 elektřiny se vyrábí spalováním fosilních paliv a podíl jaderných elektráren se blíží 30%.

Německý průmysl patří k nejvyspělejším v Evropě. Nejdůležitější je výroba automobilů a dalších dopravních prostředků.

Země má nejdelší dálniční síť v Evropě. Buduje se systém železničních tratí pro vysoké rychlosti. Velmi významná je i vodní doprava [8], [15]

### **Základní informace**

|                                |         |
|--------------------------------|---------|
| Hlavní Město:                  | Berlín  |
| Počet obyvatel(mil):           | 82,18   |
| Rozloha (km <sup>2</sup> ):    | 356 733 |
| Váha hlasu v ministerské radě: | 8,4     |
| Počet poslanců v parlamentu:   | 99      |

### **3.2.1 Vývoj Ochrany kritické infrastruktury v Německu**

Z vojenského pohledu spadá historie ochrany kritické infrastruktury už do období studené války. Hlavní událostí k řešení OKI, ale bylo 11.září 2001, a v Německu hlavně pak záplavy na Labi v roce 2002, kdy tento problém dosáhl vysoké důležitosti.

Jelikož je v Německu přes 90 % infrastruktury ve vlastnictví soukromých subjektů, tak velice důležitou roli hraje Spolkové ministerstvo hospodářství a práce (Bundesamt für Wirtschaft und Arbeit). [18]

Poměrně nová je zde instituce s názvem **Ochrana kritické infrastruktury v Německu** (Schulz Kritischer Infrastrukturen in Deutschland), která se pokusila zmapovat zranitelnost německé infrastruktury a sestavit strategii ochrany a politiku spolupráce a koordinace veřejné správy se soukromými subjekty. Zároveň zde existuje pracovní skupina na ochranu kritické infrastruktury **Arbeit Kreis Schulz von Infrastrukturen**, jejíž cílem je analýza závislostí infrastruktur a návrh strategií na minimalizování zranitelnosti.

Jako skutečný počátek budování OKI v Německu byl až rok 1997, kdy jako reakce na tzv. „Bílou knihu“ (směrnice č.64 – USA) vznikl Spolkový úřad pro informační bezpečnost (Bundesamt für Sicherheit in der Informationstechnik).

Tento úřad sestavil speciální pracovní skupinu „**AG KRITIS**“. Ta v letech 1997-2000 provedla analýzu, která obsahovala:

- Popsání možných scénářů hrozeb.
- Prověření infrastruktury prostřednictvím z hlediska možnosti její napadání přes slabá místa v infrastruktuře informačních technologií.
- Určení možností pro minimalizaci těchto slabých stránek, jakož i pro zabránění nebo zmírnění škod.
- Zpracování návrhu na vytvoření systému včasného varování a analýzu požadovaného systému.

V roce 1998 vytvořil BSI novou sekci s názvem „Ochrana kritické infrastruktury“. V reakci na září 2001 pak Německá vláda vydala **Antiteroristický balíček I** později doplněný **Antiteroristickým balíčkem II**. Ty pak uzákonila v roce 2002 jako **Antiteroristický zákon**.

Dalším důležitým krokem je vytvoření pracovní skupiny **PG KRITIS** (Project group). Tato skupina byla vytvořena v na jaře roku 2002 a funguje pod dohledem **Spolkového ministerstva vnitra**. Jejím hlavním cílem je zajištění součinnosti projektů a jejich zavádění do systému OKI v Německu. Více o této skupině v kapitole o orgánech na OKI v Německu.

.V květnu roku 2004 byl založen **Spolkový úřad civilní ochrany a pomoci při pohromách** (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe). Ten dostal na starost Fyzické aspekty bezpečnosti.



V červenci 2005 byl pak vypracován Spolkovým ministerstvem vnitra **Plán na ochranu na ochranu kritické infrastruktury** ( Nationaler Plan zum Schutz der Informationsinfrastrukturen)

### 3.2.2 Řešení ochrany kritické infrastruktury

V Německu je národní koncept ochrany kritické infrastruktury, postaven na čtyřech základních pilířích:

- Programu základní ochrany subjektů KI.
- Programech základní ochrany v odvětví KI.
- Programech speciální ochrany v odvětví KI.
- Programech ochrany pro speciální ohrožení.

Výstupem jednotlivých programů jsou doporučení pro zainteresované subjekty. V rámci vlastních program ochrany se doporučují mimo jiné tyto kroky:

- Analýza ohrožení.
- Stanovení cílů a potřeby ochrany (definice cíle, priority, zjištění potřeb ochrany).
- Objektové analýzy (poloha, okolí, stavební opatření...).
- Identifikace a ohodnocení kritických oblastí.

[12]

### 3.2.3 Jednotlivé oblasti kritické infrastruktury Německa

- **Doprava a provoz** (letectví, námořní plavba, železnice, místní doprava, vnitrozemská vodní doprava, silnice, poštovní služby).
- **Energetika** (Elektrické síť, jaderné elektrárny, plyn, ropa).
- **Nebezpečné materiály** (Chemické látky a biomateriály, Přeprava nebezpečných materiálů, Obranný průmysl).

- **Informační a komunikační technologie** (telekomunikace, informační technologie).
- **Finance, fondy a pojišťovnictví** (Banky, pojišťovny, poskytovatelé finančních služeb, burzy).
- **Zajištění služeb** (Zdravotní péče, pohotovostní a záchranné služby, dohled nad katastrofami, dodávky vody, dodávky potravin, likvidace odpadů).
- **Úřady, administrativa a justice** (správní orgány a justice, vláda, vládní agentury, administrativy, bezpečnostní orgány a organizace, spolková armáda).
- **Jiné** (celoplošná média, velké výzkumné ústavy, důležité památky).

[26]

### 3.2.4 Nebezpečí, která mohou vést k narušení infrastruktury v Německu

Dle dokumentu „*Národní strategie pro ochranu kritické infrastruktury z června roku 2009 v Německu*“ jsou považovány za závažné tyto hrozby. [21]

#### **Přírodní události**

- Události spojené s následky extrémního počasí.
- Lesní požáry.
- Zemětřesení.
- Epidemie a pandemie.

#### **Technická, či lidská selhání**

- Selhání technických systémů.
- Nedbalost.
- Nehody a mimořádné události.
- Nedostatečná organizace.

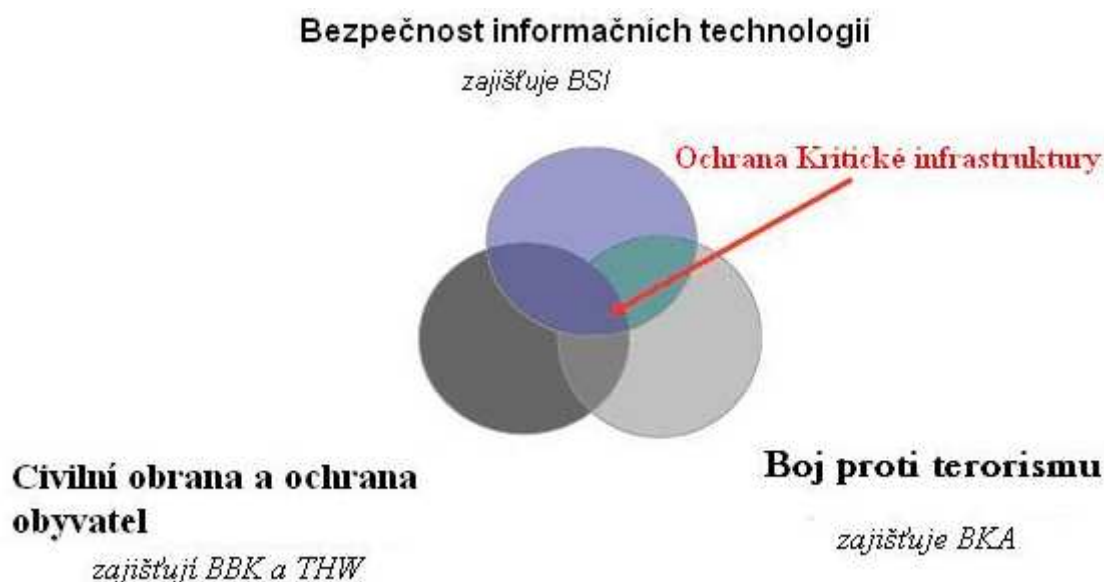
## **Terorismus, zločin, válka**

- Terorismus.
- Sabotáže.
- Jiné formy kriminality.
- Občanské a mezinárodní války.

Výčet je skutečně veliký. Pokud bychom ovšem měli vyzvednout ty hrozby, které Německo řeší nejvíce, potom to budou hrozby spojené s napadením informačních technologií a terorismem.

### **3.2.5 Orgány zabývající se ochranou kritické infrastruktury v SRN.**

Ochrana kritické infrastruktury v Německu je tvořena především třemi oblastmi a v nich působícími čtyřmi orgány. Jsou to *Spolkové ministerstvo vnitra* (BMI), *Spolkový úřad pro informační bezpečnost* (BSI), *Spolkový úřad pro civilní ochranu a pomoc při katastrofách* (BBK) a také *Spolková agentura technické pomoci* (THW). Každý z těchto orgánů má svoje povinnosti při ochraně kritické infrastruktury a jejich průnik (jak ukazuje obrázek 2) tvoří systém ochrany kritické infrastruktury. [21]



**Obrázek 2 - Představa OKI v Německu[22]**

## **Spolkové ministerstvo vnitra (BMI)**

Tento orgán je odpovědný za vnitřní bezpečnost Německa a do značné míry se podílí na jeho ochraně kritické infrastruktury.

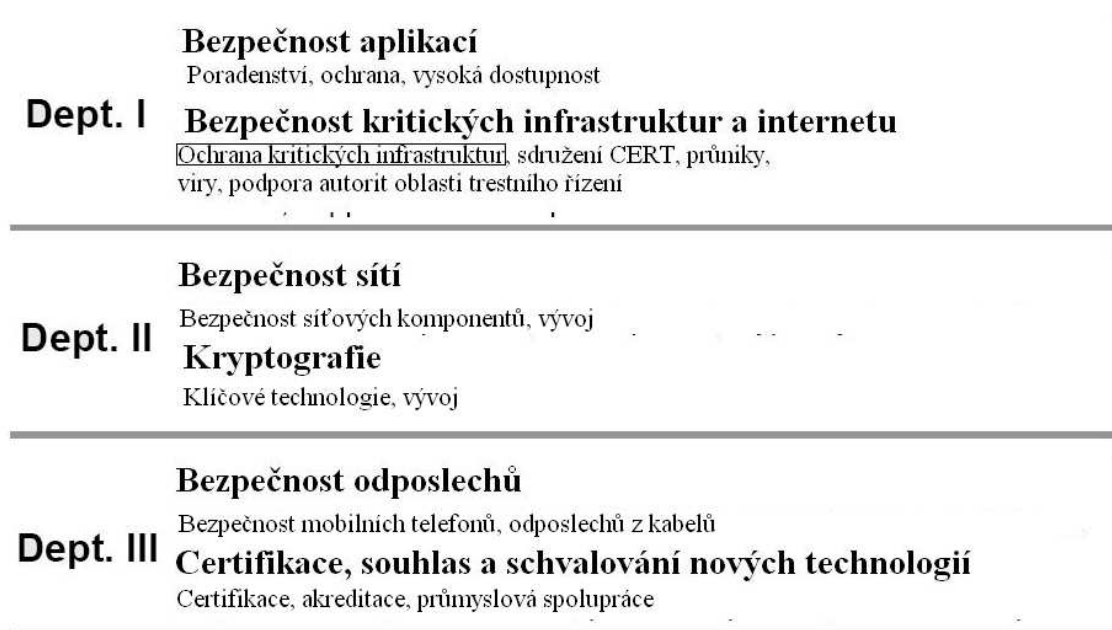
BMI zřídilo speciální pracovní skupinu na ochranu kritické infrastruktury (AK Kritis). Na ochraně kritické infrastruktury Německa v rámci ministerstva vnitra se podílejí zástupci z příslušných oddělení krizového řízení a civilní ochrany. [26]

## **Spolkový úřad pro informační bezpečnost (BSI)**

BSI se má širokou oblast působnosti, zahrnující veškeré úkoly, související s bezpečností internetu. Je aktivní v oblasti IT analýzy, IT zranitelnosti a rozvoji IT bezpečnostních opatření. Úzce spolupracuje s ostatními orgány kritické infrastruktury. Strukturu toho úřadu můžete vidět na obrázku 3.

Úřad se skládá ze tří departmentů (oddělení), nad kterými dohlíží jedna centrální divize. První department se zabývá bezpečností aplikací a bezpečností kritických infrastruktur a internetu. Ta je pro nás nejzajímavější, protože má především na starosti ochranu kritické infrastruktury. Jak je vidět, Německo bere ochranu kritické infrastruktury z pohledu možného zneužití informační technologií.

Další oddělení se zabývá bezpečností sítí a kryptografií a poslední bezpečností odposlechů a certifikací. [26]



**Obrázek 3 - Organizační uspořádání BSI [22]**

### **Spolkový úřad pro civilní ochranu a pomoc při katastrofách (BBK)**

Tento úřad byl založen v květnu 2004. BBK je pověřen informováním vlády a společnosti o KI, zvyšuje povědomí úřadů, podniků a široké veřejnosti, a objasňuje úkoly, způsoby fungování a vztahy (vzájemných) kritické infrastruktury. BBK se také podílí na vytvoření a posílení spolupráce mezi orgány veřejné správy a společnosti na témata, týkající se této problematiky. [26]

### **Federální agentura pro technické pomoci (THW)**

Federální agentura pro technickou pomoc (THW) je orgán civilní ochrany Spolkové republiky Německo. Jedná se o celostátní organizaci, schopnou reagovat na mimořádné události na místní, regionální, národní a globální úrovni. [26]

### **Spolkový vyšetřovací úřad (BKA)**

Tento úřad stíhá zločiny, které se snaží poškodit nebo zničit kritickou infrastrukturu, a které proto mohou představovat vážné ohrožení života, zdraví či obecné blaho společnosti. BKA je také odpovědný orgán pro vyšetřování trestných činů spáchaných prostřednictvím informačních a komunikačních technologií. Jeho důležitým úkolem je boj proti terorismu. [26]

### **3.2.6 Národní plán na ochranu kritické infrastruktury v Německu**

Plán byl vypracován v červenci 2005 Spolkovým ministerstvem vnitra ve spolupráci se Spolkovým úřadem pro bezpečnost. Jednalo se o strategii ochrany a zajištění bezpečnosti informačních technologií.

Odborníci ze soukromého i veřejného sektoru kritické infrastruktury byly přizváni Spolkovým ministerstvem vnitra, aby sestavili plán implementace OKI v Německu. Tento plán doporučuje celou řadu opatření, jejichž cílem je dále zvýšit ochranu informačních infrastruktur v odvětvích ochrany kritických infrastruktur. Součástí tohoto plánu je dokument, který upravuje ochranu kritických infrastruktur v Německu – Umsetzungsplan Kritis (UP Kritis)

. Na sestavování tohoto plánu se podíleli 4 pracovní skupiny (WG – working groups) z nichž každá se zabývala jinou oblastí:

- WG 1 "Nouzové a krizové cvičení".

- WG 2 "Krizové řízení a reakce.
- WG 3 "Údržba služeb kritické infrastruktury".
- WG 4 "Národní a mezinárodní spolupráce".

Už při přečtení výše uvedených bodů je nám jasné, že je kladen důraz na komunikaci mezi uvedenými sektory ochrany kritické infrastruktury. Proto jsou informační technologie považovány za klíčový faktor OKI v Německu.

### **3.2.7 Zhodnocení**

Německo jako nejvýznamnější evropská velmoc začalo s ochranou své infrastruktury téměř ve stejné době jako USA. Hlavními impulzy byly útoky na New York, ale i záplavy na Labi. Ze studia dokumentů, především Národního plánu na ochranu kritické infrastruktury, je zřejmé, že Německo se nejvíce obává situace narušení KI, v důsledku útoků na její informační infrastrukturu.

### 3.3 Švýcarsko

Tento stát střední Evropy leží na západ od Alp. Kolem 70% území tvoří krajina horského charakteru. Již v prvním století př. n. l. zde sídlili Římané, v 5. století n.l. toto území ovládali germánští Alamani. V 11. stol. se stalo součástí Svaté říše římské a začalo být pod vládou Habsburků. Proti nim se ovšem spojilo během 13. a 14. století několik místních kantonů (známo jako „spříseženstvo švýcarské“). Když v 15. století ztratili Habsburkové poslední části území, začalo být Švýcarsko uznáváno jako suverénní stát na celém území Evropy. Nástup evropské reformace vedl k náboženským bojům mezi kantony. Přestože náboženské války mezi jednotlivými státy zuřily v celé Evropě, Švýcarsko zůstalo neutrální. Neutralitu si udrželo až do 18. stol, když v roce 1794 většinu území okupovala Francie. V roce 1813, v době, ve které Francie začala ztrácet moc v Evropě, obnovilo Švýcarsko svou neutralitu a přijalo do svého spolku poslední kantony. V roce 1848 vznikla ústava po vzoru USA. Hlavním městem se stal Bern a na švýcarském neutrálním území se usídlilo mnoho mezinárodních organizací jako je Červený kříž, Liga národů nebo Ženevská konvence.

Švýcarsko si neutralitu uchovalo i během dvou světových válek. V dnešní době je sídlem mnoha mezinárodních organizací, v první řadě OSN. Sami Švýcaři ovšem vnímají členství v této organizaci jako ohrožení své neutrality a proto do této organizace nevstoupili. Jedná se o federativní republiku, kterou tvoří 20 kantonů a 6 polokantonů.. Každý kanton má vlastní ústavu, parlament i vládu. Nejvyšší zákonodárnou moc má Spolkové shromáždění o dvou komorách. Národní rada a Rada kantonů.

Švýcarsko je považováno, podle mnoha ukazatelů, za nejbohatší zemi světa. Dobrá strategická poloha ve středu Evropy, politická stabilita a důvěryhodnost učinila ze země světové finanční centrum.

Země trpí nedostatkem orné půdy a téměř polovinu potravin musí dovážet. Víc jak polovina vyrobené elektřiny připadá na vodní elektrárny a téměř 40% na jaderné (V roce 1990 byl však zakázán zákaz jejich výstavby). Švýcarsko nedisponuje nerostnými zdroji, ale jeho průmysl patří k nejvyspělejším na světě.

Tento stát má i přes horský terén výbornou komunikační síť. Síť železnic je hustá a plně elektrifikovaná. Je zde přes 70 000 km silnic. Území protíná několik důležitých transevropských spojů překonávající Alpy tunely. [8], [15]

### **Základní údaje:**

|                             |                                   |
|-----------------------------|-----------------------------------|
| Hlavní Město:               | Bern                              |
| Počet obyvatel(mil.):       | 8                                 |
| Státní zřízení:             | Federativní republika             |
| Rozloha (km <sup>2</sup> ): | 41 293                            |
| Úřední jazyk:               | němčina, francouzština, italština |

### **3.3.1 Základní informace o kritické infrastruktuře**

Problematika OKI ve Švýcarsku je řešena v rámci spolupráce úřadů mnoha různých oddělení, kantonální a místní samosprávy. Švýcarsko využívá toho, že má dlouhodobou tradici spolupráce veřejného a soukromého sektoru.

Přestože Švýcarsko dlouhá léta usilovalo o vlastní koncept ochrany kritické infrastruktury, je tato problematika řešena poměrně krátce. Konkrétní význam vlastně dostala až v roce 2002.

Po první analýze ochrany a bezpečnosti kritické infrastruktury ve Švýcarsku , která byla provedena na žádost *Kontrolní delegace Spolkového shromáždění* se *Spolková Rada* rozhodla v roce 2005 spustit projekt na ochranu kritické infrastruktury. Tímto úkolem byl pověřen *Spolkový úřad pro civilní ochranu (FOCP)*.

Ten vytvořil pracovní skupinu, která bude vést patronát na všech příslušných federálních orgánech. Její název zní „*Pracovní skupina na ochranu kritické infrastruktury*“ (WG CIP) a hlavním úkolem pracovní skupiny je vylepšit spolupráci mezi všemi orgány zapojenými do programu a v neposlední řadě spolu se soukromým sektorem stanovit národní strategii ochrany kritické infrastruktury. [27]



V roce 2007 FOCP předložila *Zprávu o Ochraně kritické infrastruktury ve Švýcarsku* Spolkové radě. Zpráva byla sestavena v úzké spolupráci se všemi příslušnými spolkovými orgány. Tento moment znamenal první velký krok směrem k vytvoření národní strategie. Zpráva<sup>1</sup> definuje klíčové pojmy ochrany a vypisuje nejvíce důležité sektory a sub-sektory CI ve Švýcarsku. Dále uvádí scénáře hrozeb od oblastí přírodních a technických rizik až po ozbrojené konflikty. Dodatky na konci této zprávy zmiňují předchozí CIP aktivity a porovnávají některé jiné mezinárodní politiky. V tomto roce má FOCP předložit národní CIP strategii s výhledem do roku 2011 . [27]

### 3.3.2 Jednotlivé oblasti kritické infrastruktury Švýcarska

- **Veřejná správa** (Parlament, vláda, justice, administrativa, výzkumné instituce, národní kulturní majetek).
- **Chemický průmysl** (výroba, doprava, skladování a zpracování chemických látek).
- **Energetika** (dodávky energie, dodávky nafty, dodávky zemního plynu).
- **Likvidace odpadů** (Plýtvání vodou, Průmyslový a domovní odpad, speciální odpad).
- **Finanční služby** (Banky, pojišťovny).
- **Veřejné zdraví**(zdravotní péče, léky, laboratoře).
- **Informační a komunikační technologie** (Telekomunikace, Informační systémy a sítě, Internet , Přístrojová technika, automatizace a kontrolní systémy, Rádio a média).
- **Voda a potraviny** (dodávky potravin, nezávadnost potravin, dodávky pitné vody).
- **Veřejná bezpečnost, záchranné a havarijní služby** (Nouzové organizacemi - policie, protipožární a záchranné služby, armáda).

---

<sup>1</sup> Zpráva je dostupná na adrese [www.infraprotection.ch](http://www.infraprotection.ch)

- **Doprava** (Silniční doprava, Železniční doprava, Letecká doprava ,Navigace,Poštovní služby a logistické ).

[27]

### **3.3.3 Orgány zabývající se ochranou kritické infrastruktury ve Švýcarsku**

#### **Spolkový úřad pro civilní ochranu (FOCP)**

Protože kritická infrastruktura pokrývá široké spektrum zájmů od energetických dodávek přes finanční služby až po kulturní majetek, účastní se její ochrany velké množství subjektů, jejichž činnost je třeba koordinovat. Tímto úkolem byl pověřen Spolkový úřad pro civilní ochranu. Spolkový úřad pro civilní ochranu (dále jen FOCP) je součástí Spolkového Ministerstva obrany, civilní ochrany a tělovýchovy (DDPS). Zajišťuje také spolupráci mezi kantony a obcemi, které nesou hlavní odpovědnost za civilní ochranu. [26]

#### **Pracovní skupina ochrany kritické infrastruktury (WG CIP)**

Skupina federálních úřadů, podílejících se na CIP ve Švýcarsku. V současné době obsahuje 23 úřadů ze všech sedmi spolkových ministerstev. WG CIP se schází zpravidla čtyřikrát do roka. Během těchto setkání se skupina zabývá konkrétními otázkami a rozhoduje o tom jaká práce by měla být provedena v budoucnu. Prvním jejím úkolem bylo vytvořit první zprávu o ochraně kritické infrastruktury a předložit jí k projednání. [26]

#### **Do této skupiny patří:**

- Sekretariát pro politické záležitosti
- Švýcarská agentura pro rozvoj a spolupráci
- Spolkový úřad pro meteorologii a klimatologii
- Švýcarský Federální úřad pro veřejné zdraví
- Spolkový úřad policie
- Federální úřad pro civilní ochranu

- Švýcarský spolkový úřad pro informační technologie, systém a telekomunikace
- Jiné

[14]

### **3.3.4 Nebezpečí, která mohou vést k narušení infrastruktury ve Švýcarsku**

Dokument „První zpráva o ochraně kritické infrastruktury“ vydaný 20.6.2007 uvádí tyto možné hrozby pro Kritickou infrastrukturu Švýcarska[14]

#### **Zemětřesení**

Spolkový úřad pro civilní ochranu vydal k tomuto problému dokument s názvem „Koncepte v případě zemětřesení ve Švýcarsku“

#### **Riziko pandemie**

Dokument „Plán chřipkové pandemie“ vydaný rok 2006 Spolkovým úřadem pro veřejné zdraví hovoří o možných dopadech na KI Švýcarska

#### **Výpadek energie**

Spolkový úřad pro národní hospodářské dodávky vytvořil scénář situace, která by nastala po výpadku energie

#### **Selhání informační infrastruktury**

### **3.3.5 Zapojení kantonů a soukromého sektoru.**

Spolupráce mezi různými federálními úřady a agenturami je sice důležitá, ale přehlédnuta by neměla být ani součinnost těchto orgánů s kantony (na jejichž území existuje kritická infrastruktura) a se soukromým sektorem (provozovateli většiny kritické infrastruktury). Spolupráce švýcarského veřejného a soukromého sektoru je již velmi dobře zavedená v mnohem odvětvích. Jedním z příkladů je Výkaznické a analytické centrum pro důvěru informací (MELANI), které sdružuje veřejné a soukromé partnery působící v oblasti informačních a komunikačních technologií. [14]

### **3.3.6 Současné projekty Švýcarska**

Švýcarsko v současné době pracuje na těchto projektech [26]

#### **Projekt „Zemětřesení“**

Cílem tohoto projektu je vyhodnotit dopad zemětřesení na čtyři sub-sektory kritické infrastruktury (elektrické sítě, dodávek oleje, navigace a železniční dopravy) a na základě zjištění dopadů navrhnout opatření.

#### **Projekt „Scénáře CIP“**

Projekt bude rozvíjet scénáře těchto tří rizik: pandemie, výpadku energie a selhání kritické informační a komunikační infrastruktury. .

#### **Projekt „Kritičnost kritérií“**

Tento projekt bude zkoumat váhu (důležitost v CIP) 31 sub-sektorů kritické infrastruktury Švýcarska

### **3.3.7 Zhodnocení**

Švýcarsko zatím není v problematice ochrany kritické infrastruktury tak daleko jako Německo. První dokument, řešící kritickou infrastrukturu jako celek, vydalo až v roce 2007. Přesto se mu díky utvoření pracovní skupiny WG CIP podařilo vtáhnout do ochrany kritické infrastruktury značné množství spolupracujících subjektů.

### 3.4 Porovnání zemí ve vybraných oblastech

Následující rozbor zabývá odlišnostmi mezi přístupy jednotlivých států k problematice ochrany kritické infrastruktury.

#### 3.4.1 Oblasti začleněné do kritické infrastruktury

Infrastruktury resp. jejich jednotlivé sektory se liší v závislosti na prioritách státu, tedy na rozhodnutí, kterým oblastem chce věnovat svoji pozornost. Jsou sektory, které jsou logicky u všech zemí stejné. Jde o ty oblasti, jejichž nefunkčnost by celý systém kritické infrastruktury ochromila, ne-li naprosto zničila. Jedná se např. o energetiku, dopravu, komunikaci atd.

**Tabulka 1 - Srovnání oblastí KI porovnávaných zemí**

| Česká rep.                                      | Německo                        | Švýcarsko                                        |
|-------------------------------------------------|--------------------------------|--------------------------------------------------|
| Energetika                                      | Energetika                     | Energetika                                       |
| Vodní hospodářství                              |                                |                                                  |
| Potravinářství a zemědělství                    |                                | Voda a potraviny                                 |
| Zdravotní péče                                  |                                | Veřejné zdraví                                   |
| Doprava                                         | Doprava a provoz               | Doprava                                          |
| Komunikační a inform. syst.                     | Komunikační a inform. syst.    | Informační a komu. tech.                         |
| Bankovní a finanční sektor                      | Finance fondy a pojišťovnictví | Finanční služby                                  |
| Nouzové služby                                  | Zajištění služeb               | Veřejná bezpečnost, záchranné a havarijní služby |
| Výroba skladování a přeprava nebezpečných látek | Nebezpečné materiály           | Likvidace odpadů/Chem.průmysl                    |
|                                                 | Úřady administrativa a justice | Veřejná správa                                   |
|                                                 | Jiné                           |                                                  |

#### **Energetika**

Jde o jednu z nejvýznamnějších oblastí kritické infrastruktury. Bez ní by se neobešla žádná vyspělá ekonomika. Nefungovala by například doprava, informační technologie, bankovní sektor zdravotnictví a i většina ostatních.

Pod tuto oblast patří jak výroba elektrické energie, tak i energie pocházející ze zemního plynu, nafty a uhlí. Zahrnujeme sem i její skladování či distribuci.

K výrobě elektrické energie ve sledovaných zemích se využívá především jaderných, tepelných a vodních elektráren. Podíl jednotlivých elektráren na výrobě elektřiny se velmi liší. Švýcarsko díky svým divokým horským řekám může vyrábět až 60% elektřiny v elektrárnách vodních[8]. Naproti tomu v České republice připadá hlavní podíl vyrobené elektrické energie na jaderné a tepelné elektrárny, zatímco vodní jsou spíše špičkové. V Německu je situace podobná jako v České republice.

## **Doprava**

Velmi důležitý sektor, mající vliv na prosperitu státu, mezinárodní obchod či sociální rozvoj. Mezi druhy dopravy patří především silniční, železniční letecká, letecká a vodní.

Ve srovnávaných zemích je nejdůležitější silniční doprava. Nejlepší dálniční síť má vybudovanou Německo. Ve Švýcarsku je stavění silnic a železnic problematičtější vzhledem k horskému terénu. I přesto má ovšem vynikající síť silnic(zhruba 70 000 km)a tunely, umožňující provoz i v zimě[8]. Nejhorší situace je v nejspíše České republice, kde je sice hustá železniční síť, ovšem je poněkud zastaralá a neumožňující velké rychlosti. Stav dálnic také není příliš uspokojivý.

Důležitou roli hrají také přírodní podmínky. Zatímco Německo hojně využívá vodní dopravu díky tomu, že má přístup k moři i velké řeky, v České republice a Švýcarsku hraje druhořadou roli.

## **Finanční sektor.**

Sektor, který stále více nabývá na významu. Patří sem bankovníctví , pojišťovnictví, obchody s cennými papíry a další. Světově uznávanou finanční jedničkou je Švýcarsko. Především pro svojí korektnost, politickou stabilitu a stabilitu měny.

Protože se dnes většina finančních transakcí odehrává pomocí výpočetní techniky, je třeba, aby byl tento sektor velmi dobře zabezpečen pro počítačovým pirátům.

## Odpovědné subjekty

V této analýze jsou subjekty, odpovídající za fungování kritické infrastruktury. Ty subjekty, které jsou uvedeny vedle sebe, mají podobné kompetence a svěřené povinnosti. Neznamená to ale, že by si byly naprosto rovný.

**Tabulka 2 - Srovnání nejdůležitějších orgánů činných při ochraně KI**

| Česká rep.                                                            | Německo                                                    | Švýcarsko                                                                                           |
|-----------------------------------------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Ministerstvo vnitra ČR                                                | Spolkové ministerstvo vnitra                               |                                                                                                     |
| Výbor pro civilní a nouzové plánování                                 | Spolkový úřad pro civilní ochranu a pomoc při katastrofách | Spolkový úřad po civilní ochranu                                                                    |
| Ministerstvo obrany ČR                                                |                                                            | Spolkové ministerstvo obrany, civilní ochrany a tělovýchovy                                         |
| Bezpečnostní rada státu<br>Hasičský záchranný sbor<br>České republiky | Spolkový úřad pro informační bezpečnost                    | Spolková strategická jednotka pro informační technologie                                            |
|                                                                       | Federální agentura technické pomoci                        |                                                                                                     |
|                                                                       |                                                            | Pracovní skupina ochrany kritické infrastruktury -celkem 23 úřadů<br>Popsány v kapitole o švýcarsku |
|                                                                       | Spolkové ministerstvo hospodářství a práce                 |                                                                                                     |

Většina orgánů již byla popsána v kapitolách o jednotlivých zemích.

Je zde ovšem jeden velmi zajímavý fakt. Zatímco v Německu a Švýcarsku poměrně dobře funguje spolupráce soukromého a veřejného sektoru (prostřednictvím např Spolkového ministerstva hospodářství a práce v Německu, či MELANI ve Švýcarsku) v České republice je tato spolupráce nedostatečná.

### 3.4.2 Uvažovaná rizika a hrozby

Každý stát má vypracovaný seznam rizik, o kterých se domnívá, že mohou ohrozit jeho infrastrukturu. Jak je vidět, mnoho z nich je pro všechny země stejné. Tato rizika jsou uvedena v tabulce.

**Tabulka 3 - Seznam rizik srovnávaných zemí**

| Česká rep.                                  | Německo                      | Švýcarsko                        |
|---------------------------------------------|------------------------------|----------------------------------|
| Živelné pohromy                             | Následky extrémního počasí   | Povodně, sucho, extrémní teploty |
|                                             | Lesní požáry                 | Velký oheň                       |
|                                             | Zemětřesení                  | Zemětřesení                      |
|                                             |                              | Lavina                           |
| Pandemie, infekční nemoci                   | Epidemie a pandemie          | Pandemie                         |
| Technické poruchy, kolaps počítačových sítí | Selhání technických systémů  | Technické selhání systému        |
|                                             | Nedbalost                    | Lidské chyby                     |
|                                             | Nehody a mimořádné události  |                                  |
|                                             | Nedostatečná organizace      |                                  |
| Teroristický útok                           | Terorismus                   | Terorismus                       |
| Důsledky války                              | Občanské a mezinárodní války | Ozbrojený konflikt               |
| Kriminální čin                              | Jiné formy kriminality       | Vydírání, organizovaný zločin    |

Jsou zde obsažena všechna rizika, která jednotlivé státy připouštějí. Ovšem ve skutečnosti se některé státy soustředí na některá více než na jiná.

Například Německo se obává hrozby terorismu. Úspěšný útok na území této velmoci by znamenal pro různé teroristické skupiny jistě velký ohlas, stejně jako tomu bylo při útoku na jiné významné země (USA, Velká Británie, Španělsko). Tato země má zkušenosti s terorismem od roku 1972, kdy se v Mnichově konala olympiáda. V současnosti nejvíce řeší problém počítačového terorismu a ochrany kritické informační infrastruktury.

Švýcarsko se podle První zprávy o ochraně kritické infrastruktury soustředí na ohrožení kritické infrastruktury v důsledku zemětřesení, pandemie, výpadků energie a narušení informační infrastruktury (tedy stejně jako Německo).

Naproti tomu stejně jako Česká republika, nepokládá hrozbu terorismu za svojí největší prioritu při ochraně kritické infrastruktury. Spíše vnímá ochranu kritické infrastruktury komplexně. Trochu je zde znát lehký důraz na přírodní rizika.



## **Terorismus**

Je všeobecně považován za jednu z největších hrozeb pro dnešní společnost. Zprávy o teroristických útocích jsou velmi běžné, ale málokdy se tak děje na území vyspělé země. Pokud se tak však stane, vždy se rozpoutají otázky, zda bylo pro bezpečnost dané země uděláno maximum. Nejznámějšími útoky teroristů ve vyspělých zemích byly události 11. září 2001 v americkém New Yorku, v roce 2004 ve španělském Madridu a konečně 2005 v Londýně.

Pokud jde o vybrané země, pak hrozbou terorismu se vážněji zabývá jen Německo. Soustřeďuje se především na hrozbu kybernetického terorismu prostřednictvím Spolkového úřadu pro informační bezpečnost.

## **Přírodní katastrofy**

Tento široký pojem v sobě zahrnuje hrozby jako jsou povodně, lesní požáry, vichřice, tornáda, laviny zemětřesení, extrémní sucha, či jiné

V této oblasti hodně záleží na geografické poloze dané země. Zatímco např. v Japonsku nebo v americkém Los Angeles je hrozba zemětřesení poměrně významná, ve střední Evropě se ho bát téměř nemusíme.

Švýcarsko se díky svému horskému profilu zabezpečuje před lavinovými nebezpečími. Zatímco Česká republika či Německo v poslední době trpělo záplavami na Vltavě resp. na Labi.

## **Epidemie a pandemie**

Touto hrozbou může být postižena jakákoliv země a její důsledky mohou být značné. Ať už jde o kvalitu života, či hospodářskou stabilitu. Podobných neštěstí jako byly morové epidemie ve středověku se díky vyspělému zdravotnictví bát nemusíme. Ale přesto je třeba se chránit před nebezpečnými nemocemi jako je např. Aids a v poslední době tzv. "Nemoc šílených krav", SARS nebo ptačí, či prasečí chřipka.

Všechny srovnávané země mají vyspělé zdravotnictví, kterému se zatím daří podobným hrozbám čelit.

## **Závěr**

Problematika kritické infrastruktury je poměrně nová. První snahy o její ochranu se objevily v USA na konci 20. století (1998 – Bílá kniha). Skutečný význam ale dostala až po 11. září 2001. Po těchto útocích se ukázalo, co může takováto mimořádná událost učinit s dostupností služeb, pocitem bezpečí, dodávkami zboží atd.

Proto se začaly všechny země světa, nebo alespoň ty vyspělé, tímto problémem více zabývat. Evropská unie udělala první velký krok v roce 2004, kdy vydala směrnici Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“. Zde definovala termín kritická infrastruktura a navrhla principy její ochrany. Posléze vydala dokument s názvem Zelená kniha, ve které byla problematika ještě více upřesněna.

V těchto dokumentech byl mezi principy ochrany uveden i princip subsidiarity. Tento princip vyjadřuje fakt, že ochrana infrastruktury na národní úrovni je především v kompetenci jednotlivých států. Hlavní odpovědnost tedy především spadá pod členské země EU. Proto se způsob její ochrany, jednotlivé oblasti, způsob ochrany, priority, rizika, zákony, pověřené orgány a další věci mohou lišit. Velká Británie a Španělsko se soustřeďují na hrozbu terorismu, Německo pak především na jeho kybernetickou formu. Naproti tomu země jako Švédsko či Česká republika se zaměřují spíše na hrozby přírodního charakteru.

Další důležitou věcí je spolupráce veřejného a soukromého sektoru. Zatímco Švýcarsko, Německo či Velká Británie těží ze spolupráce těchto dvou sektorů, v České republice se to zatím příliš nedaří.

V přístupu k ochraně kritické infrastruktury jednotlivých států hrají roli i geografické podmínky. To je vidět např. u hornatého Švýcarska, které začlenilo do seznamu svých hrozeb nebezpečí lavin.

Země, patřící do Evropské unie, ovšem pociťují i působení této instituce. Jde především o Zelenou knihu, ale i o Evropský program na ochranu kritické infrastruktury. Ten má vliv na při tvorbě dokumentů, které obsahují plánování strategie ochrany kritické infrastruktury těchto zemí.

Bude zajímavé sledovat, jestli dále bude Evropská unie nechávat hlavní odpovědnost v této problematice na členských zemích, nebo zda vezme většinu jejich současných pravomocí do svých rukou. Možná že se dočkáme dne, kdy bude věc ochrany kritické infrastruktury věcí celosvětového (nebo alespoň toho vyspělého světa) provázaného systému.

Jedna věc je ale naprosto zřejmá, a to ta, že pokud si chceme uchovat současnou kvalitu života se všemi dostupnými službami a výhodami dnešní doby, je třeba kritickou infrastrukturu udržovat stále funkční a nenarušenou.

# Seznam použité literatury

- [1] KARDA, L., KUDLÁK, A. Analýza, metody a nástroje řešení krizových situací. České Budějovice, 2007
- [2] LINHART, P. Některé otázky ochrany společnosti. Praha: MV-GŘ HZS ČR, 2005. ISBN 80-86640-43-4.
- [3] PROCHÁZKOVÁ, D., ŘÍHA, J. Krizové řízení. Praha: MV-GŘ HZS ČR, 2004. ISBN 80-86640-30-2.
- [4] Zelená kniha o Evropském programu na ochranu kritické infrastruktury [online]. Komise evropských společenství. V Bruselu dne 17. 11. 2005 KOM(2005) 576 v konečném znění. [cit. 2009-05-15]. Dostupný na WWW: <[http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005\\_0576cs01.pdf](http://eur-lex.europa.eu/LexUriServ/site/cs/com/2005/com2005_0576cs01.pdf)>
- [5] Sdělení Komise Radě a Evropskému parlamentu „Ochrana kritické infrastruktury při boji proti terorismu“ [online]. Komise evropských společenství. V Bruselu dne 20.10. 2004 KOM(2004) 701 v konečném znění. [cit. 2009-05-15]. Dostupný na WWW: <<[http://www.europarl.europa.eu/meetdocs/2004\\_2009/documents/com/com\\_com\(2004\)0701\\_/com\\_com\(2004\)0701\\_cs.pdf](http://www.europarl.europa.eu/meetdocs/2004_2009/documents/com/com_com(2004)0701_/com_com(2004)0701_cs.pdf)>
- [6] Sdělení Komise „O Evropském programu na ochranu kritické infrastruktury“ [online].. Komise evropských společenství. V Bruselu dne 12.12. 2006 KOM(2006) 786 v konečném znění. [cit. 2009-05-15]. Dostupný na WWW: <<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:CS:PDF>>
- [7] Bezpečná Evropa v lepším světě: Evropská bezpečnostní strategie [online]. Středisko bezpečnostní politiky CESES FSV UK, Praha 2007. [cit. 2009-05-18] Dostupný na WWW: <<http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIICS.pdf>>
- [8] BATEMAN, G., EGANOVÁ, V. Zeměpis světa, Praha, 1999. ISBN 80-901727-6-8
- [9] Zpráva o stavu zajištění bezpečnosti České republiky v oblasti ochrany před mimořádnými událostmi [online]. Ministerstvo vnitra – generální ředitelství, 30.března 2006 [cit. 2009-04-15] Dostupný na WWW: <<http://www.vlada.cz/assets/ppov/brs/dokumenty/Zprava.pdf>>
- [10] Výkladový slovník krizového řízení a obrany státu [online] [citace 2009-04-05] Dostupný na WWW: <[http://web.mvcr.cz/archiv2008/udalosti/slovník/index\\_odbor\\_info.html](http://web.mvcr.cz/archiv2008/udalosti/slovník/index_odbor_info.html)>
- [11] MARTÍNEK, B. Východiska a principy zajištění ochrany kritické infrastruktury v České republice [online] [citace 2009-06-08] Dostupný na WWW: <[http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana\\_22.html](http://web.mvcr.cz/archiv2008/casopisy/112/2008/duben/strana_22.html)>
- [12] ŠENOVSKÝ, M. Ochrana obyvatel 2007, Ostrava 2007. ISBN 80-86634-51-5

- [13] MALINÍK, L. Ochrana kritické infrastruktury České republiky, Zlín, 2008 [online]  
[citace 2009-06-08]  
Dostupný na WWW:  
<[http://209.85.135.132/search?q=cache:qKPmPEG7nt4J:https://www.stag.utb.cz/apps/stag/di  
pfile/index.php%3Fdownload%3D9617+ochrana+kritick%C3%A9+infrastruktury+%C4%8D  
esk%C3%A9&cd=6&hl=en&ct=clnk](http://209.85.135.132/search?q=cache:qKPmPEG7nt4J:https://www.stag.utb.cz/apps/stag/di<br/>pfile/index.php%3Fdownload%3D9617+ochrana+kritick%C3%A9+infrastruktury+%C4%8D<br/>esk%C3%A9&cd=6&hl=en&ct=clnk)>
- [14] Erster Bericht an den Bundesrat zum Schulz Kritischer Infrastrukturen [online]  
Spolkový úřad pro civilní ochranu, 2007. [citace 2009-06-08] Dostupný na WWW:  
<[http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.56405.downlo  
adList.17582.DownloadFile.tmp/2.skibericht20090605d.pdf](http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.56405.downlo<br/>adList.17582.DownloadFile.tmp/2.skibericht20090605d.pdf)>
- [15] Členské země Evropské Unie [online] [citace 2009-07-05]  
Dostupný na WWW:  
<[http://www.finance.cz/evropska-unie/seznamy/clenske-  
zeme/?form1971\[LimitPocet\]=0&form1971\[LimitOd\]=0&form1971\[OrderBy\]=0&form1971  
\[OrderDesc\]=0&form1971\[SetSettings\]=1&form1971\[detail\]=15&form1971\[internal\\_val\]=2  
#Kotva1971](http://www.finance.cz/evropska-unie/seznamy/clenske-<br/>zeme/?form1971[LimitPocet]=0&form1971[LimitOd]=0&form1971[OrderBy]=0&form1971<br/>[OrderDesc]=0&form1971[SetSettings]=1&form1971[detail]=15&form1971[internal_val]=2<br/>#Kotva1971)>
- [18] Mogza, J., Vitek M., Kovářik F. Kritická infrastruktura společnosti, Hradec králové,  
2008. ISBN 978-80-7041-299-2
- [19] Europa – portál evropské unie [online] [citace 2009-07-05] Dostupný na WWW:  
<[http://europa.eu/index\\_cs.htm](http://europa.eu/index_cs.htm)>
- [20] Bílek M. Problematika kritické infrastruktury [online] [citace 2009-07-05] Dostupný na  
WWW: <[http://www.ceses.cuni.cz/CESES-70-version1-KI\\_Bilek.pdf](http://www.ceses.cuni.cz/CESES-70-version1-KI_Bilek.pdf)>
- [21] National Strategy for Critical Infrastructure Protection [online]  
Spolkové ministerstvo vnitra, Německo, 17. června 2009 [citace 2009-07-05]  
Dostupný na WWW:  
<[http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34413/kritis\\_englis  
ch.pdf](http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34413/kritis_englis<br/>ch.pdf)>
- [22] Critical infrastructure protection in Germany [online]  
Spolkový úřad pro informační bezpečnost, 2005 [citace 2009-04-05]  
Dostupný na WWW:  
<[http://cip.gmu.edu/archive/8\\_CIPinGermany\\_2005.pdf](http://cip.gmu.edu/archive/8_CIPinGermany_2005.pdf)>
- [23] National response plans: IT-Crisis Response in Germany [online]  
Spolkový úřad pro informační bezpečnost, 29. května 2008 [citace 2009-04-05]  
Dostupný na WWW:  
<[http://www.enisa.europa.eu/doc/pdf/other/4th\\_cert\\_ws/DE\\_presentation.pdf](http://www.enisa.europa.eu/doc/pdf/other/4th_cert_ws/DE_presentation.pdf)>
- [24] Protection of Critical Infrastructures – Baseline Protection Konzept [online]  
Spolkové ministerstvo vnitra, Německo [citace 2009-04-05]  
Dostupný na WWW:  
<[http://www.en.bmi.bund.de/cln\\_028/nn\\_1016300/Internet/Content/Themen/Terrorism/Data  
AndFacts/Baseline\\_\\_Protection\\_\\_Concept\\_\\_en.html](http://www.en.bmi.bund.de/cln_028/nn_1016300/Internet/Content/Themen/Terrorism/Data<br/>AndFacts/Baseline__Protection__Concept__en.html)>

[25] Stránky Spolkového úřadu pro informační bezpečnost [online] [citace 2009-06-05]  
Dostupný na WWW: <<https://www.bsi.bund.de>>

[26] The Swiss Programme on Critical Infrastructure Protection [online] [citace 2009-08-05]  
Spolkový úřad pro civilní ochranu. Dostupný na WWW:  
<<http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.93673.DownloadFile.tmp/factsheete.pdf>>

## Seznam obrázků

|                                                        |    |
|--------------------------------------------------------|----|
| Obrázek 1 - Příklad sítě kritické infrastruktury ..... | 9  |
| Obrázek 2 - Představa OKI v Německu .....              | 42 |
| Obrázek 3 - Organizační uspořádání BSI.....            | 43 |

## Seznam tabulek

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Tabulka 1 - Srovnání oblastí KI porovnávaných zemí .....                 | 52 |
| Tabulka 2 - Srovnání nejdůležitějších orgánů činných při ochraně KI..... | 54 |
| Tabulka 3 - Seznam rizik srovnávaných zemí .....                         | 55 |